Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

Iris identification Method of Biometric Authentication

Joshi Nidhi Ghanshyam

Research Scholar, Computer Science,

Sabarmati University, Ahmedabad

Dr. Subhashchandra Desai

Professor and Director, Computer Science,

Sabarmati University, Ahmedabad

ABSTRACT

The iris is the colored, donut-shaped portion of the eye behind the cornea and surrounds the pupil. A person's iris pattern is unique and remains unchanged throughout life. Also, covered by the cornea, the iris is well protected from damage, making it a suitable body part for biometric BIOMETRICs is the measurement of human physiological characteristics for security reasons. There are so many types of biometrics existed including finger print, iris recognition, voice recognition. From the above mentioned biometric techniques Iris recognition gives better security and it has more advantages over other types of biometric authentication methods.

Keywords: Biometric authentication, Iris recognition, Normalization, Segmentation.

Introduction:

Iris biometric authentication as it has low error rates compared to other biometric authentication methods .The iris is the colored ring in our eyes, a muscle that expands and contracts the eye based on the amount of light entering the eye itself. On the surface, we don't see the complexity of the iris—we see the melanin-colored ring but not much else. These scans function as verification methods because each human iris has unique patterns and color circles that can be used to identify them. Basic idea of the method is as follows: First of all, it locates the image of iris and then it fits the contour of lower eyelid, after that normalization to the iris image is done and gets 512 columns x 64 rows rectangular iris image. Next thing is that it makes segmentation according to the filter parameters and then it adopts optimized multi directional filter so that it gives filter for each sub-block in the effective iris image area, and also gets edge response of iris image in different directions. Biometric scanning uses a user's physical features (a fingerprint, facial scan, voice authentication, or iris scan) as part of an identity verification process. The idea behind this approach to authentication is that these physical features should be almost 100% unique to the user, and as such, can serve as an un-spoofable way to verify them when they try to access their accounts. Some forms of biometrics are more common than others in the consumer and enterprise space. Fingerprint and facial scanners are more and more common on mobile devices like smartphones, tablets, and laptops. These biometrics are used to grant access to devices or to support biometric password setups for applications installed on the devices.

Features of iris recognition

- Highly accurate and fast, iris recognition boasts of having top-class precision among different types of biometric authentication technologies.
- Remains unchanged throughout life. (This does not constitute a guarantee.)
- Since the iris is different between the left and right eye, recognition can be performed separately by each eye.
- Possible to distinguish twins.
- As long as the eyes are exposed, iris recognition can be used even when the subject is wearing a hat, mask, eyeglasses or gloves.
- Because of using an infrared camera, recognition is available even at night or in the dark.
- Without the need to touch the device, contactless authentication is possible, making it hygienic to use.

Biometric Technology

Now A days in many applications, the identity of a person is necessary. For the secure access of anything personal identification is needed. There are some conventional methods for the recognition of individual. The methods include the use of cards or passwords which are not always reliable or accurate, because these cards or passwords can be stolen or forgotten. But in Biometric technology, it uses Artificial Intelligence, for the identification of particular features for the particular human body. By using the particular feature, the biometric authentication system identifies the specific user. The physical structure of the some part of human body like hand geometry, DNA, retina, iris and palm is unique. A biometric system gives automatic recognition of an individual based on unique feature possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, palm recognition, handwriting, and the retina.

Advantages of Using Biometrics:

- Easier fraud detection
- Better than password/PIN or smart cards
- No need to memorize passwords
- Requires physical presence of the person to be identify
- Unique physical or behavioural characteristic
- Cannot be borrowed, stolen, or forgotten.

Segmentation

The first step of iris recognition is to differentiate iris region in a digital eye image which can be taken from CASIA iris database. The iris region, can be divided in two circles, one for the iris /sclera boundary and another, interior for the iris/pupil boundary. The eyelids and eyelashes present at the upper and lower parts of the iris region. Spectacular reflections can present in the iris region in some of the images which corrupts the iris pattern. A technique is required to isolate and exclude these artefacts. Also, locating the circular iris region is required. The success of segmentation depends on the quality of images. Images in the CASIA iris database do not contain spectacular reflections due to the use of near infra-red light for illumination. Circular Hough transform is most of the time used for differentiating the iris and pupil boundaries. First it applies canny edge detection to create an edge map. Vertical and horizontal gradients were weighted equally for the inner iris/pupil boundary. A modified version of Kovesis Canny edge detection was implemented, which allowed for weighting of the gradients. The range of radius values to search for was set manually and that can be depending on the database used. For the CASIA database, values of the iris radius range from 90 to 150 pixels, while the pupil radius ranges from 28 to 75 pixels. For the making the circle detection process more accurate, the Hough transform for the iris/sclera boundary was performed first, then the Hough transform for the iris/pupil boundary was performed second within the iris region, instead of the whole eye region. After this process was complete, six parameters are stored, the radius, and x and y centre coordinates for both circles. The centre of the pupil was considered as the reference point, and radial vectors pass through the iris region. A number of data points are selected along each radial line and this is defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution. Since the pupil can be non-concentric to the iris, a remapping formula is needed to rescale points depending on the angle around the circle. The normalisation process is able to rescale the iris region so that it has constant dimension.

The iris has a particularly interesting structure and provides abundant texture information. For the accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made.

Literature Review

In heterogeneous iris recognition, Nianfeng Liu et al [1] proposed a code-level plan. A modified Markov network was used to demonstrate the non-linear link between binary elements coding of diverse iris pictures. The model can also provide a weight map on the reliability of binary codes in the iris template. In comparison to the present pixel-level, feature-level, and score-level solutions, broad exploratory findings of matching cross sensor, high-resolution versus low-resolution, and clear versus veiled iris images revealed that the code-level technique can achieve the most remarkable accuracy.

To establish the stand-off distance in an iris recognition framework, Sheng-Hsun Hsieh et al. [2] recommended a new hardwaresoftware hybrid technique. To increase the field depth, they used an enhanced wavefront coding approach when developing the framework hardware. On the software side, the disclosed framework used a local patch focused super-resolution method to reestablish the obscured image to its clear variation to compensate for the image obscuring induced by wavefront coding. The provided framework may triple the catch volume of a standard iris recognition framework while maintaining its high recognition rate. However, due to the hardware implementation, the planned model has the disadvantage of being expensive.

Zhiyong Peng et al. [3] have developed an improved Daugman iris identification method that incorporates two aspects: improvement for iris confinement and improvement for iris encoding and matching algorithms. In Step 1, the iris image was used to determine the pupil's location and shape. In Step 2, the potential noise from residual eyelashes was also isolated by using a "pure" iris component as a reference and making pixel-by-pixel approval decisions. The proposed method offers a demonstrable benefit in increasing speed while lowering the dismissal rate.

Imran Naseem et al. [4] proposed the concept of class-specific dictionaries for iris recognition. The query image was essentially depicted as a linear mixture of training images from each class. The problem of the well-conditioned inverse was handled using least squares regression, and the decision was made in favour of the class with the most accurate estimation. Because of the imprecise segmentation of the iris region, an augmented modular method was also recommended to combat noise. The proposed approach was compared to the newfangled Representation Classification with Bayesian Fusion, which is aimed at a wide range of industries. The complexity study of the offered algorithm proved the recommended approach's undeniable superiority.

Soubhagya Sankar Barpanda et al. [5] used a multi-resolution analysis of the iris template to project energy-centered characteristics. It was based on the triplet half-band filter bank that was recommended (THFB). The iris template was divided into six equispaced sub-templates, and each sub-template was subjected to two levels of deterioration using THFB, with the exception of the second. As a result, energy features were derived from each sub-decayed template's coefficients. A comparison was made using already available features such as the Gabor transform, the CDF 9/7 filter bank, and the Fourier transform. The proposed scheme outperformed the competition in terms of FAR, GAR, and AUC.

Francesco Marra et.al [6] offered an algorithm grounded upon convolutional neural networks aimed at iris sensor display identification. A conceivable solution comprises in first differentiating the sensor model and afterwards mapping the features extracted as of the image from one sensor to the other. They established that the presented solution beats the cream of the crop approaches utilized for the model identification task. At that point, they tried the biometric recognition framework’s performance and demonstrated that enhancing the sensor model identification stage can profit the iris sensor interoperability.

Feature Encoding Algorithms

Feature encoding was implemented by convolving the normalised iris pattern with 1D Log-Gabor wavelets. The 2D normalised pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalised pattern are taken as the 1D signal, each row corresponds to a circular ring on the iris region. The angular direction is taken rather than the radial one, which corresponds to columns of the normalised pattern, since maximum independence occurs in the angular direction. The intensity values at known noise areas in the normalised pattern are set to the average intensity of surrounding pixels to prevent influence of noise in the output of the filtering. The output of filtering is then phase quantised to four levels using the Daugman method , with each filter producing two bits of data for each phasor. The output of phase quantisation is chosen to be a grey code, so that when going from one quadrant to another, only 1 bit canges. This will minimise the number of bits disagreeing, if say two intra-class patterns are slightly misaligned and thus will provide more accurate recognition. The encoding process produces a bitwise temp late containing a number of bits of information, and a corresponding noise mask which corresponds to corrupt areas within the iris pattern, and marks bits in the template as corrupt. Since the phase information will be meaningless at regions where the amplitude is zero, these regions are also marked in the noise mask.

Matching Algorithms

Hamming distance

The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one. In com paring the bit patterns X and Y, the Hamming distance, HD, is defined as the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N, the total number of bits in the bit pattern. If two bits patterns are completely independent, such as iris templates generated from different irises, the Hamming distance between the two patterns should equal 0.5. This occurs because independence implies the two bit patterns will be totally random, so there is 0.5 chance of setting any bit to 1, and vice versa. Therefore, half of the bits will agree and half will disagree between the two patterns. If two patterns are derived from the same iris, the Hamming distance between them will be close to 0.0, since they are highly correlated and the bits should agree between the two iris codes.

What Are the Four Steps for Iris Recognition Enrolment?

The enrolment and verification process is rather seamless for users: the system scans the eye and uses it to verify identity. However, to actually use information from the iris as a form of identification, a four step enrolment process takes the information and makes it a form of biometric ID:

Image Capture: The scanner takes high quality images of the left and right eye using near infrared light for a more accurate and fine grained image of the iris and its unique features. Near infrared light also doesn't cause contractions in the iris the same way natural light would, providing a more realistic image from which to draw information.

Quality Checks and Controls: Now that the system has an image to draw information from, it performs quality checks to ensure that the image is enough to serve as a biometric template. Different image qualities are tested during this step, including analysis of the sharpness, iris sclera contrast, iris pupil contrast, pupillary dilation and the presence of any artifacts like eyelashes and eyelid occlusions. During this analysis, the scan segments of the recognizable iris from the rest of the eye in the image.

Compression: The remaining, high quality image is compressed using JPEG 2000 algorithms. This helps remove image distortions and other artifacts. Template Creation: The remaining image information is then translated into a biometric template that can be used in future verification scans. Once the template is in place, it is difficult to spoof using fake biometrics. Likewise, this information can be used across multiple authentication events so long as you use the same or similar quality NIR scanners.

What Are the Advantages of Iris Biometrics?

While not as common as other biometric verification methods, eye scans have several advantages:

Difficulty of Spoofing: Since iris information is unique to everyone and requires special technology to collect, it can be hard to spoof this information for unauthorized access.

Persistence: Iris dimensions and conditions don't vary much as we age, meaning that scans have significant longevity as verification methods. Likewise, barring trauma to the eyes, they are not typically vulnerable to physical disfigurement.

Distance and Flexibility: It might seem like it would be hard to scan an iris, but advances in cameras and light technology have made it possible to scan a human iris from up to 40 feet away.

With these advantages in mind, eye scanners are often more accurate and reliable than fingerprint or facial scanners. Fingerprint scanners are touch based, meaning that dirt, grease, or other artifacts can hinder fingerprint scans. Likewise, individuals who do hard work that damages the fingers might be unable to use the technology or find it doesn't work for them as they get older. On the other hand, eye scanners don't degrade in functionality unless there is

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.j.vidhyayanaejournal.org
Indexed in: ROAD & Google Scholar

trauma to the eyes, and eyes are self cleaning by nature. Because of this, iris scanners can serve a broader population than a fingerprint verification system, particularly populations from poor or working class backgrounds.

A method of biometric authentication that uses pattern recognition techniques based on high resolution images of the irises of an individual's eye. Iris recognition utilizes the same technology as cameras coupled with subtle infrared illumination to reduce the specular reflection from the convex cornea. This creates detail rich images of the intricate structures of the iris. When these images are converted and stored as digital templates, they provide mathematical representation of the iris that enables unambiguous positive identification of individuals.

Accuracy

Iris is formed in the early stages of an individual's life and once it is fully formed its texture remains stable throughout a person's life. The iris of the eye has a distinct pattern and iris recognition has been found to be a highly accurate biometric system. Its efficiency is rarely impeded by the presence of glasses or contact lenses. Moreover, it has a small template size that allows speedy comparisons making iris recognition technology particularly well suited for one-to-many identifications. Even genetically identical individuals have distinct iris textures which further confirm that it is a highly accurate and reliable technique.

FAR/FRR

National institute of standards technology conducts many evaluation tests to determine accuracy of biometric devices and the accuracy proven by NIST tests is considered to be the international recognition for the these devices and superior technology provided by vendors. The test for iris recognition systems conducted by NIST where FAR and FRR are the evaluation metrics is known as Iris Exchange or IREX test.

The error rates as per the ICE 2006 are

FRR=1% and FAR=0.1%

Verdict

Iris recognition is a very stable technique with high template longevity where a single enrolment can last a lifetime. Since iris is an internal organ, it is very well protected against damage and wear by a transparent and sensitive membrane known as the cornea. This feature distinguishes irises from fingerprints which can be quite difficult to recognize after certain years of manual labour. Also, the geometric configuration of the iris is only controlled by two complementary muscles. This makes the shape of the iris far more predictable than that of the face. However, iris scanners are relatively expensive as compared to other modalities and require user-cooperation. Iris recognition systems have been implemented in all of the UAE's air, land and sea ports of entry. Google too uses this technology to regulate access to its data center. The FBI has also incorporated it into its next generation biometric identification system.

Usability

Although iris recognition is the most accurate biometric system and works very well for positive identification against a large database, there are some usability concerns. It is a new technology that requires substantial investment and hence may not be suitable for small organizations. It is quite difficult to perform iris recognition from a distance larger than a few metres and moreover the subject to be identified needs to be co-operative. The subject should hold his or her head still and look into the camera. Iris recognition is also susceptible to poor quality of images as well as associated failure to enrol rates. However, iris has a fine texture similar to that of fingerprints and is formed randomly during embryonic gestation. This fine texture remains stable for many decades and attributes iris recognition to be the most accurate modality. Some iris identification schemes have succeeded over a period of almost 30 years.

CONCLUSION

The recognition of person through this iris authentication system is simple and requires few components. This system is effective enough to be integrated within security systems that require an identity check. There are negligible errors that occurred when this system used and that can be easily overcome by the use of proper and stable equipment. Iris recognition is a recent technique in the area of the personal identification and it is considered as one of the most reliable ways of biometrics.

REFERENCES

1. Nianfeng Liu, Jing Liu, Zhenan Sun and Tieniu Tan, "A Code-level Approach to Heterogeneous Iris Recognition", IEEE Transactions on Information Forensics and Security, Vol. 12, No. 10, pp. 2373 – 2386, 2017.
2. Sheng-Hsun Hsieh, Yung-Hui Li, Chung-Hao Tien, and Chin-Chen Chang, "Extending the capture volume of an iris recognition system using wavefront coding and superresolution", IEEE transactions on cybernetics Vol. 46, No. 12, pp. 3342-3350, 2016.
3. Zhiyong Peng, Hongchen Wang, Jun Wu, and Jun Li, "An improved Daugman method for iris recognition", Wuhan University Journal of Natural Sciences Vol. 20, No. 3, pp. 229-234, 2015.
4. Imran Naseem, Affan Aleem, Roberto Togneri and Mohammed Bennamoun, "Iris recognition using classspecific dictionaries", Computers & Electrical Engineering Vol. 62, pp.178-193, 2016.
5. Soubhagya Sankar Barpanda, Banshidhar Majhi, PankajKumarSa, "Region based feature extraction from non-cooperative iris images using triplet half band filterbank", Optics & Laser Technology, Vol. 72, pp. 6– 14, 2015
6. Francesco Marra, Giovanni Poggi, Carlo Sansone and Luisa Verdoliva, "A deep learning approach for iris sensor model identification", Pattern Recognition Letters pp.1–8, 2017.
7. Aman Jatain, Yojna Arora, Jitendra Prasad, Sachin Yadav, Konark Shivam, Department of Computer Science, Amity University, Gurgaon, Haryana,Design and Development of Biometric Enabled Advanced Voting System May 2020.
8. S.Sanderson, J. Erbetta. Authentication for Secure Environments Based On Iris Scanning Technology. IEE Colloquium on Visual Biometrics, 2000.
9. Chandra Keerthi Pothina , Atla Indu Reddy, Ravikumar CV,Electronics and Communication Engineering, Vellore Institute of Technology, Vellore,Smart Voting System using Facial Detection April 2020.
10. J. Daugman. How iris recognition work s. Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002
11. Saravanan.N, Pavithra.K, Nandhini.C,Dept. of MCA Priyadarshini Engineering College, vaniyambadi, Tamilnadu, India,Iris Based E- Voting System Using Aadhar Database,April-2017
12. Judith Liu-Jimenez,Raul Sanchez-Reillo. Iris Biometrics For Embedded Systems IEEE Transaction Vol 19 NO 2 February 2011
13. J Nithya, G.Abinaya, B.Sankareswari, M.Saravana Lakshmi ,Jeppiaar Engineering College, Chennai- 119,Iris recognition based voting system, July 2015.
14. C.Sanchez-Avila and R. Sanchez-Reillo, Two different approaches for iris recognition using Gabor filters and multi scale zero crossing.