Deformation of Iris Recognition using Dilated Deep Convolutional Neural Network

M. Vijay[1], V.D. Boobeish[2], R. Dhinesh Kumar[3], R. Dhanabalan[4], A. Divin[5]

***Abstract*:** *A biometric framework gives automatic identity proof of an individual based on unique characteristics or features of the individual. Authentication systems based on iris play important role to improve efficiency in biometric identification due to its reliability in highly secured areas. The iris recognition systems have made large progress over the past decade. Due to its unique character as a biometric feature, iris identification and verification systems have become one of the most accurate biometric modality. Iris recognition systems capture an image from an individual's eye. The iris in the image is then segmented and normalized for feature extraction process. We specifically focus on generating a robust representation of iris features by incorporating superior feature extraction network that uses dilated convolution kernels to address frequently observed deformations between the matched iris patterns. Involuntary pupil dilation and scale changes during the iris imaging constitute the key source for the frequently observed iris deformations. The framework for accurate iris recognition investigated in this project. Deeper neural networks are more difficult to train. The new architecture of this branch incorporates the dilated deep convolutional neural networks and residual learning kernels we present a residual learning framework to ease the training of networks that are substantially deeper than those used previously. The dilated convolution kernels employed in the network can support nonlinearly expanding receptive fields without degrading the resolution or coverage. Improvement in the matching accuracy can also be attributed to the usage of residual learning blocks, which can learn the residual information by increasing the depth and enrich the learning capability of the model.*

Keywords: Iris recognition, personal identification, biometrics, deep learning.

I. INTRODUCTION

Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The basic premise of biometric authentication is that every person can be accurately identified by his or her intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio meaning life and metric meaning to measure.

II. TYPES OF MEASUREMENTS

A. Physiological measurements

They can be either morphological or biological. These mainly consist of fingerprints, the shape of the hand, of the finger, vein pattern, the eye (iris and retina), and the shape of the face, for morphological analyses.

For biological analyses, DNA, blood, saliva or urine may be used by medical teams and police forensics.

B. Behavioural measurements

The most common are voice recognition, signature dynamics (speed of movement of pen, accelerations, pressure exerted, inclination), keystroke dynamics, the way objects are used, gait, the sound of steps, gestures, etc.

III. THEORY

How Biometrics work

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Some biometric methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated.

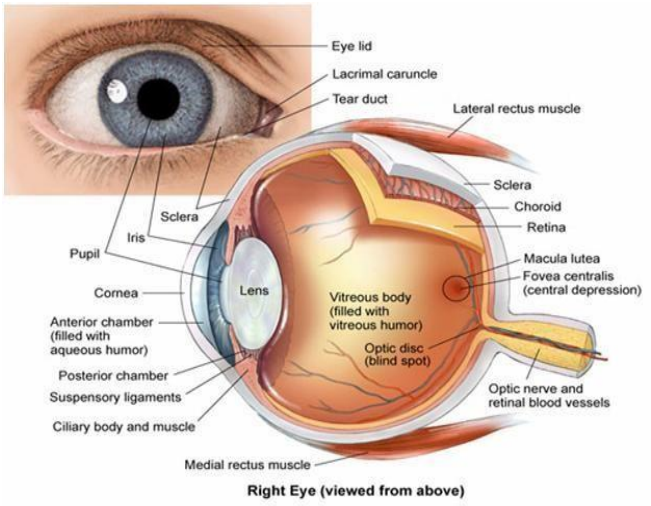
Components of biometric devices include:

- A reader or scanning device to record the biometric factor being authenticated.
- Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data.
- A database to securely store biometric data for comparison.

Biometric data may be held in a centralized database, although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it so that authentication or identification can be accomplished without direct access to the biometric data itself.

Iris

The iris is a flat and ring-shaped membrane behind the cornea of the eye with an adjustable circular opening in the center called a pupil. This is the structure that provides an individual with eye color.



Together with the pupil, the iris is responsible for regulating the amount of light that gets into the eye. Too much or too little light can hamper vision. The muscular iris moves to shrink the pupil if there is too much light and widen it if there is not enough. This is an involuntary function, controlled by the brain.

The iris is made almost entirely of connective tissue and smooth muscle fibers.

Despite a common belief, actual change in color of the iris rarely happens. While the color of an eye may appear to change, this is typically due to lighting changes or perception based off nearby colors.

Iris Recognition

Biometric iris recognition technology is closer to popular use than one might believe it to be. Over 1000 ATMs of financial institutions in Chicago and Montreal are now using iris recognition in lieu of debit cards.

Imagine being able to retrieve money from your bank account simply by looking at your ATM machine. Now stop imagining. It's already happening.

Read on to understand what exactly is biometric iris recognition technology, how it works, what are the benefits of using it and which areas of application it is being used…

The below image shows an iris based biometric authentication in ATMs

What is biometric iris recognition

Biometric iris recognition utilizes pattern recognition techniques based on high-resolution and distortion-free images of the irises of the human eyes.

Iris is an organ whose structure remains stable throughout life. Thus it serves as a very good biometric for establishing identity of an individual.

Because of its very low margin-of-error and fast speed, iris recognition is now one of the most trusted ways of confirming the identity of a person.

Technology overview: biometric iris recognition

Iris recognition systems take high resolution images of the iris of a person's eye and then utilize pattern recognition for reading and matching his iris patterns against the patterns stored in the biometric database.

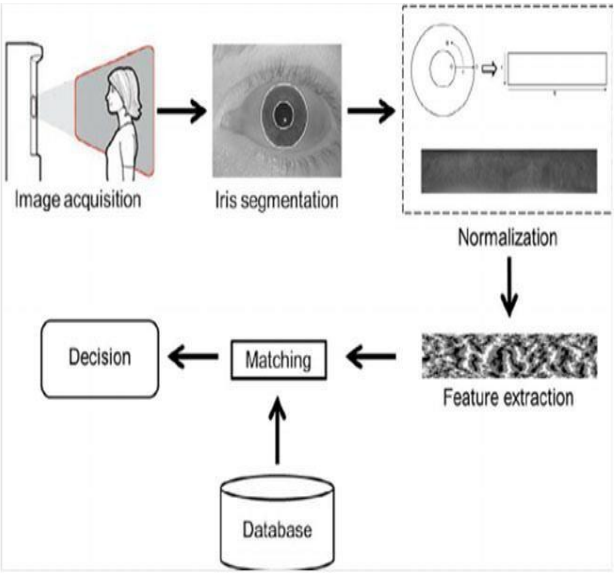


Figure: A block diagram of an iris recognition system

Iris-recognition algorithms, first created by John G. Daughman, are utilized for the image acquisition and matching process.

Most iris recognition systems use a 750 nm wavelength light source to implement near-infrared imaging. This enables the system to block out light reflection from the cornea and thus create images which highlight the intricate structure of iris. But these images become difficult to recognize in the identification step. Hence, now-a-days visual wavelength imaging is being preferred over near infrared imaging.

IV. PROPOSED SYSTEM

Deformated Iris recognition capabilities using deep learning based approaches.

- Dilated Deep Convolutional Neural Network Feature extraction is a main step in classification tasks. Traditional approaches employ hand-crafted features for classification while Dilated Deep convolutional neural networks (DDCNN) are able to extract features automatically.

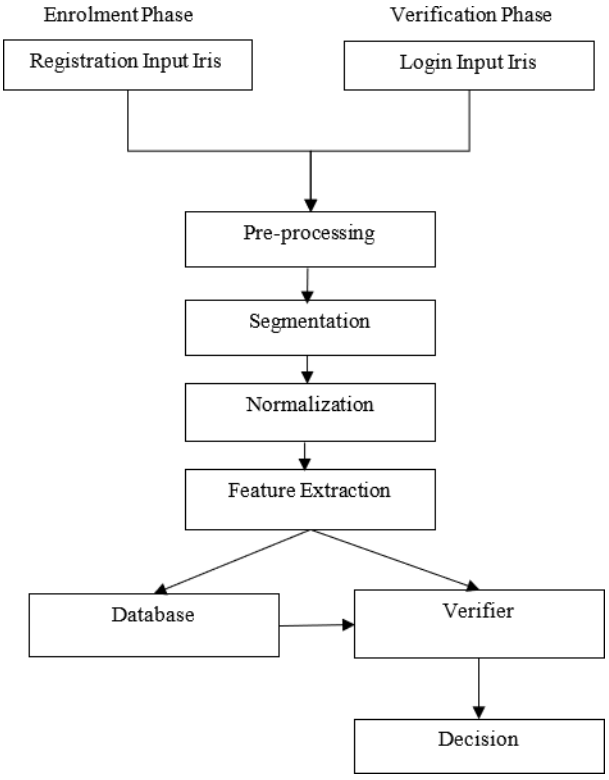


Figure: A block diagram of an iris recognition system proposed method

- Residual Learning Blocks

  The generation of feature maps using the dilated convolution kernels. The dilated kernel in our iris recognition framework is not learning the feature maps for the next layer but the residual information.

- Triplets Selection

  The triplets selection aims to optimize the training process for the triplet network. Triplet pairs are generated from the combination of an anchor sample, with a positive sample and a negative sample. These pairs are respectively fed into the three network branches, each with same parameters. Each of these network branches correspondingly generates feature maps FA, FP and FN, which are used to compute the extended triplet loss (ETL).

V. STEPS IN IRIS RECOGNITION

Iris recognition process consists of three distinct steps:

A. Image capture

The first step consists of capturing the image of the iris of the person whose identity needs to be verified. The image capture

itself can be manual or automated but it needs to be ensured that the iris is in proper focus and that the image is captured with clarity.

B. Locating the iris and optimizing the image

In this step, first the iris recognition system optimizes on the focus and the clarity of the image. It then identifies the iris boundaries followed by the center of the pupil which is also the center of the circular iris. Finally, it analyzes the area of the iris image which is suitable for feature extraction and analysis.

Once the area which is suitable for feature extraction is determined, the iris region is optimized by removing deep shadows, portions covered by eyelids and reflective areas. This optimized region is also normalized in a rectangular block so that it has fixed dimensions which are "comparable" with other iris scans.

Note that it is not possible to compare the optimized Iris image itself with stored iris images. Rather what is stored in the biometric database are biometric templates which contains the encoded structure features of the iris which are extracted from the image after applying Daughman's rubber sheet model.

C. Biometric template storage and/or matching

The encoded structural features, or biometric templates, are then stored in the biometric database at the time of enrollment of a person. If the iris scan has been taken for the purpose of authentication, then the biometric template forthe scanned image is matched with biometric templates storedin the database.

VI. ADVANTAGES

Superiority of iris as compared to other biometric traits Various characteristics of iris which makes it a highly durable and reliable biometric for use in identity management solutions as compared to other biometric traits are-

A. Irises are different for even identical twins.

B. An iris has more than 266 degrees of freedom (i.e. the number of structure variable which can varyat the same time to make iris unique between any two individuals).

C. Likelihood of damage or scratches is there in case of other biometric traits such as fingerprints. But iris is well protected behind the eyelid, cornea and aqueous humor which makes it very less susceptible to damage.

D. Iris doesn't degenerate with aging.

Use of spectacles or contact lenses has no effect whatsoever on the automated reading of iris structures.

Biometrics	Universality	Uniqueness	Collectability	Performance	Acceptability
Face	High	Low	High	Low	High
Fingerprint	Medium	High	Medium	High	Medium
Vascular	Medium	Medium	Medium	Medium	Medium
Iris	High	High	Medium	High	Low
Voice	Medium	Low	Medium	Low	High
DNA	High	High	Low	High	Low

Figure: Comparison of iris recognition with other biometric modalities

High scalability as it is ideal for handling large databases Iris recognition systems are ideal for usage in big enterprises with large number of enrollments. It is in fact the only biometric authentication technology which is capable of working in the 1:n or exhaustive search mode.

Best search speeds among biometric authentication technologies

The one to many search mode is the fastest among all biometrics. Iris recognition based systems are thus the quickest in authenticating a person.

High-levels of safety against identity theft

Iris recognition systems convert the captured iris image into 512-byte encrypted biometric template. Thus reproducing a fake iris match or a spoof is near impossible.

Iris recognition technology is high in user convenience Along with being a non-invasive, contact-less technology, iris recognition provides an intuitive user experience. The user just needs to look at the camera and the identification process gets completed smoothly.

Automated image capture technologies have been used successfully with iris recognition solutions which enhances the user convenience several notches.

VII. APPLICATIONS

A. Finance and banking

Iris recognition technology is being used in banks and financial organizations, replacing the cumbersome and time taking, pin based, and password based systems.

The use of iris recognition is expected to improve standards of financial services as the bankers will become free from time consuming document processing for identity proofs. This in turn will give them ample time and opportunity to concentrate on other important areas such as customer service.

B. Healthcare and welfare

The healthcare industry faces is plagued with the persistent problem of establishing accurate patient identification. Healthcare management applications are turning towards biometric iris recognition technology.

C. Public safety

Biometric technology has a long history with law enforcement agencies and many important identity management innovations have sprouted from this beneficial relationship. For more than a century law enforcement has been using biometric technology to track and identify criminals, helping to enhance public safety and facilitate justice.

VIII. CONCLUSION

In this work we propose a dilated deep learning framework for iris recognition, by fine-tuning a pre-trained convolutional model on ImageNet. We focused on iris recognition task, and chose a dataset with a large number of subjects, but limited number of images per subject, and proposed a transfer learning approach to perform identity recognition using a deep residual convolutional network. This framework is applicable for other biometrics recognition problems, and is specially useful for the cases where there are only a few labeled images available for each class. We apply the proposed framework on a well-known iris dataset, CASIA, IIT-Delhi, and achieved promising results, which outperforms previous approaches on this datasets. We train these models with very few original images per class. We also present a visualization technique for detecting the most important regions while doing iris recognition.

References

[1] J. Daugman, "Iris recognition border-crossing system in the UAE," International Airport Review, vol. 8, no. 2, 2004.

[2] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: A survey," Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281–307, 2008.

[3] L. Masek, "Recognition of human iris patterns for biometric identification," The University of Western Australia, 2003.

[4] J. Daugman, "How iris recognition works," in The essential guide to image processing. Elsevier, 2009, pp. 715–739.

[5] D. M. Monro, S. Rakshit, and D. Zhang, "Dct-based iris recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 586–595, 2007.

[6] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An effective approach for iris recognition using phase-based image matching." IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 10, pp. 1741–1756, 2008.

[7] Y. Zhou and A. Kumar, "Personal identification from iris images using localized Radon transform," in Pattern Recognition (ICPR), 2010 20th International Conference on. IEEE, 2010, pp. 2840–2843.

[8] O. C. Reyes, R. Vera-Rodriguez, P. Scully, and K. B. Ozanyan, "Analysis of spatio-temporal representations for robust footstep recognition with deep residual neural networks," IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018.

[9] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Exploring recurrent neural networks for on-line handwritten signature biometrics," IEEE Access, vol. 6, no. 5128-5138, pp. 1–7, 2018.