Iris Recognition System

Nofal Nadim
Calculatoare si Tehnologia Informatiei
Facultatea de Automatica si Calculatoare
Iasi,Iasi
nadim.nofal@student.tuiasi.ro

I. Introduction

Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person's iris. It is a form of biometric technology in the same category as face recognition and fingerprinting. Iris scanning measures the unique patterns in irises, the colored circles in people's eyes. Biometric iris recognition scanners work by illuminating the iris with invisible infrared light to pick up unique patterns that are not visible to the naked eye. Iris scanners detect and exclude eyelashes, eyelids, and specular reflections that typically block parts of the iris. The final result is a set of pixels containing only the iris. Next, the pattern of the eye's lines and colors are analyzed to extract a bit pattern that encodes the information in the iris. This bit pattern is digitized and compared to stored templates in a database for verification (one-to-one template matching) or identification (one-to-many template matching).

Iris scanning cameras may be mounted on a wall or other fixed location, or they may be handheld and portable. Researchers at Carnegie Mellon University are developing long-range scanners that could even be used to capture images surreptitiously from up to 40-feet away. [12]

Advocates of iris scanning technology claim it allows law enforcement officers to compare iris images of suspects with an existing database of images in order to determine or confirm the subject's identity. They also state that iris scans are quicker and more reliable than fingerprint scans since it is easier for an individual to obscure or alter their fingers than it is to alter their eyes. Technologies that exploit biometrics have the potential for application to the identification and verification of individuals for controlling access to secured areas or materials.1 A wide variety of biometrics have been marshaled in support of this challenge. Resulting systems include those based on automated recognition of retinal vasculature, fingerprints, hand shape, handwritten signature, and voice [4], [5]. Provided a highly cooperative operator, these approaches have the potential to provide acceptable performance. Unfortunately, from the human factors point of view, these methods are highly invasive: Typically, the operator is required to make physical contact with a sensing device or otherwise take some special action (e.g., recite a specific phonemic sequence). Similarly, there is little potential for covert evaluation. One possible alternative to these methods that has the potential to be less invasive is automated face recognition. However, while automated face recognition is a topic of active research, the inherent difficulty of the problem might prevent widely applicable technologies from appearing in the near term [6], [7]. Automated iris recognition is yet another alternative for noninvasive verification and identification of people. Interestingly, the spatial patterns that are apparent in the human iris are highly distinctive to an individual [8], [9] . Like the face, the iris is an overt body that is available for remote (i.e., noninvasive) assessment. Unlike the human face, however, the variability in appearance of any one iris might be well enough constrained to make possible an automated recognition system based on currently available machine vision technologies[19]

II. State-of-the-art & Related Work

A. *State-of-the-Art*

Iris recognition has become a popular research in recent years. Due to its reliability and nearly perfect recognition rates, iris recognition is used in high security areas. Among its applications are border control in airports and harbors, access control in laboratories and factories, identification for Automatic Teller Machines (ATMs) and restricted access to police evidence rooms. This paper provides a review of major iris recognition researches. There are three main stages in iris recognition system: image preprocessing, feature extraction and template matching. Biometric identification is an emerging technology which gains more attention in recent years. It employs physiological or behavioral characteristics to identify an individual. The physiological characteristics are iris, fingerprint, face and hand geometry. Voice, signature and keystroke dynamics are classified as behavioral characteristics. Among these characteristics, iris has distinct phase information which spans about 249 degrees of freedom [10]. This advantage let iris recognition be the most accurate and reliable biometric identification.

The three main stages of an iris recognition system are image preprocessing, feature extraction and template matching.

The iris image needs to be preprocessed to obtain useful iris region. Image preprocessing is divided into three steps: iris localization, iris normalization and image enhancement. Iris localization detects the inner and outer boundaries of iris. Eyelids and eyelashes that may cover the iris region are detected and removed. Iris normalization converts iris image from Cartesian coordinates to Polar coordinates. The normalized iris image is a rectangle image with angular resolution and radial resolution. The iris image has low contrast and non-uniform illumination caused by the position of the light source. All these factors can be compensated by the image enhancement algorithms.

Feature extraction uses texture analysis method to extract features from the normalized iris image. The significant features of the iris are extracted for accurate identification purpose.

Template matching compares the user template with templates from the database using a matching metric. The matching metric will give a measure of similarity between two iris templates. It gives a range of values when comparing templates from the same iris, and another range of values when comparing templates from different irises. Finally, a decision of high confidence level is made to identify whether the user is an authentic or imposter.[19]

B. Related Work

At least 1.5 billion persons around the world (including 1.2 billion citizens of India, in the UIDAI / Aadhaar programme) have been enrolled in iris recognition systems for national ID, e-government services, benefits distribution, security, and convenience purposes such as passport-free automated border-crossings. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches, is the stability[11] of the iris as an internal and protected, yet externally visible organ of the eye.

The commercially deployed iris-recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 1011 if a Hamming distance threshold of 0.26 is used, meaning that up to 26% of the bits in two IrisCodes are allowed to disagree due to imaging noise, reflections, etc., while still declaring them to be a match). While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

Iris recognition works with clear contact lenses, eyeglasses, and non-mirrored sunglasses. The early Sensar technology worked by first finding the face, then the eyes, and then took the Iris images. This was all done using infrared lighting. It is possible to identify someone uniquely in a dark room while they were wearing sunglasses.

Mathematically, iris recognition based upon the original Daugman patents or other similar or related patents define the strongest biometric in the world. Iris recognition will uniquely identify anyone, and easily discerns between identical twins. If a human can verify the process by which the iris images are obtained (at a customs station, entering or even walking by an embassy, as a desktop 2nd factor for authentication, etc.) or through the use of live eye detection (which varies lighting to trigger slight dilation of the pupil and variations across a quick scan which may take several image snapshots) then the integrity of the identification are extremely high. Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing.[14] The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession. The accuracy of scanners can be affected by changes in lighting. Iris scanners are significantly more expensive than some other forms of biometrics, as well as password and proximity card security systems.

Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("Standoff Iris" or "Iris at a Distance" as well as Princeton Identity's "Iris on the Move" for persons walking at speeds up to 1 meter/sec).[15][16]

As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates. As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will. Researchers have tricked iris scanners using images generated from digital codes of stored irises. Criminals could exploit this flaw to steal the identities of others.[17]

The first study on surgical patients involved modern cataract surgery and showed that it can change iris texture in such a way that iris pattern recognition is no longer feasible or the probability of falsely rejected subjects is increased.[18]

As with most other biometric identification technology, an important consideration is live-tissue verification. The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified and is not a manufactured template. Besides a person's physical characteristics, which includes the eyes, one's voice and handwriting too, are not protected by the Fourth Amendment even though they are all constantly exposed.[20] Many commercially available iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face,[citation needed] which makes such devices unsuitable for unsupervised applications, such as door access-control systems. However, this is not the case with all iris recognition algorithms. The problem of live-tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture.

Methods that have been suggested to provide some defence against the use of fake eyes and irises include changing ambient lighting during the identification (switching on a bright lamp), such that the pupillary reflex can be verified and the iris image be recorded at several different pupil diameters; analysing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses; analysing the temporal frequency spectrum of the image for the peaks caused by computer displays.[13]

Other methods include using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material; observing the characteristic natural movement of an eyeball (measuring nystagmus, tracking eye while text is read, etc.); testing for retinal retroreflection (red-eye effect) or for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape.[citation needed] Another proposed[citation needed] method is to use 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features.[13]

A 2004 report by the German Federal Office for Information Security noted that none of the iris-recognition systems commercially available at the time implemented any live-tissue verification technology. Like any pattern-recognition technology, live-tissue verifiers will have their own false-reject probability and will therefore further reduce the overall probability that a legitimate user is accepted by the sensor.[13]

III. Method description

A. Iris localization

Iris localization detects the inner and outer boundaries of the iris. Both the inner and outer iris boundaries can be approximately modeled as circles. The center of iris does not necessarily concentric with the center of pupil. Iris localization is important because correct iris region is needed to generate the templates for accurate matching. Five iris localization algorithms would be discussed in this section. They include Integro-differential operator, Hough transform, Discrete Circular Active Contour, Bisection method and Black hole search method. Eyelids and eyelashes may cover the iris region. Eyelids can be detected using texture segmentation and Daubechies wavelets method. The eyelashes detection algorithms consist of Gabor filter, variance of intensity and combination of both edge and region information. Iris may be captured in different size with varying imaging distance. Due to illumination variations, the radial size of the pupil may change accordingly. The resulting deformation of the iris texture will affect the performance of subsequent feature extraction and matching stages. Therefore, the iris region needs to be normalized to compensate for these variations. The normalized iris image has low contrast and non-uniform illumination caused by the light source position. The image needs to be enhanced to compensate for these factors. Local histogram analysis is applied to the normalized iris image to reduce the effect of non-uniform illumination and obtain well-distributed texture image [27]. Reflections regions are characterized by high intensity values close to 255. A simple thresholding operation can be used to remove the reflection noise [28].

B. Feature extraction

In this stage, texture analysis methods are used to extract the significant features from the normalized iris image. The extracted features will be encoded to generate a biometric template. 2D Gabor filters are used to extract iris features in both [29] and [30]. Gabor filter's impulse response is defined by a harmonic function multiplied by a Gaussian function. It provides optimum localization in both spatial and frequency domains. Each pattern is demodulated to extract its phase information using quadrature 2D Gabor wavelets. The phase information is quantized into four quadrants in the complex plane. Each quadrant is represented with two bits phase information. Therefore, each pixel in the normalized image is demodulated into two bits code in the template. The phase information is extracted because it provides the significant information within the image . It does not depend on extraneous factors, such as imaging contrast, illumination and camera gain . A Log Gabor filter which is Gaussian on a logarithmic scale is proposed by . It has strictly band pass filter to remove the DC components caused by background brightness . Wavelet transform decomposes the iris region into components with different resolutions. The commonly used wavelets are Daubechies, Biorthogonal, Haar and Mexican Hat wavelet. The advantage of wavelet transform over Fourier transform is that it has both space resolution and frequency resolution. The features are localized in both space and frequency domains with varying window sizes. A bank of wavelet filters is applied to the normalized iris region. Each filter is tuned for each resolution with each wavelet defined by scaling functions. The output of the filters is encoded to generate a compact biometric template. Laplacian of Gaussian filters are used to encode feature by decomposing the iris region. The filtered image is realized as a Laplacian pyramid. A cascade of Gaussian-like filters is applied to the image. The Laplacian pyramid is constructed with four levels to generate a compact biometric template. This approach compresses the data to obtain significant data. The compressed data can be stored and processed effectively. Key local variations are used to represent the characteristics of the iris . The normalized iris image is decomposed into a set of 1D intensity signals. Dyadic wavelet transform is applied to each signal. Local extrema of the wavelet transform results correspond to sharp intensity variations of the original signal. The local maximum and minimum points are encoded into a feature vector. The feature vector is converted to a binary template with the same size as the normalized iris image. Hilbert transform is used to extract significant information from iris texture. Analytic image is constructed by the original image and its Hilbert transform. It can be used to analyze the iris texture. Emergent frequency and instantaneous phase is computed from the analytic image. Emergent frequency is formed by three different dominant frequencies of the analytic image. Instantaneous phase is the arctangent function of the real and imaginary parts of the analytic image. Feature vector is encoded by thresholding the emergent frequency and the instantaneous phase. The advantage of this approach is computationally effective. The filtering is performed in the Fourier domain using pure real filters. Iris is coded based on differences of discrete cosine transform (DCT) coefficients of rectangular patches . The normalized image is divided into diagonal 8×12 patches. The average over width is windowed using a Hanning window to reduce the effects of noise. A similar Hanning window and DCT is applied to the patch along its length. The differences between the DCT coefficients of adjacent patches are obtained. A binary template is generated from the zero crossings of the differences between the DCT coefficients. This coding method has low complexity and good interclass separation. It is superior to other approaches in terms of both speed and accuracy.

C. Template matching

The templates generated from the feature extraction stage need a corresponding matching metric. The matching metric compares the similarity between the templates. A threshold is set to differentiate between intra-class and inter-class comparisons. Hamming distance is defined as the fractional measure of dissimilarity between two binary templates. A value of zero would represent a perfect match. The two templates that are completely independent would give a Hamming distance near to 0.5. A threshold is set to decide the two templates are from the same person or different persons. The fractional hamming distance is sum of the exclusive-OR between two templates over the total number of bits. Masking templates are used in the calculation to exclude the noise regions. Only those bits in the templates that correspond to '1' bit in the masking template will be used in the calculation. The advantage of Hamming distance is fast matching speed because the templates are in binary format. The execution time for exclusive-OR comparison of two templates is approximately 10s . Hamming distance is suitable for comparisons of millions of template in large database. Weighted Euclidean distance is used to compare two templates to identify an iris . The templates are composed of integer values. Weighted Euclidean Distance is defined as a measure of similarity between two templates. It is calculated using Pythagorean Theorem to obtain the distance between two points. An iris template is compared with all templates in the database. The two templates are matched if the Weighted Euclidean Distance is a minimum. Normalized correlation between two representations is calculated for goodness of match. It is defined as the normalized similarity of corresponding points in the iris region. The correlations are performed over small blocks of pixels in four different spatial frequency bands. Normalized correlation accounts for local variations in image intensity. However, normalized correlation method is not computationally effective because images are used for comparisons. Nearest feature line is an efficient classification method in template matching stage [6]. Feature line passes through any two feature points of the same class. The feature line extracts more variations of the feature vector than the feature points. The distance from a feature point to the feature line is calculated. The nearest feature line distance will be used in the classification stage.

IV. Preliminary Results and Conclusions

For at least a century, it has been suggested that the iris can subserve biometrically based recognition of human individuals. Recent efforts in machine vision have yielded automated systems that take strides toward realizing this potential. As currently instantiated, these systems are relatively compact and efficient and have shown promising performance in preliminary testing. Extant systems require a fair amount of operator participation and work at rather close range. Therefore, they are best suited to controlled assessment scenarios (e.g., portal entry and the like). The notion that the iris is a useful biometric for recognition stems largely from anecdotal clinical and indirect developmental evidence. This body of evidence suggests that the structure of individual irises is highly distinctive and stable with age. Empirical testing of documented irisrecognition systems provide additional support for these claims; however, these tests were limited in scope. An important direction for future efforts is the design and execution of controlled, large-scale, longitudinal studies. Only via reference to such studies can the true accuracy of iris recognition be determined for both the verification and identification tasks. Another potentially rich direction for future research would be to relax the constraints under which current iris-recognition systems operate. In this regard, it would be particularly desirable to decrease the required level of operator participation even while increasing the physical distance from which evaluation takes place. If such goals can be achieved, then iris recognition can provide the basis for truly noninvasive biometric assessment. Further, if these enhancements can be had while maintaining compact, efficient, and low-cost implementations, then iris recognition will be well positioned for widespread deployment.

V. Deployed applications

-United Arab Emirates IrisGuard's Homeland Security Border Control has been operating an expellee tracking system in the United Arab Emirates (UAE) since 2003, when the UAE launched a national border-crossing security initiative. Today, all of the UAE's land, air and sea ports of entry are equipped with systems. All foreign nationals who need a visit visa to enter the UAE are now processed through iris cameras installed at all primary and auxiliary immigration inspection points. To date, the system has apprehended over 330,000 persons re-entering the UAE with either another name or nationality (which needs a visa), or even fraudulent travel documents.[21]

-Bank United - Texas. In 1999 Bank United became the first bank in the world[22] to deploy iris recognition ATMs. These ATMs were manufactured by Diebold using Sensar iris recognition technology. The pilots deployed by Bank United received national television coverage. Coverage and interviews of Sensar executives and Bank United executives included Good Morning America, USA Today, and many other national television shows.

-Hashemite Kingdom of Jordan - 2009, IrisGuard deployed one of the world's first operational iris-enabled automated teller machine at Cairo Amman Bank, where bank customers can seamlessly withdraw cash from ATM's without a bank card or pin but simply by presenting their eye to the iris recognition camera on the ATM. Since June 2012, IrisGuard is also providing financial inclusion to UNHCR registered Syrian refugees in Jordan on ATM's. The system is designed to facilitate cash-supported interventions that help deliver financial assistance to refugees with speed and dignity while lowering overhead costs and boosting accountability.[23]

-Aadhaar began operation in 2011 in India, whose government is enrolling the iris patterns (and other biometrics) of more than one billion residents for the Aadhaar scheme for entitlements distribution, run by the Unique Identification Authority of India (UIDAI).[4] This programme at its peak was enrolling about one million persons every day, across 36,000 stations operated by 83 agencies. By October 2015, the number of persons enrolled exceeded 926 million, with each new enrollee being compared to all existing ones for deduplication checks (hence 926 trillion, i.e. 926 million-million, iris cross-comparisons per day).[24] Its purpose is to issue residents a biometrically provable unique entitlement number (Aadhaar) by which benefits may be claimed, and social inclusion enhanced; thus the slogan of UIDAI is: ”To give the poor an identity.” Iris technology providers must be granted a STQC (Standardisation Testing and Quality Certification) certificate in order to supply iris scanners for the project. By far, there are providers such as: IriTech Inc. (dual iris scanner IriMagic 100BK), Cogent (CIS-202), Iris ID (icam TD 100), Iris Guard (IG-AD-100), etc.[25]

-Police forces across America planned to start using BI2 Technologies' mobile MORIS (Mobile Offender Recognition and Information System) in 2012. The New York City Police Department was the first, with a system installed in Manhattan in the fall of 2010.[26]

References

[1] https://hmn.wiki/ro/Iris_recognition

[2] https://www.globenewswire.com/en/news-release/2022/11/03/2547633/0/en/Iris-Recognition-Market-Projected-to-Hit-USD-9-74-Billion-at-a-16-21-CAGR-by-2030-Report-by-Market-Research-Future-MRFR.html

[3] https://www.eff.org/ro/pages/iris-recognition

[4] J. P. Holmes, L. J. Wright, and R. L. Maxwell, “A performance evaluation of biometric identification devices,” Sandia National Laboratories, Albuquerque, NM, Tech. Rep. SAND91-0276, 1991.

[5] B. Miller, “Vital signs of identity,” IEEE Spectrum, vol. 31, pp. 22–30, Feb. 1994.

[6] R. Chellappa, C. L. Wilson, and S. Sirohey, “Human and machine recognition of faces: A survey,” Proc. IEEE, vol. 83, pp. 705–740, May 1995

[7] A. Samal and P. A. Iyengar, “Automatic recognition and analysis of human faces and facial expressions: A survey,” Pattern Recognit., vol. 25, pp. 65–77, 1992.

[8] F. H. Adler, Physiology of the Eye. St. Louis, MO: Mosby, 1965

[9] A. L. Kroeber, Anthropology. New York: Harcourt Brace Jovanovich, 1948.

[10] D. H. Ballard and C. M. Brown, Computer Vision. Englewood Cliffs, NJ: Prentice-Hall, 1982.

[11] P. Grother, J. Matey, E. Tabassi, G. Quinn, and M. Chumakov, IREX VI: temporal stability of iris recognition accuracy, NIST Interagency Report 7948, pp. 1–3, 2013

[12] Richard Yew Fatt Ng, Yong Haur Tay, Kai Ming Mok :2008 International Symposium on Information Technology

[13] https://en.wikipedia.org/wiki/Iris_recognition

[14] ”Hacker Finds a Simple Way to Fool IRIS Biometric Security Systems”. thehackernews.com. 6 March 2015. Retrieved 17 March 2017.

[15] Martin, Zach (23 March 2011). ”Biometric Trends: Will emerging modalities and mobile applications bring mass adoption?”. SecureIDNews. Retrieved 14 July 2013.

[16] Whittaker, Zack (29 September 2018). ”Princeton Identity debuts a new walkthrough biometric scanner”. TechCrunch. Retrieved 29 March 2019

[17] ”Iris scanners 'can be tricked'”. BBC News. 26 July 2012.

[18] R. Roizenblatt, P. Schor et al. Iris recognition as a biometric method after cataract surgery. Biomed Eng Online. 2004; 3: 2

[19] R.P. Wildes : Iris recognition: an emerging biometric technology

[20] Hashemi, Soheil; Tann, Hokchhay; Buttafuoco, Francesco; Reda, Sherief (March 2018). Approximate Computing for Biometric Security Systems: A Case Study on Iris Scanning. 2018 Design, Automation Test in Europe Conference Exhibition (DATE). IEEE

[21] ”European Business Review - Identification in the Twinkle of the Eye, Oct 7, 2008”

[22] ”Bank United Announces Results of First U.S. Iris Recognition ATM Consumer Survey”. www.atmmarketplace.com. 16 April 2002. Retrieved 5 June 2021.

[23] ”UNHCR Innovation — Biometric Cash Assistance”. innovation.unhcr.org. Retrieved 3 November 2016.

[24] ”Aadhaar - Unique Identification”. portal.uidai.gov.in. Archived from the original on 4 June 2017. Retrieved 2 November 2015.

[25] ”STQC Certificate granted suppliers” (PDF)

[26] ”Police to begin iPhone iris scans amid privacy concerns”. Reuters. 20 July 2011. Archived from the original on 18 September 2012. Retrieved 26 September 2012.

[27] Y. Zhu, T. Tan, and Y. Wang (2000). ”Biometric Personal Identification Based on Iris Patterns”, Proceedings of the 15 International Conference on Pattern Recognition, vol. 2, pp. 2801-2804.

[28] J. Huang, Y. Wang, T. Tan, and J. Cui (2004). ”A New Iris Segmentation Method for Recognition”, Proceedings of the 17 International Conference on Pattern Recognition.

[29] J. Daugman (1993). ”High Confidence Visual Recognition of Persons by a Test of Statistical Independence”, IEEE Tans. Pattern Analysis and Machine Intelligence, vol.15, pp.1148-1161.

[30] J. Daugman (2004). ”How iris recognition works”, IEEE Trans. CSVT, vol. 14, no. 1, pp. 21 - 30.