

*Help us provide free content to the world by **donating today!***

Iris recognition

From Wikipedia, the free encyclopedia

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irides of an individual's eyes.

Not to be confused with another less prevalent ocular-based technology, retina scanning, iris recognition uses camera technology, with subtle IR illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

Iris recognition efficacy is rarely impeded by glasses or contact lenses. Iris technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. The only biometric authentication technology designed for use in a one-to many search environment, a key advantage of iris recognition is its stability, or template longevity as, barring trauma, a single enrollment can last a lifetime.

Breakthrough work to create the iris recognition algorithms required for image acquisition and one-to-many matching was pioneered by John G. Daugman, Ph.D, OBE (University of Cambridge Computer Laboratory). These were utilized to effectively debut commercialization of the technology in conjunction with an early version of the IrisAccess system designed and manufactured by Korea's LG Electronics. Daugman's algorithms are the basis of almost all currently (as of 2006) commercially deployed iris-recognition systems. (In tests where the matching thresholds are – for better comparability – changed from their default settings to allow a false-accept rate in the region of 10^{-3} to 10^{-4} [1] (http://iris.nist.gov/ICE/ICE_2005_Results_30March2006.pdf) , the IrisCode false-reject rates are comparable to the most accurate single-finger fingerprint matchers [2] (<http://fpvte.nist.gov>) .)



Iris
The iris is the green/grey/brown area. The other structures visible are the pupil in the centre and the white sclera surrounding the iris. The overlying cornea is pictured, but not visible, as it is transparent.

Contents

- 1 Operating principle
- 2 Advantages
- 3 Disadvantages
- 4 Security considerations
- 5 Deployed applications
- 6 Iris recognition in fiction
- 7 See also
- 8 References
- 9 External links

Operating principle

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used resemble those of modern lossy compression algorithms for photographic images. In the case of Daugman's algorithms, a Gabor wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result are a set of complex numbers that carry local amplitude and phase information for the iris image. In Daugman's algorithms, all amplitude information is discarded, and the resulting 2048 bits that represent an iris consist only of the complex sign bits of the Gabor-domain representation of the iris image. Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination and virtually negligibly by iris color, which contributes significantly to the long-term stability of the biometric template. To authenticate via identification (one-to many template matching) or verification (one-to one template matching) a template created by imaging the iris, is compared to a stored value template in a database. If the Hamming distance is below the decision threshold, a positive identification has effectively been made.

A practical problem of iris recognition is that the iris is usually partially covered by eye lids and eyelashes. In order to reduce the false-reject risk in such cases, additional algorithms are needed to identify the locations of eye lids and eyelashes, and exclude the bits in the resulting code from the comparison operation.

A graphic, entitled "The Challenge of Rapid Iris Capture", illustrates the movement of the eyelids and eyelashes, as well as the contemporaneous



An IriScan model 2100 iris scanner

movements of the eyeball within the orbit (eye socket). See: http://www.biometricbits.com/Iris_Challenge.htm

Advantages

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

- It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.
- The iris is mostly flat and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae), which control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.
- The iris has a fine texture that – like fingerprints – is determined randomly during embryonic gestation. Even genetically identical individuals have completely independent iris textures, whereas DNA (genetic "fingerprinting") is not unique for the about 1.5% of the human population who have a genetically identical monozygotic twin.
- An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against finger-print scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).
- Some argue that a focused digital photograph with an iris diameter of about 200 pixels contains much more long-term stable information than a fingerprint.
- The originally commercially deployed iris recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 10^{-11}).
- 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.

Disadvantages

- Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.
- 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.
- As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates. [3] (http://www.biometricgroup.com/reports/public/reports/ITIRT_report.htm)
- 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.

Security considerations

Like with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of "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. Many commercially available iris recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. 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
- 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)
- Testing for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape
- Using 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features

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.

Deployed applications

- United Arab Emirates Homeland Security Border Control / IrisGuard Iris Expellee Tracking System® based on its Iris Farm Architecture® (IFA) has been operating in the United Arab Emirates (UAE) since 2001 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 IrisGuard systems. All foreign nationals who possess a visa to enter the UAE are processed through IrisGuard iris cameras installed at all primary and auxiliary immigration inspection points.

See <http://www.irisguard.com/> View: - IrisGuard TV Channel (<http://www.youtube.com/irisguard>)

- One of three biometric identification technologies internationally standardized by ICAO for use in future passports (the other two are fingerprint and face recognition)
- At Schiphol Airport, Netherlands, iris recognition has permitted passport free immigration since 2001
- UK's IRIS - Iris Recognition Immigration System (<http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris/>)
- Used to verify the recognition of the "Afghan Girl" (Sharbat Gula) by National Geographic photographer Steve McCurry. See <http://www.cl.cam.ac.uk/~jgd1000/afghan.html>
- In a number of US and Canadian airports, as part of the NEXUS program that facilitates entry into the US and Canada for pre-approved, low-risk travellers.
- In several Canadian airports, as part of the CANPASS Air (<http://www.cbsa-asfc.gc.ca/newsroom/factsheets/2005/0419-e.html>) program that facilitates entry into Canada for pre-approved, low-risk air travellers.



UAE Enrollment Station



A U.S. Marine Corps Sergeant uses an iris scanner to positively identify a member of the Baghdaddi city council prior to a meeting with local tribal figureheads, sheiks, community leaders and U.S. service members.

Iris recognition in fiction

- Demolition Man (1993) Character played by Wesley Snipes uses security guard's gouged eye to gain access through security door.
- In Dan Brown's 2000 novel Angels and Demons, an assassin gains access to a top secret CERN laboratory using a scientist's eye.
- Steven Spielberg's 2002 science fiction film Minority Report depicts a society in which what appears to be a form of iris recognition has become daily practice. The principal character undergoes an eye transplant in order to change his identity but continues to use his original eyes to gain access to restricted locations.
- The Simpsons Movie (2007) features a scene that illustrates the difficulty of image acquisition in iris recognition.[4] (<http://www.cl.cam.ac.uk/~jgd1000/simpsons.html>)
- Numbers features a scene where a robber gets into the CalSci facility by cracking the code assigned to a specific iris.
- NCIS uses an Iris scanner in the garage, where forensic vehicle investigations are carried out and evidence is stored. The sequence of Leroy Jethro Gibbs being verified is shown in the title sequence.

See also

- Iris Recognition Immigration System

References

- WO patent 8605018 (<http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=WO8605018>) Leonard Flom, Aran Safir: Iris recognition system. 28 August 1986; also: US patent 4641349 (<http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=US4641349>) issued 2/3/1987.
- US patent 5291560 (<http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=US5291560>) John Daugman: Biometric personal identification system based on iris analysis. 1 March 1994
- John Daugman: How iris recognition works (<http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf>) . IEEE Transactions on Circuits and Systems for Video Technology 14(1), January 2004, pp 21–30
- John Daugman: The importance of being random: statistical principles of iris recognition (<http://www.cl.cam.ac.uk/~jgd1000/patrec.pdf>) . Pattern recognition 36, 2003, pp 279–291.
- John Daugman: Results from 200 billion iris cross-comparisons (<http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-635.html>) . Technical Report UCAM-CL-TR-635, University of Cambridge Computer Laboratory, June 2005.

External links

- Home page of IrisCode designer John Daugman (<http://www.cl.cam.ac.uk/users/jgd1000>)

- Interview with John Daugman (http://www.findbiometrics.com/Pages/feature_daugman_camuk.htm)
- NIST Iris Challenge Evaluation (<http://iris.nist.gov/ice/>) – a contest for competing iris-recognition algorithms
- Iris recognition test results, analysis (<http://www.biometricgroup.com/reports/public/ITIRT.html>)
- Iris recognition algorithm reidentifies Sharbat Gula – Afghan National Geographic cover girl in 1985 – two decades later (<http://magma.nationalgeographic.com/ngm/afghangirl/>)
- Jan Ernst's iris recognition page (<http://www.iris-recognition.org>)
- Bath University Iris Image Database (<http://www.bath.ac.uk/elec-eng/research/sipg/irisweb/index.htm>)
- John G. Daugman's original patent application (<http://google.com/patents?id=KRkpAAAAEBAJ>) at Google Patents
- World largest current deployment (<http://www.cl.cam.ac.uk/~jgd1000/deployments.html>)
- Iris recognition in Poland (http://www.biometriclabs.pl/index.php?option=com_content&task=view&id=47&Itemid=104&lang=en_US)
- Iris On the Move - Sarnoff Corporation (<http://www.sarnoff.com/products/iris-on-the-move>)

Retrieved from "http://en.wikipedia.org/wiki/Iris_recognition"

Categories: Applications of computer vision | Biometrics

- This page was last modified on 6 August 2008, at 14:43.
- All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)
Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.