COVERT IRIS RECOGNITION: BALANCE BETWEEN ETHICS & INNOVATION

Abraham Garcia

Abstract:

This paper introduces IR and IAAD systems, explaining their operation and types, evaluating their impacts on privacy, security, and regulation, and concluding with future considerations.

Key Words: Iris Recognition (IR), Iris-Recognition-at-a-Distance (IAAD), Privacy, Regulatory Challenges, Security

Introduction

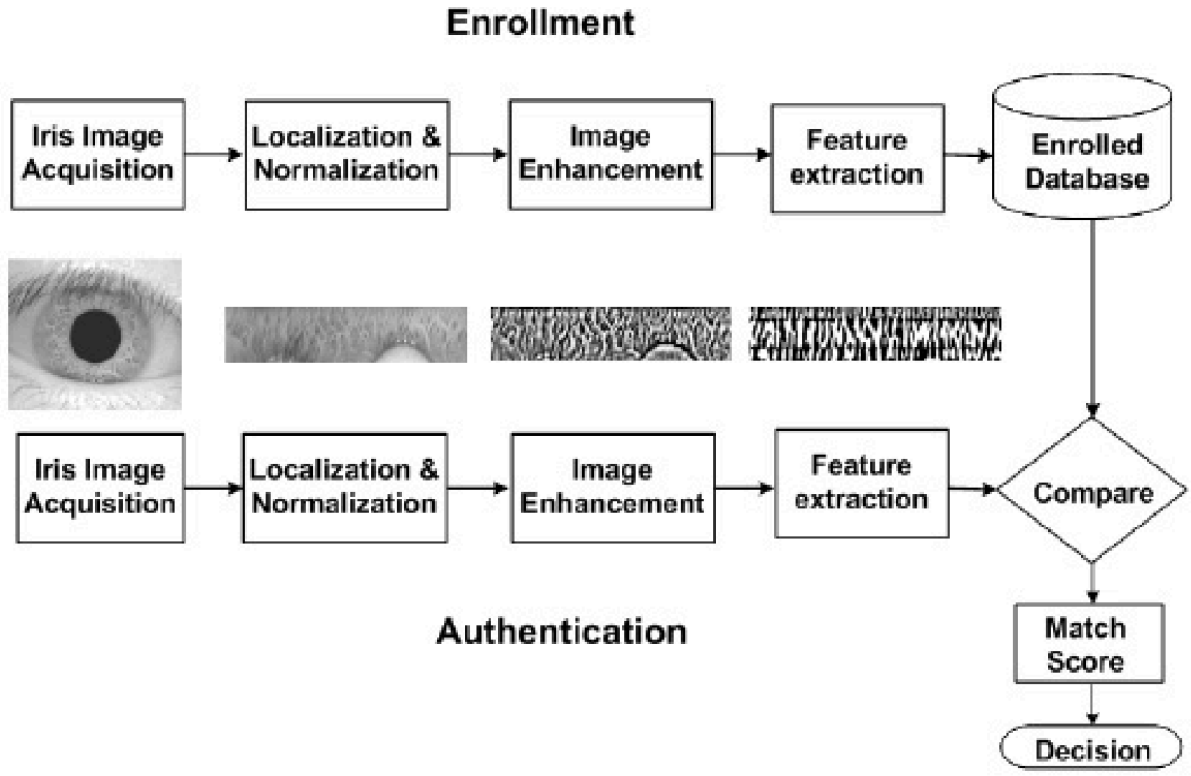
Iris Recognition (IR) is one of the most accurate and reliable biometric methods used to identify individuals due to the iris's unique and complex epigenetic pattern, with over 100 distinctive points, more than fingerprints[6]. The iris is a stable, highly visible, and protected organ, and IR systems can detect and extract encoded information with high accuracy, even if the user wears glasses or contact lenses. Current IR systems typically operate at distances of 3-10 meters using Near Infrared (NIR) wavelengths to read the iris pattern[3].

Increasing interest from government agencies, surveillance, and service industries demands more covert iris recognition (IR) systems, leading to the development of iris-recognition-at-a-distance (IAAD) systems[4]. These systems, designed to operate from greater distances with minimal user cooperation, have advanced to capture moving subjects, accommodate varied heights, and function up to 30 meters away using NIR wavelengths with high accuracy[5].

Despite these advancements, covert IAAD systems remain largely experimental, often requiring some user cooperation, such as directly facing sensors. The most covert systems involve manipulating environments to align subjects' irises with sensors unknowingly. The implementation of IAAD systems raises privacy concerns, security risks, and regulatory challenges[7]. Questions about data necessity, storage, and disposal, alongside the irreversible nature of iris data, highlight significant risks if data is misused. Current regulatory bodies are only now addressing the issue and still have much room for improvement.

How IR Systems Work

The IR process involves two main parts: enrollment and verification. During enrollment, an image of the user's iris is captured, localized, normalized, enhanced, and its features are extracted and encoded into a database. During verification, the system captures the user's iris image again, processes it similarly, and compares it with the database to decide if the user is genuine, using a match score based on the Hamming Distance between iris patterns. Feature extraction is performed using Quadrature 2D Gabor Wavelets[6] to capture local phasor data, and angles are quantized into one of four 2-bit sets. Iris normalization is crucial, especially at increased distances, and is achieved by "unwrapping" the segmented iris using Daugman's algorithm[6].



Dr. S. Latifi

Figure 1. IR Enrollment and Authentication Flow Chart [7]

IR Challenges

Several factors can impact iris image quality, such as occlusion, defocus, motion blur, and nonuniform illumination, which become more significant as the distance and covert nature of iris acquisition increase[6]. Iris segmentation is challenging due to the irregular texture and shape of the iris, which can be partially blocked by eyelashes. This is mitigated by the contrast between the iris and the pupil and sclera, with boundaries approximated using circles.

IR Systems Evolution

Advancements in IR have addressed factors like height differences among public users by incorporating pan-tilt units (PTUs) and wide-angle lenses[5]. The development of iris-recognition-at-a-distance (IAAD) systems aims to reduce user cooperation and increase the covert nature of IR systems. For instance, systems developed by CASIA can follow moving subjects, while those by Fancourt require users to face the camera directly. Covert IR systems for public applications need to operate at a distance, leaving users less aware of the IR system. IAAD systems like those developed by Fancourt function at ranges of 5-10 meters[4]. IOM systems, such as Sarnoff, track moving irises using multiple high-resolution cameras and powerful LED flashing NIR, applicable in airports, stadiums, and border crossings, though they suffer from low-quality iris capture[2].

To achieve near-complete covert IR, a network of several computers across a

Category	Camera	Distance	Motion	User	Example systems	Applications
Close-range IR	Passive	Close-range	Static	Single	BM-ET330 (Panasonic) [7], IrisAssess 4000 (LG) [8], CASIA-IrisCamV1	Access control, Time & Attendance, Banking, Personal security, etc.
Active IR	Active	Close-range	Static	Single	IRISPASS-M (OKI) [9], CASIA-IrisCamV2 [12]	
IR at a distance	Passive	Long-range	Static	Single	Iris at a Distance (Sarnoff) [10],	Pre- research for IR on move
Active IR at a distance	Active	Long-range	Static	Single	Mitsubishi [11], CASIA-IrisCamV3	
Passive IR on move	Passive	Long-range	Movement to an access control point	Single	Iris on Move (Sarnoff) [13]	Border-crossing, Airport, Stadium, Park, Hall, etc.
Active IR on move	Active	Long-range	Movement to an access control point	Single		
IR for Surveillance	Active	Long-range	Free movement	Multiple		Covert personal identification, Security surveillance, Watch-list, Homeland security, etc.

Table 1. IR systems [4]

wide area targeting the same space is required, often incorporating other biometric measures to improve accuracy. Despite advancements, the implementation of IAAD systems raises privacy concerns, potential for discriminatory practices, security risks, and regulatory challenges[4]. Current frameworks are inadequate to address these issues, especially given the irreversible nature of iris data. This paper introduces IR and IAAD systems, explains their operation and types, evaluates their impacts on privacy, security, and regulation, and concludes with considerations for the future of these technologies.

IR vs IAAD

The main difference between traditional iris recognition (IR) and iris-recognition-at-a-distance (IAAD) systems lies in their methodologies and the level of user cooperation required. Traditional IR systems offer high accuracy with less advanced technology, requiring a high-quality camera and significant user cooperation, as users must be stationary and close to the IR camera (1-3 meters)[1].

In contrast, IAAD systems function at distances ranging from 1 to 60 meters with minimal user cooperation. They can capture moving users using the IOM feature developed by Sarnoff, giving the user free movement while working covertly. However, IAAD systems require higher quality cameras and generally have a lower accuracy rate due to most datasets being imperfect from blurry images to subject movement and varying lighting conditions, increasing algorithm complexity. To improve accuracy, advanced IAAD systems use multiple cameras with different focal lengths, significantly raising costs and complexity[4].

Despite the higher costs and technical complexities, IAAD systems are preferable and more beneficial than traditional IR systems for covert biometric acquisition due to their ability to function over greater distances with minimal user cooperation.

Privacy and Security

A significant privacy concern with IR systems is the potential for spoofing attacks, where fake eyes or contact lenses trick the system into recognizing a false iris. To counteract this, liveness detection tests have been developed to determine if an iris is from a genuine user. One such approach, proposed in 2008 by Zhenan Sun, Wenbo Dong, and Tieniu Tan from the Chinese

Academy of Sciences, aims to detect when a user is wearing contact lenses. Their method achieved a 95% correct classification rate, including 640 fake iris images[4].

Despite these advancements, there have been notable instances where current liveness detection methods were insufficient. For example, the German hacker group Chaos Computer Club successfully tricked the Samsung Galaxy S8 iris scanner using an artificial eye. Engling, the spokesperson for the club, remarked, “The security risk to the user from iris recognition is even bigger than with fingerprints, as we expose our irises a lot,”[11]. This incident highlights how high-resolution pictures can capture irises and trick some IR systems, exposing users to significant security risks.

Further demonstrating these vulnerabilities, Javier Galbally's research team from Universidad Autónoma de Madrid and West Virginia University reverse-engineered a "replicated" eye from real iris codes stored in security databases. Their eyes bypassed leading commercial IR systems 80% of the time[12]. They exploited the fact that most IR systems only look for the iris code and not an actual eye. By using the binary iris code, they reconstructed an image of the original iris. This demonstrates that if an IR system's database is compromised, attackers can reconstruct clients' eyes using a genetic algorithm and print the image onto a contact lens to access protected information.

While Zhenan Sun's research group tackles concerns related to contact lenses and liveness detection, many more presentation attacks still threaten IR systems. Assistant professor Adam Czajka of Notre Dame's Department of Computer Science and Engineering notes, "If you have something that is accurate and fast, then, of course, it is exposed more to attacks." In collaboration with Domingo Mery from Universidad Católica de Chile, Czajka developed an algorithm originally used for facial recognition to detect more biometric attacks[8]. Despite its accuracy and speed, iris recognition's exposure to attacks increases its risk profile, underscoring the importance of robust countermeasures and international collaborations to enhance the technology's security.

As the market for covert IAAD systems increases, the risk of attackers capturing our irises without our knowledge also rises, leading to severe privacy violations[8]. This technology enables attackers to bypass traditional IR system defenses by capturing an iris directly from the user without their consent. With covert IAADs, attackers no longer need access to a secured database. They can create their own templates by covertly capturing the target's iris, significantly increasing the risk of unauthorized access to sensitive information. Although the probability of such attacks is currently low, the possibility that our most personal data can be leaked without our knowledge or consent leaves the public deeply concerned.

Regulatory Policy

IR and other biometric systems have been in place since the 90s, and only recently, about 30 years later, have governments laid out basic policy guidelines on biometric use and data collection. These policies are often barebone, raising concerns about how long it will take governmental regulators to address future developments in biometric systems and their potential risks to public security and privacy. The use of covert IAADs exacerbates these concerns, as their inherent goal of operating with little to

no client consent increases the likelihood of such attacks on the public.

The Federal Trade Commission (FTC) has warned companies against illegally selling and collecting consumer data. A primary concern is the sale of biometric data to advertisement companies, which could use personal information to sell products aggressively, or to insurance companies to raise rates based on medical conditions[13]. The FTC also monitors third parties' marketing practices related to this data. As FTC Regional Director Chuck Harwood states, "What the policymakers are trying to do right now is simply ensure that we all know what data is being collected," highlighting their effort but also how much further the FTC has to go[13]. Currently, they are still trying to gather all the data around them.

Despite these challenges, the FTC has made some strides in protecting consumers' biometric data, requiring “affirmative express consent” and punishing companies for failing to fulfill their privacy promises[10]. The FTC demonstrated their commitment to biometric data security when they protected video and audio recordings taken from families' homes using Alexa and Ring. In another case, a company named Vitagene stored genetic data with identifying information and did not ensure third-party labs destroyed genetic samples. This led to large financial settlements for Vitagene and CRI Genetics, along with mandates for data destruction, prohibitions on misrepresentations, consumer notices, affirmative consent for data use, and security programs with independent assessments.

In August 2020, Senators Bernie Sanders and Jeff Merkley introduced the National Biometric Information Privacy Act, mirroring Illinois’s BIPA law[14]. It mandates consent for biometric data collection, allows private legal action for violations, and requires data protection akin to Social Security Numbers. The bill proposes $1,000 statutory damages per violation, mandates data retention policies, and limits retention to one year post-consumer interaction. It also includes a "right to know" provision for consumers and mandates written consent before biometric data disclosure[14].

Despite being read twice in the Senate and referred to the Judiciary Committee with no further action has been taken. Privacy advocates urge swift Committee action, emphasizing the need for federal regulation over the current patchwork state-by-state approach, which lacks efficiency and consistency in regulating multinational corporations.

In Canada, biometric data collection, use, and disclosure fall under the jurisdiction of the Privacy Act for federal government use and the Personal Information Protection and Electronic Documents Act (PIPEDA) for private sector companies[9]. The Office of the Privacy Commissioner of Canada is increasingly focusing on the privacy challenges posed by biometric systems. One significant concern is the covert collection and use of biometric data. Such as the IAAD and IR systems. Similarly, palm, facial, and finger vein patterns can be captured covertly when people pass over hidden recording devices.

Cross-matching or function creep is another privacy issue, where a biometric trait collected for one purpose is used without a person’s knowledge and consent for a different purpose. Additionally, secondary information found in biometric characteristics, such as health information

from iris images, can be used against vulnerable members of society. This practice violates the right to health privacy as companies seek to extract as much value from our data as possible[14].

To address these concerns, the Office of the Privacy Commissioner of Canada advocates for proactive privacy measures. Privacy Impact Assessments (PIAs) are mandatory for federal institutions proposing programs with privacy implications[9]. These assessments help identify and mitigate privacy risks at the start. To ensure companies comply with privacy laws, the Office of the Privacy Commissioner of Canada conducts privacy audits and investigations[9].

The Office of the Victorian Information Commissioner in Australia has issued comprehensive guidelines for public and private organizations collecting biometric data, stressing the need to prioritize privacy[8]. The regulatory body encourages these organizations to collect biometric data only when necessary and ensure its use is fair and non-intrusive. For those unable or unwilling to participate in biometric systems, alternatives should be provided. Clear communication about data collection, disclosure, and use is key to build trust and comply with the guideline, ensuring informed consent and mitigating privacy risks.

The office suggests that these organizations conduct privacy impact assessments (PIAs) to identify and address potential privacy risks early in the process[8]. Additionally, having a transparent complaint system, accountability protocols, and a robust governance framework is essential to maintaining privacy standards. Assigning a senior officer within the organization to oversee and manage privacy concerns is also recommended. The office further advises adopting best practices and guidelines from organizations like the Biometric Institute.

The Privacy and Data Protection Act (PDP Act) and the Information Privacy Principles (IPPs) in Australia, which regulate the use and storage of biometric information, are additional tools that regulators in Australia have[8]. According to IPP 1, biometric data should be collected only if necessary to fulfill an organization’s functions and should be fair and not unreasonably intrusive. IPP 2 limits the use and disclosure of biometric data to avoid function creep and restricts it to the primary purpose for which it was collected. IPP 4 emphasizes the need for secure storage of biometric data and mandates its destruction once it is no longer needed for any purpose, which can be refined to ensure data is destroyed once it is no longer used for the specific and explicit purpose it was initially collected for. These guidelines and principles ensure that the implementation and use of biometric systems, including IR and IAAD systems, protect citizens' privacy and security.

Conclusion

IR and IAAD systems, while advancing biometric identification, exacerbate privacy and security concerns. IAAD systems, especially those operating covertly without explicit consent, risk unauthorized biometric data capture and potential identity theft and fraud through spoofing attacks on IR systems. Instances such as using high-resolution cameras to capture a person's iris code to unlock a Samsung Galaxy S8 phone validates the general public's fears. With the market for covert IAADs expanding, the potential for

unauthorized access poses a direct threat to individuals' privacy and personal security.

Governments worldwide are attempting to respond with legislative efforts. In Australia, frameworks like the Privacy and Data Protection Act (PDP Act) and Information Privacy Principles (IPPs) provide guidelines for the lawful use and secure storage of biometric information, emphasizing informed consent and secure practices. However, regulating the covert nature of IAADs remains challenging, undermining privacy protections and exposing individuals to heightened risks.

Additionally, the US Congress's failure to pass the National Biometric Information Privacy Act highlights the difficulty in establishing comprehensive national regulations that effectively address the complexities of biometric technologies and their impacts on privacy and security.

References

[1] K. Nguyen, C. Fookes, R. Jillela, S. Sridharan, and A. Ross, "Long range iris recognition: A survey," *Pattern Recognition*, vol. 72, pp. 123–143, Dec. 2017, doi: https://doi.org/10.1016/j.patcog.2017.05.021.

[2] Barry Fox, "Invention: Covert iris scanner," *New Scientist*. https://www.newscientist.com/article/dn11110-invention-covert-iris-scanner/ (accessed Jun. 14, 2024).

[3] K. Bylappa Raja, "Robust Iris Recognition Using Light-field Camera," Master Erasmus Mundus in Color in Informatics and Media Technology (CIMET), 2013. Accessed: Jun. 14, 2024. [Online]. Available: https://www.ntnu.edu/documents/1268217450/0/Master_Thesis_KiranRaja_Compressed.pdf/b6545cdd-ec58-0f7c-43aa-1283df2ba647?t=1707297293375

[4] Z. Sun, W. Dong, and T. Tan, "Technology Roadmap for Smart Iris Recognition ," Center for Biometrics and Security Research & National Laboratory of Pattern Recognition Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, Beijing, 100190, P.R. China, 2008. Accessed: Jun. 14, 2024. [Online]. Available: https://nlpr.ia.ac.cn/2008papers/gjhy/gh108.pdf

[5] W. Dong, Z. Sun, and T. Tan, "A design of iris recognition system at a distance," Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, 2009. Accessed: Jun. 14, 2024. [Online]. Available: https://nlpr.ia.ac.cn/2009papers/gjhy/gh99.pdf

[6] Lecture 6. Iris Recognition, Biometrics Course, UNLV, Summer 2024.

[7] M. C. W. | U. of N. Dame, "Biometric security: Defending against attacks in iris recognition | Notre Dame Global | University of Notre Dame," *Notre Dame Global*, Aug. 04, 2021. https://global.nd.edu/news-stories/news/biometric-security-defending-against-attacks-in-iris-recognition/#:~:text=Author:%20Abby%20Urban (accessed Jul. 07, 2024).

[8] "Biometrics and Privacy – Issues and Challenges," Office of the Victorian Information Commissioner https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/#consent (accessed Jul. 07, 2024).

[9] O. of the P. C. of Canada, "Data at Your Fingertips Biometrics and the Challenges to Privacy," *www.priv.gc.ca*, Nov. 01, 2011. https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/

[10] E. Jillson, "The DNA of privacy and the privacy of DNA," *Federal Trade Commission*, Jan. 05, 2024. https://www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna (accessed Jul. 07, 2024).

[11] A. Hern, "Samsung Galaxy S8 iris scanner fooled by German hackers," *the Guardian*, May 24, 2017. https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security

[12] "Black Hat presentation shows iris-scanning breach," *phys.org*. https://phys.org/news/2012-07-black-hat-iris-scanning-breach.html

[13] "Jesse Jones: FTC cracking down on companies who collect biometric data," *KIRO 7 News Seattle*, Jul. 06, 2023. https://www.kiro7.com/news/jesse-jones/jesse-jones-ftc-cracking-down-companies-who-collect-biometric-data/7UWXV32RPNCSHGAYD3P2CU6MUE/ (accessed Jul. 11, 2024).

[14] I. Ducey, "Issue 2 Issue 2 Harvest Biometric Data," *Seattle Journal of Technology, Environmental & Innovation Law Seattle Journal of Technology, Environmental & Innovation Law*, vol. 12, no. 2, Available: https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1036&context=sjteil

Here's an improved version of your feedback:

The overall format and organization of your paper are satisfactory. However, I suggest some refinements:

1.

In the abstract, consider moving everything prior to "This paper introduces..." to the introduction section. The abstract should succinctly outline what the paper covers: your methodology, key findings, and conclusions. A glance at archived papers will provide a clearer template.
2.

Differentiate between regular (IR) and (IAAD) more explicitly. How do their methodologies diverge? Unlike IR, IAAD achieves its objectives without extensive user cooperation. Explore the performance of IAAD, acknowledging potential limitations due to handling imperfect data compared to overt IR. Include your findings in this comparison.

Your progress is satisfactory.
Dr. Latifi

1. I moved everything prior to “This paper introduces …” to the introduction section.
2. I have added a section that explicitly focuses on the differences between IR and IAAD systems and how their methodologies diverge. The section labeled 'IR vs IAAD' should hopefully sufficiently address these concerns. Also, I explored the performance and limitations of IAAD systems in comparison to overt IR systems in the sections 'IR Systems Evolution' and 'IR vs IAAD'.
3. The incremental work I have done since the midterm highlights concerns regarding privacy and security associated with biometric data collection and use. I emphasized how IAAD systems operating covertly exacerbate these risks, supported by examples of these concerns materializing. Additionally, I added a section focusing on governmental actions and failures in regulating these systems, and discussed how IAAD systems operating covertly will challenge current regulations.