NIST Technical Note TN 2018

Iris Cameras: Standards Relevant for Camera Selection - 2018

James R. Matey
George W. Quinn
Patrick Grother
Craig Watson
Shahram Orandi

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2018

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Technical Note TN 2018

Iris Cameras: Standards Relevant for Camera Selection - 2018

James R. Matey
George W. Quinn
Patrick Grother
Craig Watson
Shahram Orandi
{james.matey, george.w.quinn, patrick.grother, craig.watson, shahram.orandi}@nist.gov
Information Technology Laboratory, Information Access Division, Image Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2018

September 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Technical Note TN 2018
Natl. Inst. Stand. Technol. Tech. Note TN 2018, 8 pages (September 2018)
CODEN: NTNOEF

This publication is available free of charge from:
https://doi.org/10.6028/NIST.TN.2018

Key words

camera; compatibility; image acquisition; iris recognition; iris recognition standards; interoperability.

Table of Contents

1. Introduction

Iris recognition has been and is being adopted for a variety of government applications, including law enforcement.

The adoption of iris recognition in government applications faces many of the issues that arose during the adoption of live scan fingerprint collection, including setting standards for collection devices. Appendix F for fingerprints[1] and the standards on which it is based were developed to ensure that fingerprint collection systems are inter-operable across government entities – that a fingerprint collected by one government agency can be compared with one collected by another. The Certified Products List[2] for fingerprint scanners was created to enable end users to know whether specific products were Appendix F compliant.

To enable a consistent process for iris camera selection by disparate government agencies, it would be useful to have the iris camera equivalent of (1) Appendix F and (2) the corresponding Certified Products list. At the present time (2018), an "Appendix F" for iris cameras does not exist, nor does a process for generating a Certified Products List for iris cameras, though this is a topic for discussion within the Iris Experts Group (IEG)[3].

Developing an "Appendix F" for iris cameras is generally recognized to be more difficult than it was for flatbed fingerprint scanners because (1) the eye/iris is a more complicated structure than the friction ridges on our fingertips; (2) in flatbed fingerprint scanners the finger is pressed against a fixed flat platen – a constraint that enables a two-dimensional, contact capture; in iris capture the three-dimensional eye/iris is not so constrained. The capture issues for iris are similar to those for contactless fingerprint as discussed in NIST Special Publication 500-305, Guidance for Evaluating Contactless Fingerprint Acquisition Devices [1]. We note that development of an "Appendix F" for contactless fingerprint devices remains an ongoing effort.

The primary focus of this paper is the review of standards and processes for iris cameras that enable interchange of data between government entities, as permitted by regulation and policy, and that enable cost-effective improvements as technology advances. We summarize the status of standards relevant for iris camera selection in scenarios where interoperability is important and provide interim guidance to those who need to understand the factors involved in iris camera selection. This paper is also intended to foster discussion between stakeholders in the law enforcement community, the standards community, and the iris camera vendor/manufacturer community and contribute to the ongoing discussion

[1] Appendix F is a specification of image quality for fingerprint scanners. Details may be found at https://www.fbibiospecs.cjis.gov/Certifications/FAQ.

[2] https://www.fbibiospecs.cjis.gov/certifications

[3] The IEG meetings are currently hosted and organized by NIST. Additional details and a history of the group can be found at https://www.nist.gov/programs-projects/iris-experts-group-ii-homepage.

that began at the last IEG meeting (June 2018).

Comments and recommendations about this paper may be directed to james.matey@nist.gov.

2. Need for Interoperability in Biometric Recognition Systems

There are cases in which the nature of a biometric recognition application does not require interoperability. The most common case may be using a fingerprint to unlock a cell phone. In this case the fingerprint image never leaves its associated cell phone and it is only compared with other images collected on that cell phone. The cell phone does not need Appendix F certification to fulfill its purpose. Indeed, from the standpoint of personal privacy, the lack of interoperability might be considered a feature rather than a bug.

In contrast, for systems where an identity first established at one location needs to be determined/verified at another location, interoperability is crucial. If we could not compare fingerprint images from booking station A with those from booking station B, most of the utility of a fingerprint database would be lost.

3. Relevant Standards for Iris Camera Interoperability

The most important considerations in the selection of iris cameras use revolve around standards:

- Conformance to standards that ensure compatibility/interoperability with other biometric recognition systems.
- Retention of imagery in standard formats to enable future system improvements.

These sorts of considerations are not unique to iris cameras – they apply in one form or another to many purchases in the law enforcement communities and even in our private lives.

Building on earlier comments, fingerprint systems that conform to standards enable queries against fingerprint databases built/purchased by other agencies. Use of closed, non-standardized, proprietary[4] fingerprint acquisition systems would make it difficult to coordinate efforts between local, state, national and international agencies.

[4]In the sense of features that make it incompatible with competing items; see http://www.businessdictionary.com/definition/proprietary.html and https://www.merriam-webster.com/dictionary/proprietary.

The same is true for iris recognition. The relevant standards/specifications for interoperability of iris cameras are listed in table 1. To ensure compatibility/interoperability across government uses/entities, *any* iris camera purchased for *any* government use should conform to those standards. Of particular note at the system level is conformance to the data transmission standards in ISO/IEC 19794-6:2011 [2], ANSI/NIST-ITL 1-2011:2015 [3], and EBTS [4] – especially the type 17 iris image record that can be ingested by national databases. Of particular note at the device level are the Iris Acquisition Quality metrics described in Section 7 of ISO/IEC 29794-6, which we can briefly summarize as the near infrared (NIR) wavelengths at which images are captured, the resolution and related modulation transfer function of the camera (resolvable pixels across the iris), and the camera signal-to-noise ratio.

To enable interoperability with other iris recognition algorithms and technology, the imagery collected by such cameras should be capable of retention (subject to policy constraints) in standard, *lossless* image formats [5], e.g., lossless versions of PNG, BMP, JPEG2000, so that future improvements in iris recognition technology can be adopted[5] *without* re-collection of all previously collected imagery – a daunting and likely impossible task in most circumstances.

To enable interoperability with other iris recognition algorithms and technology, the imagery collected by such cameras and any software system associated with the cameras should be under the control and ownership of the government agency with the authority and responsibility for its collection and should not require the permission or intervention of the vendor for its use in systems/applications not provided by the vendor[6]. As one example, it is easy to imagine advances in technology by a third-party that would enable more efficient investigation of cold case files – provided that the technology can be employed on the imagery. Lack of control and ownership would likely hinder utilization of such advances.

In any selection decision for biometric capture hardware, it is important to note that the initial data capture device cost is a small part of the overall cost of capturing the biometric data. The primary cost drivers for data capture are operational: the labor involved in working with subjects and capturing and entering biographical information and case history can easily dominate the long-term costs[7]. The image database that results from such

[5]Image retention will not guarantee that all future improvements can be adopted, e.g. a future method could rely on higher resolution or wider field of view than is available with current cameras. However, lack of image retention does guarantee that re-enrollment of subjects *will NOT* be possible without the subject present.

[6]Image ownership and control will not guarantee that all future improvements can be adopted. As noted earlier, an alternate algorithm could rely on higher resolution or wider field of view than was collected. However, lack of image ownership and control does guarantee that re-enrollment of subjects *will NOT* be possible without the subject present – unless the owner agrees.

[7]For example, http://ward43.org/wp-content/uploads/2015/09/Cost-per-Police-Officer_vF.pdf estimates the average fully loaded cost of a Chicago police officer at $150,000 /year or about $75/hour. If a booking takes 30 minutes of an officer's time, the labor cost for the officer is $37.50 /booking. If the capture device cost is

operation grows in size over time and becomes steadily more valuable as a result of that growth; the government entity needs to retain ownership and control of that increasingly valuable resource. As such, they should be careful to not get locked into solutions that make it difficult or impossible to engage with other sources for newer, better or less expensive technology in the future.

In short, any government procurement of iris cameras and associated software should require:

- Conformance to the standards in table 1 for both image quality and image transmission (e.g., type 17 records).
- Ownership and control of all collected imagery by the government agency with the authority for its collection.

4. Determining Conformance

There are third-party conformance tools and services for the data interchange standards: ISO/IEC 19794-6, ANSI-NIST 1-2011, and EBTS:

- The NIST/ITL Computer Security Division (CSD) Biometric Conformance Test Software (BioCTS) project[8] provides tools that can be used to test software for conformance to various biometric data format standards including select record types of ANSI/NIST-ITL 1-2011, particularly the Type 17 iris image record.
- At this writing we know of one US-based testing organization that is accredited through NIST's National Voluntary Laboratory Accreditation Program (NVLAP)[9] for conformance testing to the interchange standards discussed here. Such organizations could provide an alternative to self-test conformance statements by vendors testing using the tools noted above. Other testing organizations may become accredited; readers should consult the NVLAP website for details.

At present (2018) there are no widely available third-party conformance tools and services for the image quality standard, ISO/IEC 29794-6. Vendors use the measurement processes defined in the standard to evaluate their products and should document conformance of their products to the standard. The Independent Device Qualification Test (IDQT)

$2000, the labor cost exceeds the device cost after about 53 bookings. At one booking per week that would approximate a year's worth of bookings.

[8] NIST/Information Technology Laboratory Computer Security Division, https://www.nist.gov/itl/csd/biometrics/biometric-conformance-test-software-biocts

[9] https://nist.gov/nvlap

development effort [10] was an attempt at developing a third-party conformance process for ISO/IEC 29794-6. It has been dormant since 2013. As noted above, discussion at the June 2018 Iris Expert's Group meeting showed continuing interest in an IDQT-like process on the part of vendors and end users. NIST is working with stakeholders to foster further discussion on this topic. Interested parties can inquire at ieg-ii@nist.gov.

5. Issues Not Yet Fully Addressed by Standards

There are issues of importance for iris camera selection that are currently not addressed by standards or best practices. In the absence of formal standards for the following issues, deployment-specific consideration should be paid to the following operational issues. We note that other issues, not listed below, were discussed at the IEG meeting and will be considered in the further discussions mentioned above.

5.1 Capture Sequence and Cardinality Issues: Dual-Eye vs. Single-Eye Capture

Iris cameras may be designed to capture images of a single eye or both eyes at one time. Capturing images of the left and right eye separately can introduce transposition/labeling errors where the left eye may be incorrectly labeled as the right eye and vice versa. Keeping transposition errors out of the system can result in a two-fold improvement in response time or a two-fold decrease in the amount of hardware required to support a given response time.

In addition, dual-eye cameras can estimate subject head roll angle. Head roll adversely affects false non-match rates and is mitigated in matching algorithms by searching over a range of possible head roll angle. A good estimate of head roll can enable optimizations that can improve matching accuracy and speed. The optimizations can result in improved response time or a decrease in the amount of hardware required to support a given response time.

Since dual-eye iris cameras can reduce labeling errors and help optimize matcher performance through subject head roll angle measurement, dual-eye cameras should be given preference.

5.2 Ambient Lighting: Sunlight and Other Bright Illumination

Iris cameras can have difficulty coping with bright ambient illumination, in particular strong sunlight. Bright ambient illumination can cause excessive pupil constriction, poor

[10] See https://www.nist.gov/itl/iad/image-group/iris-device-qualification-test-idqt.

image contrast, and reflections of the ambient surroundings from the cornea that can lead to poor quality images. See NIST IREX V materials, Guidance for Iris Image Collection [6] for examples. Bright ambient lighting can be mitigated by utilizing cameras (e.g., binocular cameras) that provide physical shielding of the head or eyes.

5.3 Training

Capturing iris images is about as difficult as taking conventional photos, and is susceptible to similar errors. Such errors can result in low-quality images that may not be usable for iris recognition. Inclusion of such images into databases can result in poor matching performance.

Operators should be trained in the use of iris cameras to avoid the sorts of errors that are common in regular photography such as occluding the lens, improper focus, strong back lighting, and poor framing as well as iris camera specific errors. The NIST IREX V materials, Guidance for Iris Image Collection [6] provide examples of errors including those specific to iris cameras, as well recommendations for mitigation of those errors. IREX V can provide a useful basis for training; it has been used by some vendors as part of the training they provide. Vendors should be asked about any system-specific training that will be provided with their systems.

Acknowledgments

Particular thanks to our colleagues Michael Garris and James St. Pierre of NIST for detailed comments that improved the clarity and utility of the manuscript. Thanks also to our colleagues in the Iris Experts Group and in the biometric recognition community at large for input and advice that has and continues to help us think through the issues discussed in this paper.

Table 1. Standards/Specifications Relevant for Iris Recognition

Standard/Specification #		Standard/Specification Name	URL
ISO/IEC 19794-6:2011	[2]	Information technology – Biometric data interchange formats – Part 6: Iris image data	www.iso.org/standard/50868.html
ISO/IEC 29794-6:2015	[7]	Information technology – Biometric sample quality – Part 6: Iris image data	www.iso.org/standard/54066.html
ANSI/NIST-ITL 1-2011 Update: 2015	[3]	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	dx.doi.org/10.6028/NIST.SP.500-290e3
EBTS Version 10.0.8 2017	[4]	Electronic Biometric Transmission Specification	www.fbibiospecs.cjis.gov/EBTS/Approved

References

[1] Libert JM, et al. (2018) Guidance for Evaluating Contactless Fingerprint Acquisition Devices, NIST Special Publication 500-305. NIST, Technical report. https://doi.org/10.6028/NIST.SP.500-305

[2] ISO/IEC (2011) ISO/IEC ISO-19794-6:2011, information technology - biometric data interchange formats - part 6: Iris image data. ISO/IEC, Technical report.

[3] NIST (2015) ANSI/NIST-ITL 1-2011. Update: 2015 information technology: American national standard for information systems data format for the interchange of fingerprint, facial and other biometric information. ANSI/NIST-ITL, Technical report. https://doi.org/10.6028/NIST.SP.500-290e3

[4] US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division (2018) Electronic Biometric Transmission Specification, Version 10.0.8, . URL https://www.fbibiospecs.cjis.gov/.

[5] Brown A (2003) Digital preservation guidance note: 4, graphics file formats. The National Archives, United Kingdom, Technical report. URL https://www.nationalarchives.gov.uk/documents/graphic-file-formats.pdf.

[6] Quinn GW, Matey J, Tabassi E, Grother PJ (2014) IREX V: guidance for iris image collection. National Institute of Standards and Technology, Technical Report NISTIR-8013. https://doi.org/10.6028/NIST.IR.8013. URL https://www.nist.gov/publications/irex-v-guidance-iris-image-collection

[7] ISO/IEC 29794-6:2015 (2015) *Information technology – Biometric sample quality – Part 6: Iris image data* (ISO, Geneva, Switzerland), . URL https://www.iso.org/standard/54066.html.