Halmstad University

This is a submitted version of a paper published in *IEEE Security and Privacy*.

Citation for the published paper:

Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J. (2012)

"Quality Measures in Biometric Systems"

IEEE Security and Privacy, 10(6): 52-62

URL: <http://dx.doi.org/10.1109/MSP.2011.178>

Access to the published version may require subscription.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-16810>

<http://hh.diva-portal.org>

Quality Measures in Biometric Systems

Fernando Alonso-Fernandez | Halmstad University

Julian Fierrez and Javier Ortega-Garcia | Universidad Autónoma de Madrid

Biometric signals' quality heavily affects a biometric system's performance. A review of the state of the art in these matters gives an overall framework for the challenges of biometric quality.

Biometric recognition is a mature technology used in many government and civilian applications such as e-passports, ID cards, and border control. Examples include the US-Visit (United States Visitor and Immigrant Status Indicator Technology) fingerprint system, the Privium iris system at Schiphol airport, and the SmartGate face system at Sydney Airport.

However, during the past few years, biometric quality measurement has become an important concern after biometric systems' poor performance on pathological samples. Studies and benchmarks have shown that biometric signals' quality heavily affects biometric system performance. This operationally important step has nevertheless received little research compared to the primary feature-extraction and pattern-recognition tasks.

Many factors can affect biometric signals' quality, and quality measures can play many roles in biometric systems. Here, we summarize the state of the art in quality measures for biometric systems, giving an overall framework for the challenges involved.

How Signal Quality Affects System Performance

One of the main challenges facing biometric technologies is performance degradation in less controlled situations.¹ The proliferation of portable handheld devices with at-a-distance and on-the-move biometric acquisition capabilities are just two examples of nonideal scenarios that aren't sufficiently mature. These will require robust recognition algorithms that can handle a range of

changing characteristics.² Another important example is forensics, in which intrinsic operational factors further degrade recognition performance and generally aren't replicated in controlled studies.³

Conditions that are progressively more difficult significantly decrease performance, despite improvements in technology. For example, the 2009 evaluation in the Multiple Biometric Grand Challenge (<http://face.nist.gov/mbgc>) showed decreased performance of face recognition for uncontrolled illumination conditions and severe image compression with respect to the controlled conditions used in the 2006 Face Recognition Vendor Test evaluation (see Figure 1a). In the 2000 and 2002 Fingerprint Verification Competitions (<https://biolab.csr.unibo.it/fvcongoing>), fingerprint data was acquired without any special restriction, resulting in a decrease of one order of magnitude in the equal error rate (see Figure 1b). In 2004, researchers in the competition intentionally corrupted samples (for example, by asking people to exaggeratedly rotate or press their finger against the sensor, or by artificially drying or moisturizing the skin with water or alcohol). A corresponding performance decrease occurred. Finally, the performance of Vasir (Video-Based Automatic System for Iris Recognition; www.nist.gov/itl/iad/ig/vasir.cfm) dramatically decreased when it used distant video (unconstrained acquisition) instead of classic close-up controlled acquisition (see Figure 1c).

Figure 2 shows more examples of data degradation related to face and fingerprint recognition. The

Figure 1. How low-quality data affects recognition algorithms' performance. Results for (a) the best performing algorithm in independent face evaluations as part of the Multiple Biometric Grand Challenge (MBGC) and the Face Recognition Vendor Test evaluation, (b) the best performing algorithm in the Fingerprint Verification Competitions (FVCs), and (c) Vasir (Video-Based Automatic System for Iris Recognition). Conditions that are progressively more difficult significantly decrease performance, despite improvements in technology.

face similarity scores come from a verifier that is based on linear discriminant analysis. It uses Fisher's linear discriminant projection for indoor images and an eigenface-based system with principal component analysis for outdoor images. The fingerprint similarity scores come from the publicly available minutia-based matcher released by the US National Institute of Standards and Technology (NIST). The data is from the BioSecure Multimodal Database.⁴

Face recognition performance degrades with the webcam and further degrades when the webcam image is acquired in the more challenging outdoor environment (see Figure 2a).

With flat sensors, fingerprint acquisition employs the touch method—the subject simply places a finger on the scanner. Conversely, in sweep sensors, the subject sweeps the finger vertically across a tiny strip only a few pixels high. As the finger sweeps across this strip, the system forms partial images of the finger, which it combines to generate a full fingerprint image. This procedure allows reductions in the acquisition area and the sensing element's cost (thus facilitating its use in consumer products such as laptops, PDAs, and mobile phones). However, reconstructing the full fingerprint image is

error-prone, especially for poor-quality fingerprints and nonuniform sweep speeds (see Figure 2b).

What Is Biometric Sample Quality?

Broadly, a biometric sample is of good quality if it's suitable for personal recognition. Recent standardization efforts (ISO/IEC 29794-1) have established three components of biometric-sample quality (see Figure 3):

- *character* indicates the source's inherent discriminative capability;
- *fidelity* is the degree of similarity between the sample and its source, attributable to each step through which the sample is processed; and
- *utility* is a sample's impact on the biometric system's overall performance.

The character and fidelity contribute to or detract from the sample's utility.¹

The most important thing we expect a quality metric to do is to mirror the sample's utility so that higher-quality samples lead to better identification of individuals.¹ So, quality should be predictive of recognition performance. This statement, however, is largely subjective:

Figure 2. Performance degradation with portable handheld devices. (a) Face similarity scores and input. (b) Fingerprint similarity scores and input. For faces, recognition performance degrades with the webcam and degrades even more when the webcam image is acquired outdoors. For fingerprints, sweep sensors perform worse than flat sensors; however, they're easier to implement in laptops, PDAs, mobile phones, and so on.

Figure 3. Defining biometric quality from three different points of view: character, fidelity, and utility. The character and fidelity contribute to or detract from the sample's utility.

not all recognition algorithms work the same (that is, they aren't based on the same features), and their performance isn't affected by the same factors. For example, face recognition algorithm A might be insensitive to illumination changes, whereas such changes severely

affect algorithm B. In this situation, a measure of illumination will be useful for predicting B's performance but not A's. Therefore, an algorithm's efficacy will usually be linked to a particular recognition algorithm or class thereof.

Figure 4. Factors affecting biometric signals' quality are related to users, user-sensor interaction, the acquisition sensor, and the system. For a look at some of these factors in more detail, see the "Additional Factors Influencing Biometric Quality" sidebar.

Factors Influencing Biometric Quality

Following Eric Kukula and his colleagues' framework⁵ and other previous research,^{6–8} we classify quality factors on the basis of their relationships with the system's different parts.⁹ We distinguish four classes: user-related, user-sensor interaction, acquisition sensor, and processing-system factors (see Figure 4). User-related factors can affect the biometric sample's character; the remaining factors affect the sample's fidelity.

User-Related Factors

These factors include physical, physiological, and behavioral factors. Because they have to do entirely with the user—a person's inherent features are difficult or impossible to modify—they're the most difficult to control.

Physical or physiological. Consider age, gender, or race—subjects can't alter these factors for the convenience of recognition studies' requirements. Therefore, recognition algorithms must account for data variability in these categories—for example, differences in speech between males and females. Also, diseases or injuries can alter features such as the face or finger, sometimes irreversibly, possibly making them infeasible for

recognition. On the other hand, such alterations can make it possible to narrow a person's identity (for example, an amputated leg might make gait recognition more precise in some cases).

Behavioral. Sometimes, people can modify their behaviors or habits. You can alleviate many behavioral factors by taking corrective actions—for example, by instructing subjects to remove eyeglasses or keep their eyes open. But this isn't always possible, like in forensic or surveillance applications. On the other hand, depending on the application, such corrective actions could be counterproductive, resulting in subjects being reluctant to use the system.

User-Sensor Interaction Factors

In principle, these factors, which include environmental and operational factors, are easier to control than user-related factors, provided that we can supervise the interaction between the user and the sensor—for example, in controllable premises. Unfortunately, requirements of less controlled scenarios, such as mobility or remoteness, make a biometric algorithm to account for environmental or operational variability necessary.

Additional Factors Influencing Biometric Quality

Here we look in more detail at some of the factors listed in Figure 4 in the main article.

Outdoor operation is especially problematic because control of other environmental factors can be lost. It also demands additional actions regarding sensor conditions and maintenance.

Background and *object occlusion* are related to uncontrolled environments (for example, surveillance cameras) and can greatly degrade face recognition systems' performance.

Temperature and *humidity* affect skin properties (in fingerprint and palm print recognition).

Illumination and *light reflection* can affect iris images owing to the eye's reflective properties. They can also affect face images.

Ambient noise affects the quality of speech.

Feedback to the user regarding the acquired data has been demonstrated to lead to better acquired samples, which can lead to *user familiarity* with the system.

Sensors sometimes incorporate *physical guides* to facilitate acquisition (for example, for fingerprint and palm print recognition).

Ergonomics refers to how the acquisition device's design facilitates user interaction.

Time between acquisitions can greatly affect system performance because data acquired from an individual at two different moments might differ considerably.

The user's *age* can affect recognition in several ways. Although iris pigmentation and fingerprint characteristics are highly stable, they change until adolescence and during old age. Other traits such as a subject's face, speech, and signature evolve throughout life. The user's age can also degrade the sample owing to, for example, medical conditions or the loss of certain abilities.

Gender can cause differences in face or speech characteristics.

Ethnic origin can affect basic facial features and the iris (in some ethnic groups, pigmentation is different or the iris isn't visible owing to eyelid occlusion or long eyelashes). It can also affect a user's behavior, for example, the user's facial appearance (hairstyle, beard, jewelry, and so on), speech (language, lexicon, intonation, and so on), and signature (American signatures typically consist of a readable written name, European signatures normally include a flourish, and Asian signatures often consist of independent symbols).

Skin condition refers to factors such as skin moisture, sweat, cuts, and bruises, which can affect traits involving analysis of skin properties (for example, in fingerprint and palm print recognition).

Manual labor might affect the skin condition, in some cases irreversibly.

A user's *illiteracy* could affect signature recognition or the user's ability to use the system when reading or writing is required.

Acquisition Sensor Factors

In most cases, the sensor is the only physical point of interaction between the user and the biometric system. Its fidelity in reproducing the original biometric pattern is crucial for the recognition system's accuracy. The diffusion of low-cost sensors and portable devices (such as mobile cameras, webcams, telephones and PDAs with touchscreen displays, and so on) is rapidly growing in the context of convergence and ubiquitous access to information and services. This represents a new scenario for automatic biometric recognition systems.

Unfortunately, these low-cost, portable devices produce data very different from that obtained by dedicated, more expensive sensors. This is primarily owing to smaller input areas, poor ergonomics, and the possibility of user mobility. Additional problems arise when data from different devices coexists in a biometric system—something common in multivendor markets. Algorithms must account for data variability in this scenario of interoperability—something that can be achieved through the use of quality measures.¹⁰

Processing-System Factors

These factors relate to how a biometric sample is

processed after it has been acquired. In principle, they're the easiest to control. Constraints on storage or exchange speed might impose data compression techniques—for example, in the case of smart cards. Also, governments, regulatory bodies, or international standards organizations might specify that biometric data must be kept in raw form (rather than in postprocessed templates that might depend on proprietary algorithms), which could affect data size.

So, data compression's effects on recognition performance become critical. The necessity for data compression, together with packet loss effects, has played a part in recent applications of biometrics over mobile networks or the Internet.

Ensuring Biometric Samples' Quality

Table 1 provides helpful guidelines for controlling biometric samples' quality.⁶ We've identified three points of action:

- the capture point (a critical point of action because it acts as the main interface between the user and the system),
- the quality assessment algorithm, and
- the system performing the recognition.

Table 1. Biometric quality assurance's three points of action.

Capture point	Quality assessment algorithm	System
Supervision by an operator Adequate operator training and environment Repetitive task: avoid tiredness, boredom, and so on	Time of response vs. good quality tradeoff Real-time quality assessment	Quality-based processing Additional enhancement Alternative feature extraction Different matching algorithm
Adequate sensor With enough capabilities for the application (size, resolution, and so on) Newer designs with enhanced capabilities to acquire bad-quality sources (for example, touchless or 3D fingerprint)	Problems/corrective actions Acquisition loop/recapture until satisfaction Invoke different processing Invoke human intervention Reject acquired sample	Quality-based fusion Combine different algorithms, biometric traits, and so on
Enhanced GUI Large display Real-time feedback of acquired data	Adhesion to standards Use certified quality measures	Template substitution/update Use the new acquired signal to enhance the stored template
Proper user interaction User-friendly process Clear procedure (for example, open your eyes) Ergonomics (sensor placement, user positioning, distance, and so on) Physical guides (brackets, and so on)		Monitoring and periodic reporting Statistics by application, site, device, subject, specific hours or day of the week, and so on Identify user-scanner learning curve
Adequate environment Light, temperature, background, and so on Both for user and operator		Adhesion to standards Use certified software and interfaces
Good sensor maintenance Periodical cleaning Substitution if deterioration		
Adhesion to standards Use certified sensors Ensure good acquisition practices		

Improved quality, by either capture point design or system design, can lead to better performance. For aspects of quality you can't design in, you need the ability to analyze a sample's quality and initiate corrective action. This ability is a key component in quality assurance management. It includes, for example, initiating reacquisition from a user, selecting the best sample in real time, or selectively evoking different processing methods (see the Quality assessment algorithm column in Table 1).

Quality Assessment Algorithms

Researchers have developed quality assessment algorithms mainly for fingerprints,¹¹ irises,¹² voices,¹³ faces,¹⁴ and signatures.¹⁵ Figure 5 shows examples of properties assessed by some of these algorithms. Unfortunately, almost all of the many algorithms have been tested under limited, heterogeneous frameworks. This is primarily because the biometrics community has only recently formalized the concept of sample quality and developed evaluation methodologies. Here, we describe two proposed frameworks for this purpose.

Measuring Entropy Change

Richard Youmaran and Andy Adler developed a theoretical framework for measuring biometric sample fidelity.¹⁶ They related biometric sample quality to the amount of identifiable information in a sample and suggested that this amount decreases as quality decreases. They measured this amount as $D(p||q)$, the relative entropy between the population feature distribution q and the subject's feature distribution p . On this basis, you can measure the information loss due to degradation in sample quality as the relative change in entropy.

Measuring Prediction Capability

Most operational approaches for quality estimation of biometric signals focus on signal utility. Patrick Grother and Elham Tabassi presented a framework for evaluating and comparing quality measures in terms of the capability of predicting system performance.¹ Broadly, they formalized sample quality as a scalar quantity monotonically related to biometric matchers' recognition

Figure 5. Some properties measured by biometric quality assessment algorithms. Unfortunately, almost all of the many algorithms have been tested under limited, heterogeneous frameworks.

Figure 6. Evaluating the utility of four fingerprint quality measures (orientation certainty level [OCL], local clarity score [LCS], concentration of energy in annular bands, and NIST Fingerprint Image Quality [NFIQ]).¹¹ Results show the verification performance when samples with the lowest-quality value are rejected. Each measure results in a different performance improvement for the same fraction of rejected samples.

performance. So, by partitioning the biometric data into different groups according to some quality criteria, the quality measure will give an ordered indication of performance between quality groups. Also, rejection of

low-quality samples will decrease error rates in proportion to the fraction rejected.

Figure 6 shows an example of this framework evaluating the utility of fingerprint quality metrics. The similarity scores come from the same minutia-based matcher from Figure 2, and the data is from the BioSec multimodal database.¹¹

As we mentioned before, a quality algorithm's efficacy is usually tied to a particular recognition algorithm. This is evident in Figure 6, in which each quality metric results in different performance improvement for the same fraction of rejected low-quality samples.

Also, although biometric matching involves at least two samples, we don't acquire them at the same time. Reference samples are stored in the system database and are later compared with new samples provided during system operation. So, a quality assessment algorithm should be able to work with individual samples, even though it ultimately aims to improve recognition performance when matching two or more samples.

Human versus Automatic Quality Assessment

There's an established community of people who are expert in recognizing biometric signals for certain applications (such as with signatures on bank checks or fingerprints in the forensics field). Also, some biometric applications include manual quality verification in their workflows (such as with immigration screening and passport generation). In addition, many researchers use datasets with manually labeled quality measures to optimize and test their quality assessment algorithms. A common assumption is that a human's assessment of biometric quality is a gold standard against which to measure biometric sample quality.¹⁷

To the best of our knowledge, only one study has sought to test the relevance of human evaluations of biometric sample quality.¹⁷ From this study, it's evident that human and computer processing aren't always functionally comparable. For instance, if a human judges a face or iris image to be good because of its sharpness, but a recognition algorithm works in low frequencies, then the human statement of quality isn't appropriate. Human inspectors' judgments can improve with adequate training on the recognition system's limitations, but this could be prohibitively expensive and time-consuming. In addition, incorporating a human quality checker could create other problems, such as inaccuracy due to the tiredness, boredom, or lack of motivation that a repetitive task such as this might cause.¹⁸

Incorporating Quality Measures in Biometric Systems

The incorporation of quality measures in biometric

Figure 7. The roles of a sample quality measure in biometric systems. These roles aren't mutually exclusive; prevention of poor-quality data requires a holistic, systemwide focus.

systems is an active field of research with many proposed solutions. Figure 7 summarizes different uses of sample quality measures in this context. These roles aren't mutually exclusive; indeed, prevention of poor-quality data requires a holistic, systemwide focus.

In Figure 7, the recapture loop implements an “up to three attempts” policy, giving feedback in each subsequent acquisition to improve quality. Selections from video streams can also be implemented, if possible.

Quality-based processing involves

- quality-specific enhancement algorithms;
- conditional execution of processing chains, including specialized processing for poor-quality data;
- extraction of features robust to the signal's degradation;
- extraction of features from useful regions only; and
- ranking of extracted features based on the local regions' quality.

Template updating (updating of the enrollment data and database maintenance) involves

- storing multiple samples representing the variability associated with the user (for example, different portions of the fingerprint to deal with partially overlapped fingerprints, or multiple viewpoints of the face) and
- updating the stored samples with better-quality samples captured during system operation.¹⁹

Quality-based matching, decision, and fusion involve

- using different matching or fusion algorithms;
- adjusting those algorithms' sensitivity;

- quantitative indication of the acceptance or rejection decision's reliability;
- quality-driven selection of data sources to be used for matching or fusion—for example, weighting schemes for quality-based ranked features or data sources;¹⁰ and
- using soft biometric traits (age, height, sex, and so on) to assist in recognition.

Monitoring and reporting across the different parts of the system help you identify problems leading to poor-quality signals and initiate corrective actions. This process can assess signal quality according to these factors:²⁰

- *Application.* Different applications might require different scanners, environment setups, and so on, which might have different effects on the acquired signals' overall quality.
- *Site or terminal.* Such assessment identifies sites or terminals that are abnormal owing to operator training, operational and environmental conditions, and so on.
- *Capture device.* Such assessment identifies the impact due to different acquisition principles, mechanical designs, and so on. It also determines whether a specific scanner must be substituted if it doesn't provide signals that satisfy the quality criteria.
- *Subject.* Such assessment identifies interaction learning curves, which can help better train new users and alleviate the “first-time user” syndrome.⁸
- *Stored template.* Such assessment detects how the database's quality varies when new templates are stored or old ones are updated.
- *Biometric input.* If the system uses multiple biometric traits, such assessment improves how they're combined.

Monitoring and reporting can also support trend

Organizations Working in Biometric-Standards Development

International Standards Organizations

- IEC: International Electrotechnical Commission (www.iec.ch)
- ISO-JTC1/SC37: International Organization for Standardization, Committee 1 on Information Technology, Subcommittee 37 for Biometrics (www.iso.org/iso/jtc1_sc37_home)

National standards bodies

- ANSI: American National Standards Institute (www.ansi.org)

Standards-developing organizations

- ICAO: International Civil Aviation Organization (www.icao.int)
- INCITS M1: International Committee for Information Technology Standards, Technical Committee M1 on Biometrics (<http://standards.incits.org/a/public/group/m1>)
- NIST-ITL: American National Institute of Standards and Technology, Information Technology Laboratory (www.nist.gov/itl)

Other organizations

- BC: Biometric Consortium (www.biometrics.org)
- BCOE: Biometric Center of Excellence (www.biometriccoe.gov)
- BIMA: Biometrics Identity Management Agency (www.biometrics.dod.mil)
- IBG: International Biometric Group (www.ibgweb.com)
- IBIA: International Biometrics and Identification Association (www.ibia.org)

Standardizing Biometric Quality

The entire quality assurance process should adhere to biometric quality standards with regard to sensors, software, and interfaces. Standards give flexibility and modularity, as well as fast technology interchange, sensor and system interoperability, and proper interaction with external security systems. Standards compliance lets you replace parts of deployed systems with various technological options from open markets. Often, as biometric technology becomes extensively deployed, several multivendor applications from different agencies will exchange information; this can involve heterogeneous equipment, environments, and locations.²

So, as a response to the need for interoperability, biometric standards allow modular integration of products, also facilitating future upgrades. Examples of interoperable scenarios include using e-passports readable by different countries or exchanging lists (for instance, of criminals) among security forces.

The “Organizations Working in Biometric-Standards Development” sidebar lists standards organizations and other bodies working in biometric-standards development. Current development focuses on acquisition practices, sensor specifications, data formats, and technical interfaces (see Figure 8 and Table 2).²¹ Also, a registry of US-government-recommended biometric standards (www.biometrics.gov/standards) offers high-level guidance for their implementation.

Concerning the specific incorporation of quality information, most standards define a quality score field aimed to incorporate quality measures. However, this field’s content isn’t explicitly defined and is somewhat subjective owing to a lack of consensus on

- how to provide universal quality measures that various algorithms can interpret and
- which key factors define quality in a given biometric trait.

ISO/IEC 29794-1/4/5 is addressing these problems. A prominent approach in this standard is the *quality algorithm vendor ID (QAID)*, which incorporates standardized data fields that uniquely identify a quality assessment algorithm, including its vendor, product code, and version. You can easily add QAID fields to existing data interchange formats such as the Common Biometric Exchange Formats Framework (CBEFF). This enables a modular multivendor environment that accommodates samples scored by different quality assessment algorithms in different data interchange formats.

Figure 8. The use of standards in biometric systems to ensure good-quality signals. Table 2 describes the standards.

analysis by providing statistics of all applications, sites, and so on. This will let analysts identify trends in signal quality or sudden changes that need further investigation.

A variety of civilian and commercial biometric systems applications’ deployments are being limited

Table 2. Biometric standards.

Standard	Description
ANSI/NIST-ITL 1-2000	Supports the exchange of biometric data, including fingerprints, faces, scars, marks, and tattoos, between law enforcement and related criminal justice agencies.
ANSI/NIST-ITL 1-2007/2-2008	Defines a common format for exchanging and storing a variety of biometric data including faces, fingerprints, palm prints, irises, voices, and written signatures.
BioAPI (Biometric Application Programming Interface)	Defines the architecture and necessary interfaces to allow biometric applications to be integrated from different vendors' modules. Versions 1.0 and 1.1 were produced by the BioAPI Consortium, a group of more than 120 companies and organizations with an interest in the biometrics market. BioAPI 2.0 is specified in ISO/IEC 19784-1 (published May 2006).
CBEFF (Common Biometric Exchange Formats Framework)	Supports the exchange of biometric information between different systems or system components. The CBEFF Development Team at the US National Institute of Standards and Technology (NIST) and the BioAPI Consortium developed it from 1999 to 2000.
DHS-IDENT-IXM (DHS Automated Biometric Identification System-Exchange Messages Specification)	Supports the exchange of biometric data with the US Department of Homeland Security. Version 5.0 was released in November 2009.
DoD-EBTS (DoD Electronic Biometric Transmission Specification)	Supports the exchange of biometric data with the US Department of Defense. It's an implementation of ANSI/NIST ITL 1-2007. Version 3.0 was released in December 2011.
FBI-EBTS (FBI Electronic Biometric Transmission Specification)	Supports the exchange of biometric data with the US FBI. It's an implementation of ANSI/NIST ITL 1-2007. Version 9.3 was released in December 2011.
FBI-WSQ (FBI Wavelet Scalar Quantization)	Defines a compression algorithm for fingerprint images. The FBI and NIST developed the algorithm to archive the large FBI fingerprint database (with more than 100 million prints as of this writing). Version 3.1 was released in October 2010.
ISO/IEC-19794	Specifies a common format to exchange and store a variety of biometric data, including faces, fingerprints, palm prints, irises, voices, and written signatures.
Annex to ISO/IEC-19794-5	Includes recommendations for taking photographs of faces for e-passport and related applications and includes indications about lighting, camera arrangement, and head positioning.
ISO/IEC 29794-1/4/5	Enables harmonized interpretation of quality scores from different vendors, algorithms, and versions by setting key factors to define quality in different biometric traits. It also addresses the interchange of biometric quality data via ISO/IEC 19794.

by unsatisfactory performance observed in newer scenarios of portable or low-cost devices, remote access, and surveillance cameras. Increasing user convenience by relaxing acquisition constraints has been identified as having the greatest impact in mass acceptance levels and widespread adoption of biometric technologies. This makes the capability of handling poor-quality data essential—an area of research we hope to continue to see grow. ■

Acknowledgments

A Juan de la Cierva postdoctoral fellowship from the Spanish Ministry of Science and Innovation (MICINN) supported Fernando Alonso-Fernandez's research at the Biometric Recognition Group—ATVS. The Swedish Research Council and European Commission (Marie Curie Intra-European Fellowship program) funded Alonso-Fernandez's postdoctoral research at Halmstad University. Cátedra Universidad Autónoma de Madrid-Telefónica, Projects Contexts (S2009/

TIC-1485) from Comunidad de Madrid (CAM), Bio-Challenge (TEC2009-11186) from MICINN, and Tabula Rasa (FP7-ICT-257289) and BBfor2 (FP7-ITN-238803) from the EU also supported this research. We also thank the Spanish Dirección General de la Guardia Civil for its support.

References

1. P. Grother and E. Tabassi, "Performance of Biometric Quality Measures," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, 2007, pp. 531–543.
2. A.K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview," *Second Generation Biometrics*, Springer, 2010.
3. A.K. Jain, B. Klare, and U. Park, "Face Recognition: Some Challenges in Forensics," *Proc. Int'l Conf. Automatic Face and Gesture Recognition (FG 11)*, IEEE, 2011, pp. 726–733.
4. J. Ortega-Garcia et al., "The Multi-scenario Multi-environment BioSecure Multimodal Database (BMDB),"

- IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, 2009, pp. 1097–1111.
5. E.P. Kukula, M.J. Sutton, and S.J. Elliott, “The Human-Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements,” *IEEE Trans. Instrumentation and Measurement*, vol. 59, no. 4, 2010, pp. 784–791.
 6. J.-C. Fondeur, “Thoughts and Figures on Quality Measurements,” US Nat’l Inst. Standards and Technology, 2006; http://biometrics.nist.gov/cs_links/quality/workshopI/proc/fondeur_quality_1.0.pdf.
 7. T. Mansfield, “The Application of Quality Scores in Biometric Recognition,” US Nat’l Inst. Standards and Technology, 2007; http://biometrics.nist.gov/cs_links/quality/workshopII/proc/mansfield_07-11-07_NISTQWkshp.pdf.
 8. M. Theofanos et al., “Biometrics Systematic Uncertainty and the User,” *Proc. IEEE Conf. Biometrics: Theory, Applications and Systems (BTAS 07)*, IEEE, 2007, pp. 1–6.
 9. F. Alonso-Fernandez, “Biometric Sample Quality and Its Application to Multimodal Authentication Systems,” doctoral dissertation, Dept. Signals, Systems, and Radiocommunications, Universidad Politécnica de Madrid, 2008.
 10. F. Alonso-Fernandez et al., “Quality-Based Conditional Processing in Multi-biometrics: Application to Sensor Interoperability,” *IEEE Trans. Systems, Man, and Cybernetics, Part A*, vol. 40, no. 6, 2010, pp. 1168–1179.
 11. F. Alonso-Fernandez et al., “A Comparative Study of Fingerprint Image Quality Estimation Methods,” *IEEE Trans. Information Forensics and Security*, vol. 2, no. 4, 2007, pp. 734–743.
 12. N.D. Kalka et al., “Estimating and Fusing Quality Factors for Iris Biometric Images,” *IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 3, 2010, pp. 509–524.
 13. A. Harriero et al., “Analysis of the Utility of Classical and Novel Speech Quality Measures for Speaker Verification,” *Proc. Int’l Conf. Biometrics (ICB)*, LNCS 5558, Springer, 2009, pp. 434–442.
 14. D.P. D’Amato, N. Hall, and D. McGarry, “The Specification and Measurement of Face Image Quality,” US Nat’l Inst. Standards and Technology, 2010; http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/DAmato_Daon_The%20Specification%20and%20Measurement%20of%20Face%20Image%20Quality-Final.pdf.
 15. N. Houmani, S. Garcia-Salicetti, and B. Dorizzi, “A Novel Personal Entropy Measure Confronted with Online Signature Verification Systems Performance,” *Proc. IEEE Conf. Biometrics: Theory, Applications and Systems (BTAS 08)*, IEEE, 2008, pp. 1–6.
 16. R. Youmaran and A. Adler, “Measuring Biometric Sample Quality in Terms of Biometric Information,” *Proc. Biometric Consortium Conf.: Special Session on Research at the Biometrics Symp.*, IEEE, 2006, pp. 1–6.
 17. A. Adler and T. Dembinsky, “Human vs. Automatic Measurement of Biometric Sample Quality,” *Proc. Canadian Conf. Electrical and Computer Eng. (CCECE 06)*, IEEE CS, 2006, pp. 2090–2093.
 18. K.E. Wertheim, “Human Factors in Large-Scale Biometric Systems: A Study of the Human Factors Related to Errors in Semiautomatic Fingerprint Biometrics,” *IEEE Systems J.*, vol. 4, no. 2, 2010, pp. 138–146.
 19. A. Rattani et al., “Template Update Methods in Adaptive Biometric Systems: A Critical Review,” *Proc. Int’l Conf. Biometrics (ICB)*, LNCS 5558, Springer, 2009, pp. 847–856.
 20. T. Ko and R. Krishnan, “Monitoring and Reporting of Fingerprint Image Quality and Match Accuracy for a Large User Application,” *Proc. 33rd Applied Image Pattern Recognition Workshop (AIPR 04)*, IEEE CS, 2004, pp. 159–164.
 21. E. Tabassi and P. Grother, “Biometric Sample Quality, Standardization,” *Encyclopedia of Biometrics*, S.Z. Li, ed., Springer, 2009; www.springerreference.com/docs/html/chapterdbid/70982.html.
-
- Fernando Alonso-Fernandez** is a postdoctoral researcher at Halmstad University’s Intelligent Systems Laboratory. His research interests include signal and image processing, pattern recognition, and biometrics. Alonso-Fernandez received a PhD in electrical engineering from Universidad Politécnica de Madrid. He’s a member of IEEE. Contact him at feralo@hh.se.
-
- Julian Fierrez** is an associate professor in the electronics and communications technology department at the Escuela Politécnica Superior, Universidad Autónoma de Madrid. His research interests include signal and image processing, pattern recognition, and biometrics, particularly signature and fingerprint verification, multibiometrics, biometric databases, and system security. Fierrez received a PhD in telecommunications engineering from Universidad Politécnica de Madrid. He’s a member of IEEE. Contact him at julian.fierrez@uam.es.
-
- Javier Ortega-García** is a full professor in the electronics and communications technology department at the Escuela Politécnica Superior, Universidad Autónoma de Madrid. His research interests include speaker recognition, face recognition, fingerprint recognition, online signature verification, data fusion, and multimodality in biometrics. Ortega-García received a PhD in electrical engineering from Universidad Politécnica de Madrid. He’s a senior member of IEEE. Contact him at javier.ortega@uam.es.
-

Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.