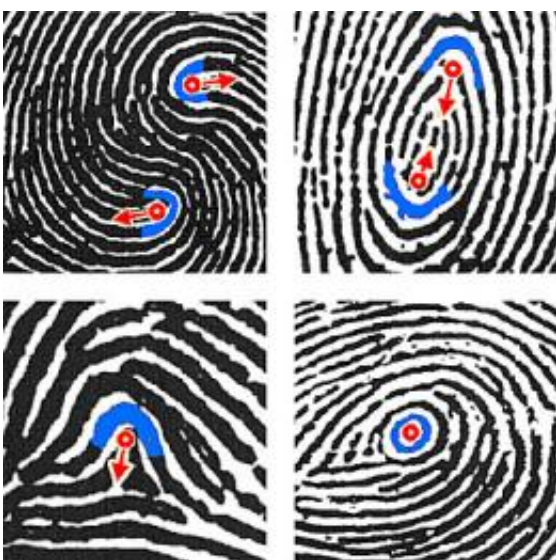


# New NIST biometric data standard adds DNA, footmarks and enhanced fingerprint descriptions

December 7 2011, By Evelyn Boswell

---



These examples of the new standards Extended Features Set show forensic scientists how to mark core locations (clockwise from from top left) for a double loop whorl, plain whorl, central pocket loop whorl and tented arch. Credit: NIST

The National Institute of Standards and Technology (NIST) published a revised biometric standard in November, 2011, that vastly expands the type and amount of information that forensic scientists can share across their international networks to identify victims or solve crimes.

Biometric data is a digital or analog representation of physical attributes that can be used to uniquely identify us.

The new standard is the Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information and is referenced as "ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290." Earlier versions have been used throughout the United States and six continents to provide a common language and format for the exchange of biometric data and associated metadata—information about the biometric characteristics or how it was collected. The Department of Defense, the Federal Bureau of Investigation, the Department of Homeland Security, the government of Argentina and others are already in the process of adopting the new standard.

"The additions to this version of the standard represent a great leap forward," said NIST Biometrics Standards Coordinator Brad Wing. The capabilities of the system have been greatly expanded from that of matching a fingerprint, facial image or iris sample collected directly from a live person and comparing it to samples previously stored in a database. New types of biometric data—DNA and plantars/footprints—were added as well as updates to existing record types.

This is the first international standard for the exchange of DNA data. DNA can be used for criminal case identification, such as in a rape case, or in a forensic setting to identify victims, such as those in a plane crash, where it is necessary to have an original DNA sample from the victim, or establish kinship by taking DNA samples from purported relatives. The standard handles both types of cases.

Another new addition is the Extended Feature Set (EFS) for forensic examiner markups that allow for marking and exchanging a very rich set of latent ridge print—[fingerprints](#), palmprints and footprints—information that ensures analysts use the same terminology, references and procedures to describe details such as pores and linear discontinuities. Also new is the capability to share images of all body

parts and anthropometric markups of face and iris images.

The standard now defines how to specify and share the geo-positioning coordinates of biometric sample collection. Information concerning the circumstances surrounding the collection of the biometric data can also be included. This includes pictures of items found around the crime scene and audio and video clips. Data handling logs show chain-of-custody of the biometric data for legal purposes, including the steps necessary to prepare the biometric sample for processing in a matching system.

NIST biometric research contributed heavily to the standard. In addition to part of the DNA work, the standard uses a NIST-developed compact format to exchange iris images, and the Mobile ID Best Practice Recommendations.

Researchers already are at work on new additions to the standard, including voice biometrics, traumatic injury imaging and analysis (such as bite marks), dental forensics (used to identify persons when DNA is not readily available, such as with skeletons) and conformance testing to the standard specifications.

NIST is involved with many standards development organizations (SDO), but the Information Technology Laboratory that produced this standard is NIST's only SDO, and is certified by the American National Standards Institute (ANSI). The standard is developed according to a consensus process and this update involved almost 70 voting organizations participating in 16 working groups over a two-year period.

The new [biometric](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136) standard may be found at:  
[www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=910136](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136) .

**More information:** NIST Interagency Report 7629 Supplement One,

IREX I: Performance of Iris Recognition Algorithms on Standard Images, January 12, 2010, [www.nist.gov/itl/iad/ig/irexi.cfm](http://www.nist.gov/itl/iad/ig/irexi.cfm)

NIST Special Publication 500-280 Mobile ID Device Best Practice Recommendation Version 1.0, July 2009, [www.nist.gov/customcf/get\\_pdf.cfm?pub\\_id=903169](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=903169)

Provided by National Institute of Standards and Technology

Citation: New NIST biometric data standard adds DNA, footmarks and enhanced fingerprint descriptions (2011, December 7) retrieved 18 April 2024 from <https://phys.org/news/2011-12-nist-biometric-standard-dna-footmarks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.