Stabilized as
INCITS 381-2009 (S2019)

American National Standard

for Information Technology –
Finger Image Based Data Interchange Format

INCITS 381-2009

Developed by

incits SM

*Where **IT** all begins*

Approved American National Standard
ANSI

INCITS 381-2009
Revision of
INCITS 381-2004

American National Standard
for Information Technology –

Finger Image Based Data Interchange Format

Secretariat

Information Technology Industry Council

Approved September 14, 2009

American National Standards Institute, Inc.

Abstract

This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.

American National Standard

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgement of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

CAUTION: The developers of this standard have requested that holders of patents that may be required for the implementation of the standard disclose such patents to the publisher. However, neither the developers nor the publisher have undertaken a patent search in order to identify which, if any, patents may apply to this standard. As of the date of publication of this standard and following calls for the identification of patents that may be required for the implementation of the standard, no such claims have been made. No further patent search is conducted by the developer or publisher in respect to any standard it processes. No representation is made or implied that licenses are not required to avoid infringement in the use of this standard.

Published by

American National Standards Institute, Inc.
25 West 43rd Street, New York, NY 10036

Printed in the United States of America

Contents

Page

Figure

Tables

Foreword (This foreword is not part of American National Standard INCITS 381-2009.)

This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.

This document contains three annexes. Annex A, which is considered part of this standard, is normative and describes image quality requirements specified by the image acquisition settings. Annex B is an informative annex. It provides an example of the use of this standard and is not considered part of this standard. Annex C, the Bibliography, is also informative and is not considered part of this standard.

INCITS (The International Committee for Information Technology Standards) is the ANSI recognized Standards Development Organization for information technology within the United States of America. Members of INCITS are drawn from Government, Corporations, Academia and other organizations with a material interest in the work of INCITS and its Technical Committees. INCITS does not restrict membership and attracts participants in its technical work from 13 different countries, and operates under the rules of the American National Standards Institute.

In the field of Biometrics, INCITS has established the Technical Committee M1. Standards developed by this Technical Committee have reached consensus throughout the development process and have been thoroughly reviewed through several Public Review processes. In addition, this American National Standard has been approved by the INCITS Executive Board and ANSI Board of Standards Review for Publication as an ANSI-approved INCITS Standard.

Requests for interpretation, suggestions for improvement or addenda, or defect reports are welcome. They should be sent to InterNational Committee for Information Technology Standards (INCITS), ITI, 1101 K Street, NW, Suite 610, Washington, DC 20005.

This standard was processed and approved for submittal to ANSI by INCITS. Committee approval of this standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, INCITS had the following members:

Don Wright, Chair
Jennifer Garner, Secretary

Organization Represented	*Name of Representative*
Adobe Systems, Inc.	Scott Foshee
	Steve Zilles (Alt.)
AIM Global, Inc.	Dan Mullen
	Charles Biss (Alt.)
Apple Computer, Inc.	Kwok Lau
	Helene Workman (Alt.)
	David Singer (Alt.)
Distributed Managment Task Force	Tony DiCenzo
	Jeff Hilland (Alt.)
	Winston Bumpus (Alt.)
Electronic Industries Alliance	Edward Mikoski, Jr.
EMC Corporation	Gary Robinson
Farance, Inc.	Frank Farance
	Timothy Schoechle (Alt.)
Google	Zaheda Bhorat
	Robert Tai (Alt.)

Organization Represented	*Name of Representative*
GS1 US	Ray Delnicki
	Frank Sharkey (Alt.)
	James Chronowski (Alt.)
	Mary Wilson (Alt.)
Hewlett-Packard Company	Karen Higginbottom
	Paul Jeran (Alt.)
IBM Corporation	Ronald F. Silletti
	Robert Weir (Alt.)
IEEE	Judith Gorman
	Terry DeCourcelle (Alt.)
	Bill Ash (Alt.)
	Jodie Haasz (Alt.)
	Bob Labelle (Alt.)
	Susan Tatiner (Alt.)
Intel	Philip Wennblom
	Dave Thewlis (Alt.)
	Grace Wei (Alt.)
	Steven Balogh (Alt.)
Lexmark International	Don Wright
	Dwight Lewis (Alt.)
	Paul Menard (Alt.)
Microsoft Corporation	Jim Hughes
	Dave Welsh (Alt.)
	Mark Ryland (Alt.)
National Institute of Standards & Technology	Michael Hogan
	Elaine Barker (Alt.)
	Dan Benigni (Alt.)
	Fernando Podio (Alt.)
	Teresa Schwarzhoff (Alt.)
	Wo Chang (Alt.)
Oracle Corporation	Donald R. Deutsch
	Jim Melton (Alt.)
	Michael Kavanaugh (Alt.)
	Peter Lord (Alt.)
	Toshihiro Suzuki (Alt.)
	Jeff Mischkinsky (Alt.)
Purdue University	Stephen Elliott
Storage Networking Industry Association (SNIA)	Gary Phillips
	Rick Bauer (Alt.)
	Arnold Jones (Alt.)
	Dave Thiel (Alt.)
US Department of Defense	Jerry Smith
	Dennis Devera (Alt.)
	Dave Brown (Alt.)
	Leonard Levine (Alt.)
US Department of Homeland Security	Peter Shebell
	Gregg Piermarini (Alt.)

Technical Committee M1, Biometrics, which reviewed this standard, had the following members:

Fernando Podio, Chair
Steve Elliott, Vice-Chair for Membership and Ballots
Wayne Kyle, Vice-Chair for Administrative Affairs
Catherine Tilton, International Representative

Organization Represented	*Name of Representative*
Aoptix Corporation	Dan Potter
Authenti-Corp	Valorie Valencia
Aware	David Benini
Bion	John Campbell
Cogent Systems	Anne Wang
Crossmatch	Greg Cannon
CSC	Richard Lazarick
DAON	Cathy Tilton
EDS	Jeff Stephens
Fujitsu	Jonathan Agre
ID Technology Partners	Fred Herr
International Biometric Group	Michael Theime
L-1	Tim Brown
Morpho	Ramon Reyes
NBSP	Ryan Triplett
	Dominique Harrington (Alt.)
NIST	Patrick Grother
Noblis	Larry Nadel
OSS Nokalva	Allesandro Triglia
Purdue University	Eric Kukula
	Michael Frick (Alt.)
	Stephen Elliot (Alt.)
Recognition Systems	Samir Tamer
Retica Systems	Nicholas Accomando
Safe Skies	Anthony McInturff
Sonovation, Inc.	Omid Jahromi
UL	Lou Chavez
Unisys	Steve Vican
UPEK	Mike Chaudoin
U.S. Department of Defense - Biometric Task Force	Mike Ko
	Dale Hapeman (Alt.)
U.S. Department of Homeland Security	Charles Kelley
	John Neumann (Alt.)
U.S. Department of Justice - FBI	Michael McCabe
U.S. Department of State	Barry Kefauver
Y-12 National Security Complex	David Speaks

Task Group M1.3 on Biometric Data Interchange Formats, which developed this standard, had the following members:

Greg Cannon, Chair
Patrick Grother, Vice-Chair
John Mayer-Splain, Secretary

Organization Represented	*Name of Representative*
AOptix	Dan Potter
	Mark Fredrikson (Alt.)
Aware, Inc.	David Benini
Bearing Point	Bart Elberg
	Ron Sutton (Alt.)
Cogent Systems, Inc.	Anne Wang
	Xian Tang (Alt.)
CSC	Rick Lazarick
	Dan Munyan (Alt.)
CrossMatch	Greg Cannon
	James Cambier (Alt.)
Daon	Cathy Tilton
	Matt Swayze (Alt.)
Fujitsu	Jon Agre
	Gerry Byrnes (Alt.)
Iritech	Daehoon Kim
	Travis Jaeger (Alt.)
L1	Tim Brown
	Kirsten Nobel (Alt.)
	Udo Mahlmeister (Alt.)
LG Electronics	Jun Hong
	Samir Shah (Alt.)
Motorola	Artour Karaguizian
	Guy Cardwell (Alt.)
NIST	Elham Tabassi
	Patrick Grother (Alt.)
	Michael Hogan (Alt.)
Noblis	Donald D'Amato
	Larry Nadel (Alt.)
Purdue University	Shimon Modi
	Stephen Elliot (Alt.)
Recognition Systems, Inc.	Samir Tamer
Retica Systems, Inc.	Nick Accomando
	Tosa Yasonari (Alt.)
Sagem Morpho, Inc.	John Douglas
	Ramon Reyes (Alt.)
Sonovation, Inc.	Omid Jahromi
United States Dept. of Defense - BTF	Gregory Zektser
	Robert Yen (Alt.)
United States Dept. of Homeland Security	John Mayer-Splain
	Brad Wing (Alt.)
United States Dept. of Justice - FBI	Thomas Callahan
	Michael McCabe (Alt.)
Voice XML Forum Liaison	Judith Markowitz

Introduction

This standard is one of a family of American National Standards being developed by INCITS that support interoperability and data interchange among biometrics applications and systems. This family of standards specifies requirements that solve the complexities of applying biometrics to a wide variety of personal recognition applications, whether such applications operate in an open systems environment or consist of a single, closed system. Open systems are built on standards-based, publicly defined data formats, interfaces, and protocols to facilitate data interchange and interoperability with other systems, which may include components of different design or manufacture. A closed system may also be built on publicly defined standards, and may include components of different design or manufacture, but inherently has no requirement for data interchange and interoperability with any other system.

Biometric data interchange format standards and biometric interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment. The INCITS biometric standards family includes a layered set of standards consisting of biometric data interchange formats and biometric interfaces, as well as application profiles that describe the use of these standards in specific application areas.

The biometric data interchange format standards specify biometric data interchange records for different biometric modalities. Parties that agree in advance to exchange biometric data interchange records as specified in a subset of the INCITS biometric data interchange format standards should be able to perform biometric recognition with each other's data. Parties should also be able to perform biometric recognition even without advance agreement on the specific biometric data interchange format standards to be used, provided they have built their systems on the layered INCITS family of biometric standards.

The biometric interface standards include the Common Biometric Exchange Formats Framework (CBEFF) and the Biometric Application Programming Interface (BioAPI). These standards support exchange of biometric data within a system or among systems. The CBEFF standard specifies the basic structure of a standardized Biometric Information Record (BIR) which includes the biometric data interchange record with added metadata, such as when it was captured, its expiry date, whether it is encrypted, etc. The BioAPI standard specifies an open system API that supports communications between software applications and underlying biometric technology services. BioAPI also specifies a CBEFF BIR format for the storage and transmission of BioAPI-produced data.

The biometric application profile standards facilitate implementations of the base standards (e.g., the INCITS biometric data interchange format and biometric interface standards, and possibly non-biometric standards). These profile standards define the functions of an application (e.g., Biometrics-Based Verification and Identification of Transportation Workers, Biometric-Based Personal Identification for Border Management, Point-of-Sale Biometric-Based Verification and Identification) and then specify use of options in the base standards to ensure biometric interoperability.

In the forensic community, the capture and transmission of fingerprint images has been a common choice for the exchange of fingerprint information used by Automatic Fingerprint Identification Systems (AFIS) for the identification of individuals. In the past there was a general lack of agreement between vendors on the amount and type of information to capture, the method of capture, and the information to be exchanged.

This standard is intended for those applications requiring the exchange of raw or processed fingerprint images that may not necessarily be limited by the amount of resources required for data storage or transmitting time. It can be used for the exchange of scanned fingerprints containing detailed image pixel information. The standard can also be used to exchange processed fingerprint image data containing considerably fewer pixels per inch and/or a lesser number of greyscale levels. This is in contrast to the standard formats used for exchanging lists of fingerprint characteristics such as minutiae, patterns, or other variants. These formats require considerably less storage than a fingerprint image. However, by using any of these formats, information recorded in one standard format cannot be used by algorithms designed to operate with another type of information. In other words, minutiae data cannot be used by pattern matching algorithms and pattern data cannot be used by minutiae matching algorithms.

Although the minutiae, pattern, or other approaches produce different intermediate outputs, all must initially capture a reasonably high quality fingerprint image before reducing the size of the image (in bytes) or developing a list of characteristic data from the image. Use of the captured or processed image can provide interoperability among vendors relying on minutiae-based, pattern-based or other algorithms. As a result, data from the captured finger image offers the developer more freedom in choosing or combining matching algorithm technology. For example, an enrollment image may be stored on a contactless chip located on an identification document. This will allow future verification of the holder of the document with systems that rely on either minutiae based or pattern based algorithms. Establishment of an image-based representation of fingerprint information will not rely on pre-established definitions of minutiae, patterns or other types. It will provide implementers with the flexibility to accommodate images captured from dissimilar devices, varying image sizes, resolutions, and different grayscale depths. Use of the fingerprint image will allow each vendor to implement their own algorithms to determine whether two fingerprint records are from the same finger.

American National Standard
for Information Technology –

Finger Image Based Data Interchange Format

1 Scope

This standard specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas. This standard can be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with this standard can be recorded on machine-readable media or may be transmitted by data communication facilities.

2 Conformance

A system conforms to this standard for producing data interchange records if it satisfies the mandatory and implemented optional requirements herein for encoding and decoding finger image data and the associated parameter data as specified by Clauses 6 through 8. A system conforms to this standard for using data interchange records if it can parse data interchange records that conform to Clause 8. A data record conforms to this standard if it satisfies the mandatory, and optional, if implemented, requirements for structure and content as specified in Clause 8.

3 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ANSI INCITS 398-2008, *Common biometric exchange formats framework (CBEFF)*

ANSI/NIST-ITL 1-2007, *Information systems – Data format for the interchange of fingerprint, facial, & other biometric information*

IAFIS-IC-0110 (V3), *WSQ Gray-scale fingerprint image compression specification* 1997

IAFIS-Doc-01078-8.002, *Electronic biometric transmission standard (EBTS)* April 1, 2008

ISO 10918-1:1994, *Information technology – Digital compression and coding of continuous-tone still images – Part 1: Requirements and guidelines* (Commonly referred to as JPEG.)

ISO 15444:2004, *Information technology – JPEG 2000 image coding system: Core coding system* (Commonly referred to as JPEG 2000.)