International Journal of Computer and Communication Technology

Volume 5 | Issue 1 Article 2

January 2014

Standardized Biometric Templates in Indian Scenario: Interoperability Issues and Solutions

Zia Saquib
Executive Director, C-DAC Mumbai & Elec. City, saquib@cdac.in

Santosh Kumar Soni
Sr. Staff Scientist, Biometrics Division, C-DAC, santoshsoni@cdac.in

Sweta Suhasaria
Project Engineer, Biometrics Division, C-DAC, swetas@cdac.in

Anamika Singh
Senior Technical Associate, Biometrics Division, C-DAC, anamika@cdac.in

Recommended Citation

Saquib, Zia; Soni, Santosh Kumar; Suhasaria, Sweta; and Singh, Anamika (2014) "Standardized Biometric Templates in Indian Scenario: Interoperability Issues and Solutions," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 1 , Article 2.
DOI: 10.47893/IJCCT.2014.1212
Available at: https://www.interscience.in/ijcct/vol5/iss1/2

Standardized Biometric Templates in Indian Scenario: Interoperability Issues and Solutions

Zia Saquib
Executive Director,
C-DAC Mumbai & Elec. City
saquib@cdac.in

Santosh Kumar Soni
Sr. Staff Scientist,
Biometrics Division, C-DAC
santoshsoni@cdac.in

Sweta Suhasaria
Project Engineer,
Biometrics Division, C-DAC
swetas@cdac.in

Anamika Singh
Senior Technical Associate,
Biometrics Division, C-DAC
anamika@cdac.in

ABSTRACT

The compelling need for establishing the identity of a person is becoming critical in our vastly interconnected society. Biometrics is beginning to gain wide acceptance as a legitimate method for determining an individual's identity in India. Minutiae features extracted from fingerprint images are widely used for automated fingerprint recognition. The conformance of minutiae templates to standardized data interchange formats and the interoperability of minutiae extraction and comparison subsystems from multiple suppliers are important to prevent proprietary lock-in. Further, just by achieving vendor-neutral fingerprint biometric templates, doesn't guarantee seamless integration and exchange of information amongst different government agencies in India, viz., Aadhaar-enabled citizen services/applications, Seafarers' Identity Cards (ILO-SID) of DG Shipping, State-police AFISs (Automated Fingerprint Identification Systems) etc. One of the key reasons to this interoperability issue is the existence of multiple international standards for generation of minutiae-based fingerprint templates, which are primarily not interoperable.

This paper focuses on conformance and interoperability issues that are likely to arise at the time of integration of such virtually isolated govt. agencies, specifically, in applications like, conducting nation-wide criminal background checks, de-duplication of data, etc. The paper further proposes viable solutions to address these issues.

I. INTRODUCTION

In a fingerprint biometric system, the fingerprint capture subsystem captures a fingerprint image of a subject through a sensor, and outputs this raw image as a biometric sample. The digital image processing subsystem of the system extracts the distinguishing features from a biometric sample. This typically involves quality checks, enhancement, segmentation and feature extraction to ensure that the extracted features are likely to be distinguishing and repeatable. If quality check rejects the received sample/s, control returns to the data capture subsystem to collect a further sample/s. In the case of enrolment, the image processing subsystem creates a template from the extracted biometric features. The templates are stored within an enrolment database held in the data storage subsystem. Each template is associated with details of the enrolled subject. It should be noted that prior to being stored in the enrolment database, templates may be re-formatted into the specified biometric data interchange formats, i.e., standardized templates. Templates may be stored within a personal computer or in a central database. In the matching subsystem, the features from the query template are compared against one or more templates and similarity scores are passed on to the decision subsystem. The similarity scores indicate the degree of fit between the features and template/s compared. The system uses the score to declare, as per the decision policy, the case a Match/Non-Match.

In general, for finger minutiae data, the standardized fingerprint biometric templates remain in one of the following leading standards:

1. **ISO/IEC 19794-2:2005 (Information technology - Biometric data interchange formats - Part 2: Finger minutiae data):** It provides for interchange of finger minutiae data between sensing, storage and matching systems [3].
2. **ILO SID Standards (Standard adopted under the Seafarers' Identity Documents Convention (Revised) (No. 185), 2003):** Finger minutiae-based biometric profile for seafarers' identity documents, wherein, minutiae-based fingerprint biometric technology is incorporated into the SID in accordance with the Seafarers' Identity Documents Convention (Revised), 2003 (No.185) [5][6].
3. **ANSI/NIST-ITL 1-2007 (Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1) Type-9:** Type-9 records contain ASCII text describing minutiae and related information encoded from a finger [4].

As these standards are not interoperable among themselves, seamless data exchange across agency boundaries remains a goal rather than a reality. The present paper describes such interoperability issues and presents a template conversion scheme for improving access and information sharing amongst different government agencies within country.

II. STANDARDS FOR FINGER MINUTIAE DATA: INDIAN SCENARIO

To effectively exchange identification data across jurisdictional lines or between dissimilar systems implemented by different manufacturers/vendors, a standard was needed to specify a common format for the data exchange. To this end, various national/regional/international standards were developed.

The Indian government has specific present/future requirements to use fingerprints for residence permits and other civil services (most of them will be Aadhaar-enabled), travel documents (like, ILO-SID for Indian Seafarers'), Criminal services (ex: State-police AFISs) etc. Consequently, there is an urgent need to ensure the interoperability of fingerprint biometrics within country across heterogeneous systems, as shown in Figure 4. Following are the target standards, which are subject matters of this paper:

A. ISO/IEC 19794 Part 2 (ISO/IEC 19794-2: 2005)

This standard specifies a concept and data format for representation of fingerprints using the fundamental notion of minutiae. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. The standard contains definitions of relevant terms, a description of where minutiae shall be defined, a data format for containing the data, and conformance information. This standard defines "Finger Minutiae Record format", "Normal size Finger Minutiae Card format", and "Compact size Finger Minutiae Card format". However, these formats have different resolution in minutiae coordinates and direction angle. In addition, the information involved in the card format is limited. Furthermore, in the format, the fields of additional information such as fingerprint image size and minutiae quality value is not included. It is easily expected that these differences influence automated fingerprint authentication accuracy in conversion process.

The ISO/IEC 19794-2 (FMR) and ISO/IEC 19794-4 (FIR) data formats are primarily adopted as national eGovernance and Aadhaar standards. Aadhaar, the world's largest identity platform, is all set to transform how Government and Enterprises across various verticals identify and authenticate citizens and customers for various services [10][11]. So, most of the existing/futuristic civil services are going to be based on ISO (FMR) standards.

B. ILO-SID

In June 2003, the ILO (International Labour Office) adopted the Seafarers' Identity Documents Convention (Revised), 2003 (No. 185), which is a revision of the earlier Convention of 1958. The new ILO Convention was communicated to the governments of ILO Members for their consideration with a view to ratification. It will become binding, as an international treaty, on all Members that ratify it [5].

Like many other countries, Directorate General of Shipping (DG-S), Govt. of India, too aims to issue Biometric ID cards to the Indian Seafarers', as a measure to prevent acts of terrorism that threaten the security of passengers, crews and the safety of ships. The strict adherence of SID to Seafarers' Identity Documents (SID) Convention (Revised), 2003 (No. 185) will ensure the interoperability of the cards amongst all the ports (port area only) across the globe. SIDs de-duplication will be ensured through nationwide background screening (over a 24x7 national electronic database), with a possibility of an extension to conduct criminal background checks too in future. Digitally signed or encrypted BIR (Biometric Information Record) will ensure the biometric data security. The ILO-SID has basically adopted ISO/IEC NC standard (Normal size Finger Minutiae Card format).

C. ANSI/NIST-ITL 1-2007 (Type-9)

This standard, in totality, defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, scar mark & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images [4]. Specifically, Type-9 records contain ASCII text describing minutiae and related information encoded from a finger.

Crime records play a vital role in the scheme of police working for prevention and detection of crime. The Indian Police, over the years, have sought to improve the efficiency of the crime records systems to discharge their responsibilities with greater efficiency and effectiveness. However, in the context of Fingerprint Identification System, the AFIS installed in different states have certain issues involved with them:

1. State-AFIS are from different vendors. Most of them have proprietary templates (encoding) & matching algorithms, and thus they lack commonality & interoperability.
2. Such non-interoperable systems further result in integration issues while making attempts to integrate them with other police applications.
3. Lack of inter-state/inter-AFIS connectivity module and functionality, etc.

Though government has taken several excellent initiatives and brought many incredible projects into reality, these state-AFIS are still not well-connected and appear to be isolated islands. Thus, they all need be wired together to the NCRB (National Crime Records Bureau) through state-of-the-art infrastructure and a common set of standards to be followed by all states, with an easy extension for further connectivity and transactions with

INTERPOL, as shown in Figure 1 [8]. The existing/preferred standard is ANSI/NIST-ITL 1-2000/2007 or higher.

III. INTEROPERABILITY ISSUES WITH STANDARDS FOR FINGER MINUTIAE DATA

The problems and influence on the authentication accuracy of the system in accepting the data formats in ISO/IEC 19794-2 (Record Format, Normal Size Card Format, and Compact size Card Format) and ANSI/NIST-ITL 1-2007 were examined in [1]. From experimental results, as in [1], the EERs (Equal Error Rates) of the ISO/IEC 19794-2 formats become slightly worse than that of the ANSI/NIST format. The degradation of EERs of the Record format, Card format (Normal size), and Card format (Compact size) are 0.1%, 0.1%, and 0.77% respectively.

Key Problems Noticed in Converting Finger Minutiae Formats with respect to ISO/IEC 19794-2, ILO-SID and ANSI/NIST-ITL 1-2007 Type-9:

- Security agencies, in general, follow ANSI/NIST standards, whereas, national eGovernance and Aadhaar follows ISO/IEC 19794 (Part 2 and Part 4) standards.
- ILO-SID is a special case of ISO "Normal Size Card Format" with a different header structure than ISO.
- In ILO-SID, there is a limitation with respect to the number of maximum minutiae extracted from the fingerprint image that are captured in conversion and authentication processes.
- The origin of the coordinate system of the ISO/IEC19794-2 and ILO-SID formats is the upper left corner of the original image with X increasing to the right and Y increasing downward. In contrast, the origin of the ANSI/NIST format is the lower left corner.
- In ANSI/NIST, the angle of minutiae direction has the highest resolution: from 1° to 360°, whereas, in ISO/IEC19794-2 and ILO-SID formats, it is 1.40625° (360/256). So, there remains a conversion error caused by converting from 1° to 1.40625°.
- The number of bytes allocated for the storage of one minutia in ISO/IEC19794-2 is 6 bytes (binary), whereas, in ILO-SID, it is 5 bytes (binary). For ANSI/NIST, the field type is ASCII/Text and not binary.

As per the definition of the angle θ of minutia direction of each format, the resolution of the angle is same in ISO & ILO-SID formats, whereas, it is different in ANSI/NIST format. Therefore, as compared to ANSI/NIST, the ISO/IEC19794-2 and ILO-SID formats have errors in the angle conversion.

IV. PROPOSED SOLUTION

The standard fingerprint templates represent the fingerprints in a compact and interoperable manner. There are several international/regional/national standards available for fingerprint representation in an automated system. As per current scenario in our country, few of them are discussed in Sec. II. In order to make these standards interoperable, the paper proposes a solution, wherein, the standardized fingerprint templates from one disjoint system/agency are intercepted in-between by the template conversion routine for inter-conversion to the desired format specified by the intended recipient agency, as shown in Figure 2, 3 and 5. This intermediate inter-conversion scheme will positively improve the information sharing amongst the different govt. establishments in India.

This novel fingerprint template converter allows conversion of biometric templates from one standardized format to another, viz. ISO/IEC 19794-4:2005 (FIR: Finger Image Record), ISO/IEC 19794-2:2005 (FMR: Finger Minutiae Record), ANSI/NIST-ITL 1-2007 Type-9 templates, ILO-SID, ANSI/INCITS 378-2004, etc. as shown in Figure 6, 7 and 8. It also supports various image compression algorithms, like: JPEG 2000, PNG, JPEG, are few among others. The fingerprint template converter has a flexible or configurable workflow, like: support for FMR template generation with and without extended dataset etc.

V. CONCLUSION

By bringing the varied biometric-enabled services, viz. de-duplication of Seafarers' identity documents, Criminal and Civil services to one roof of Aadhaar will definitely result in significant improvement in identifying fake and ghost identities, increased solved crimes, inclusion of those without any existing identity documents, improved services through increased transparency, etc.

Seamless and transparent access to such services can only be made possible by making the underlying standards for biometric data interchange formats (for finger minutiae data) interoperable. This would mandate the frequent inter-conversions amongst the dissimilar systems/domains. Such inter-conversions can be achieved through carefully designed plugged-in biometric template converters/routines.

Though such an approach is still in nascent stages in India, in near future, similar unified and monolithic online biometric authentication/identification systems will become a necessity, and thus, a de facto standard for trusted and transparent mean of civil/criminal authentication.

KEY REFERENCES

[1] Takahiro YOSHIDA , Seiichiro HANGAI, "A Study on Accuracy and Problems in using ISO/IEC 19794-2 Finger Minutiae Formats for Automated Fingerprint Verification (IBPC 2010)", Mar. 2010.

[2] Bazin A. and Mansfield T., "An Investigation of Minutiae Interoperability, In 5th IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2007)", Alghero, Italy, June 2007.

[3] International Standard ISO/EC 19794-2:2005, Information technology - Biometric data interchange formats - Part 2: Finger minutiae data (Committee Drafts).

[4] Standard ANSI, Information systems - Data Format for the Interchange of Fingerprint, Facial, and Scar Mark & Tattoo (SMT) Information, 2007.

[5] ILO SID-0002 – Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents (ILO SID-0002)

[6] ILO seafarers' identity documents biometric testing campaign report, Part I. ILO, 2004.

[7] Standard ANSI INCITS 378:2004, Information technology – Finger minutiae format for data interchange.

[8] Soni Santosh Kumar , Saquib Zia, Sharma Purushottam (IGP, SCRB, MP Police), "Aadhaar-enabled Biometric Authentication/Identification Scheme for Unifying Citizen Services and National Security", International Conference on "Indian Biometric Scenario - Realisation of Opportunity, Experience of UID India", New Delhi, 20-22 Sep. 2011.

[9] http://www.ilo.org/global/lang--en/index.htm

[10] http://uidai.gov.in/images/FrontPageUpdates/aadhaarhandbookver1.2.pdf

[11] http://uidai.gov.in/

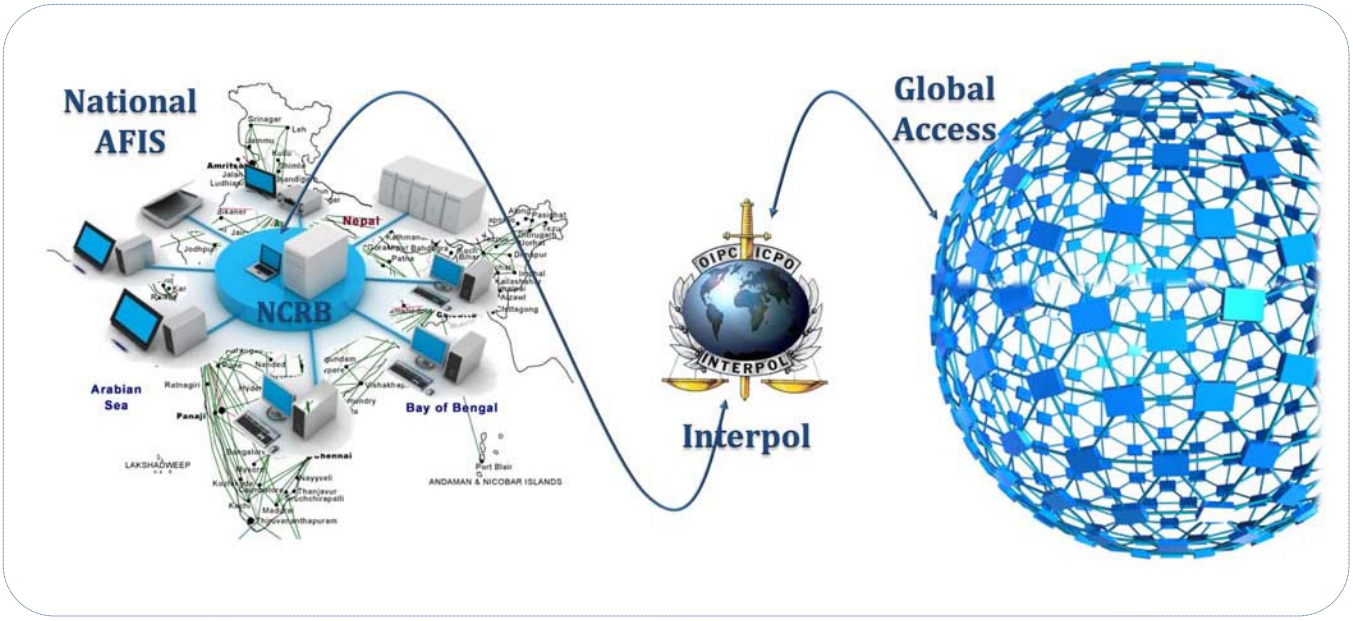

Figure 1. State-AFIS wired to NCRB, connected further to INTERPOL.

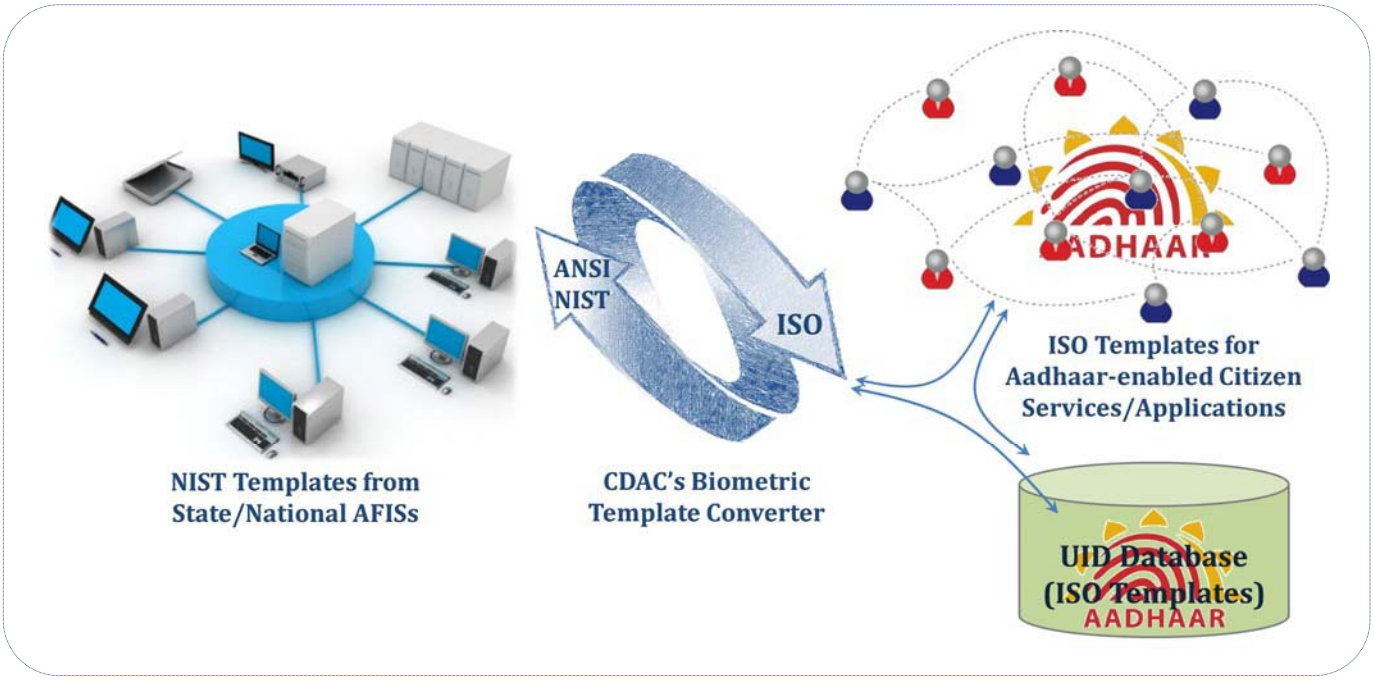

Figure 3. C-DAC's Fingerprint Template Converter: ANSI/NIST to ISO.

Figure 4. C-DAC's Fingerprint Template Converter: ISO NC to ISO.

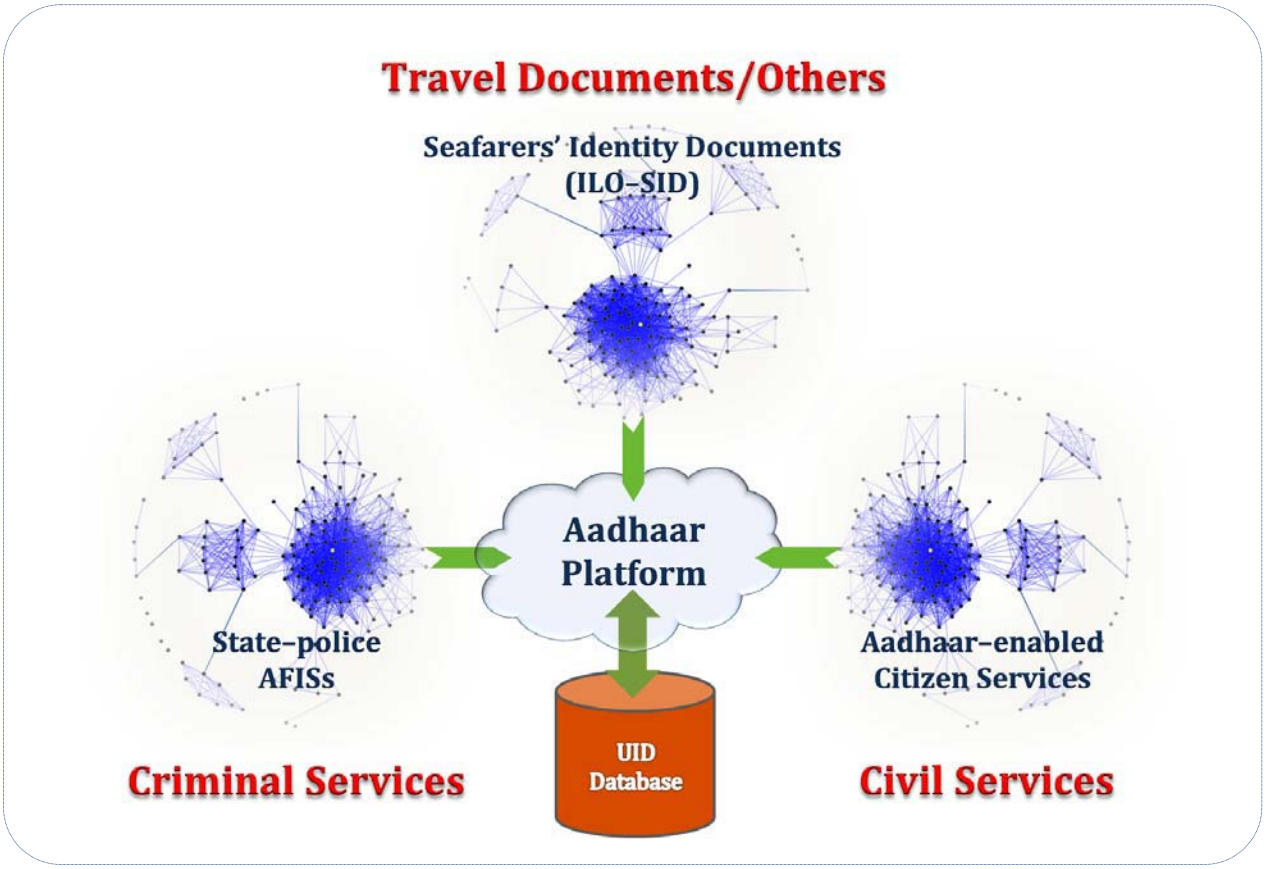

Figure 4. Integration of Virtually Isolated/Dissimilar Systems within the Country.

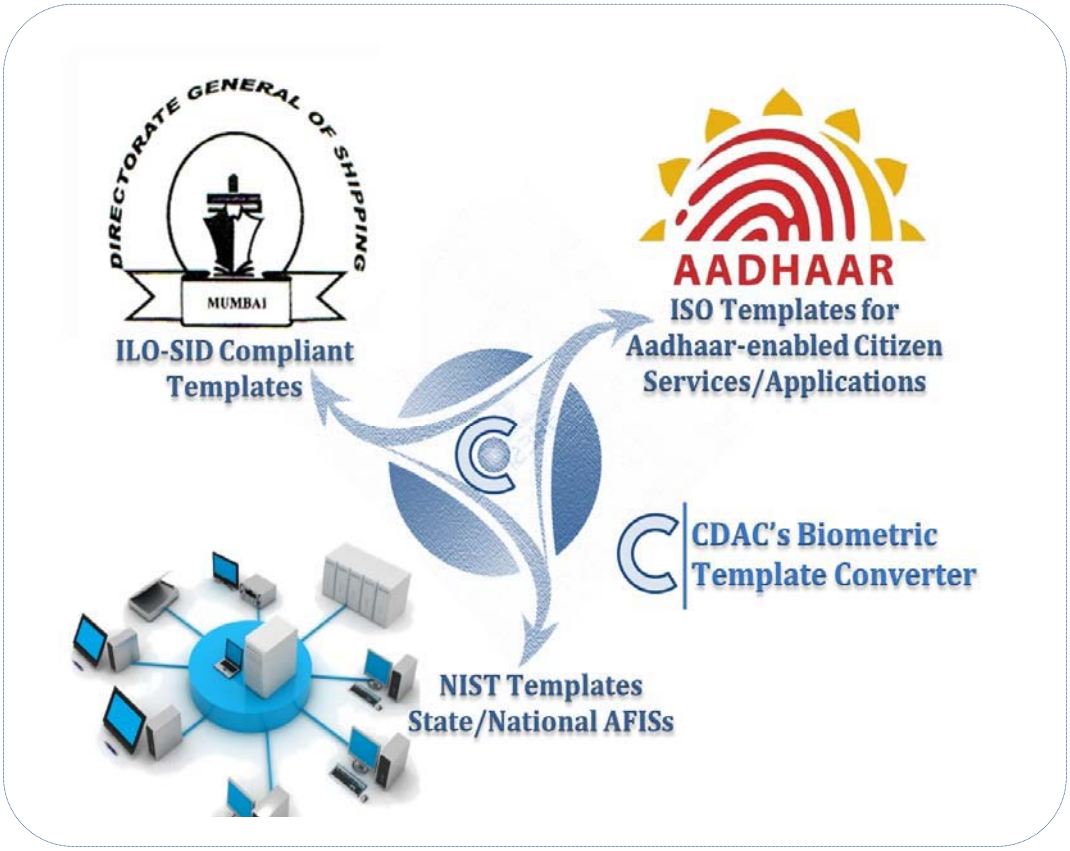

Figure 5. C-DAC's Converter for Inter-conversion of the above Fingerprint Biometric Standards.

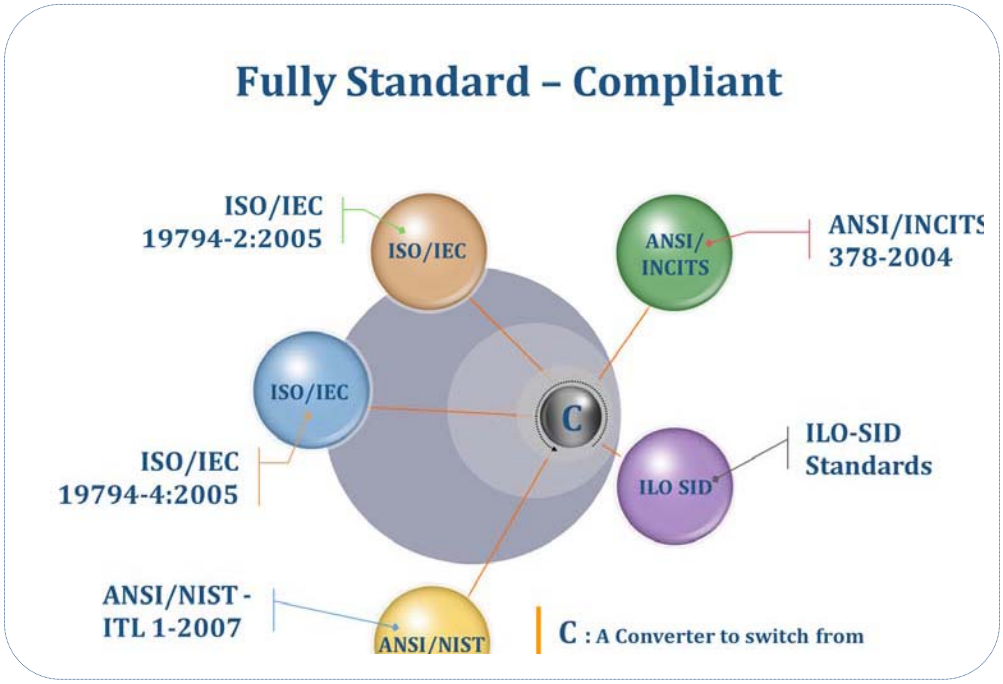

Figure 6. C-DAC's Converter: Supported Fingerprint Biometric Standards.

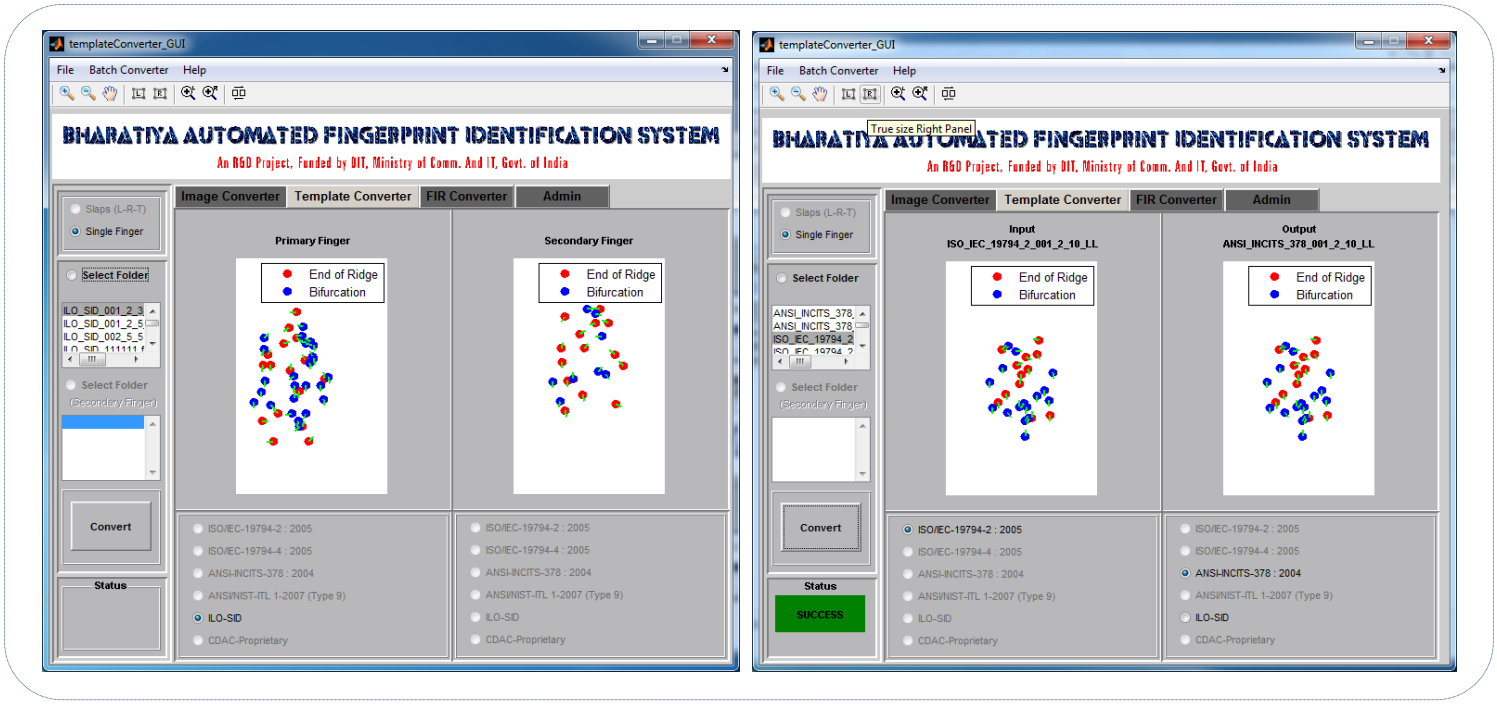

Figure 7. Fully Functional C-DAC's Converter.

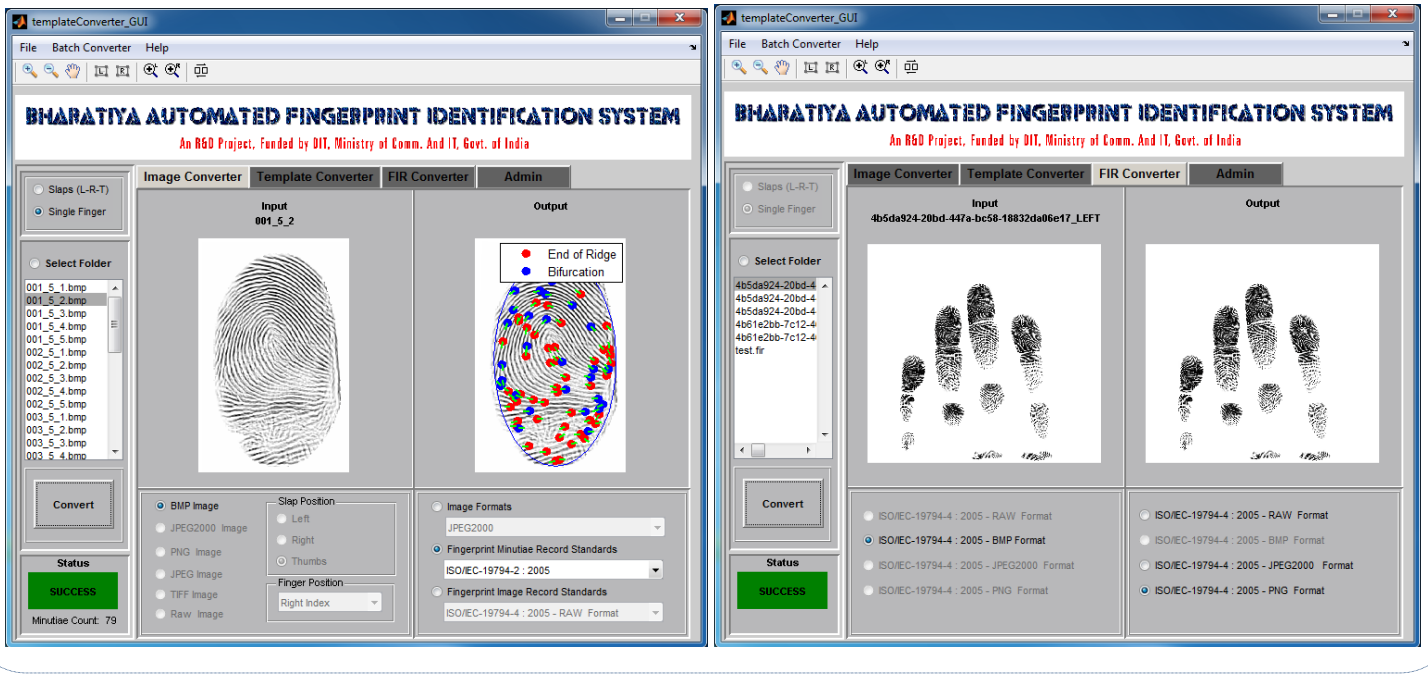

Figure 8. Fully Functional C-DAC's Converter.