NATO Automated Biometric Identification System (NABIS)

Bogdan R. NICULESCU and Cristian COMAN

***Abstract*—The NATO Nations endorsed the concept of biometrics data in support to operations. To accelerate the development of interoperability in this domain, a reference biometrics research which could be used in trials and exercises has been developed under the Defence Against Terrorism Programme of Work. Both an overview of the biometrics domain from NATO perspective and analysis of requirements for an automated biometric identification system, are presented in this document. NABIS implemented STANAG 4715 which is a valid mechanism for achieving a high degree of interoperability in the biometrics domain, even if the standard and the related documentation need enhancement particularly in areas relevant to military operations. The aim of this paper is to present a review of the work performed in the development of the NABIS product development.**

***Index Terms*—Biometrics, NATO, ABIS, PING and RING, Interchange System, STANAG 4715.**

I. INTRODUCTION

An overview of the implementation of the NATO Automated Biometric Identification System (NABIS) that was developed as part of the Defence Against Terrorism Program of Work (DAT POW), managed by the Emerging Securities Challenges Division (ESCD) under NATO HQ is presented in this document. The NABIS capability was requested and authorized by the NATO Biometrics Program of Work Coordination Group, mainly to support the interoperability demonstrations.

The paper contains an overview of biometrics concept and tools that were considered in the NABIS analysis and design phase. Biometrics information such as face, fingerprint and iris can be stored and managed through NABIS. This information can be included in NABIS from raw image files or imported from standard format files produced by enrollment devices.

NABIS has been developed by using an existing NATO framework that was used in the past to develop intelligence information sharing systems such as the NATO Intelligence Toolbox. The intelligence specific functionality available in this NATO framework is also of relevance to biometrics operational capabilities.

Biometric capture and interchange in a multi-national operational environment has posed a great challenge to NATO operations. NATO has no means by which to assist the Nations to share such data in a flexible yet standard way [1].

The paper is divided into four sections. Section II provides a brief overview of the biometrics domain including biometrics modalities, matching techniques and tools. Section III provides a description of the design applied in the development of the ABIS prototype. The last section reports on results/experience collected and also makes necessary recommendations for future work.

II. BIOMETRIC TECHNOLOGIES

A. An overview of the biometrics

A large number of systems are currently available to support collection, storage, dissemination and exploitation of biometric information. Biometrically enabled solutions are becoming more and more popular in applications such as access control, personal identification and border control. In the military application areas, biometrics is seen as a practical approach to fight the threat anonymity.

Biometrics is generally and broadly defined as "*the automated recognition of individuals based on their behavioral and biological characteristics*". In this definition the term "recognition" has a broad context and includes identification [1].

The key principle behind biometrics is that any person can (almost) uniquely be associated with some of her/his biological or behavioral characteristics. These biological and behavioral characteristics are commonly referred to as biometrics modalities.

Various technologies are used to associate the biometrics modalities with the person that they belong to and also record them for later stage for verification purposes. Biometric data is collected:

- *Directly* (by enrolment)
- *Indirectly* (through exploitation of its latent forms)

The comparison (or matching) of biometric records is the core of biometrics process. Such comparison answers the question "are two records the same or indeed similar?". A high level overview of the biometrics concept in the military domain is provided in Figure 1. In this figure the main states of biometrics data are identified by:

- *The biometric subject*, who carry live data.
- *An Identity Biometric record*, which is the reference data associating the identity of a person to her/his biometrics characteristics. These records are produced through direct enrolment methods.
- *Unknown Biometric record*, which represents biometrics data collected indirectly via forensic exploitation process.

The work described in this paper was carried out under Project NAT009621 of the NCIA Programme of Work for NATO HQ ESCD DAT POW and Biometrics-Ping and Ring of the NCIA Internship with Mission nr. 104619.

B. R. Niculescu is with the Military Technical Academy, 39-49 George Coşbuc Ave., Sector 5, 050141, Bucharest, Romania (e-mail: niculescu.bogdan.romeo@gmail.com).

C. Coman is with the NATO Communication and Information Agency, Oude Waalsdorperweg 61, 2597 AK, The Hague, Netherlands (e-mail: cristian.coman@ncia.nato.int).

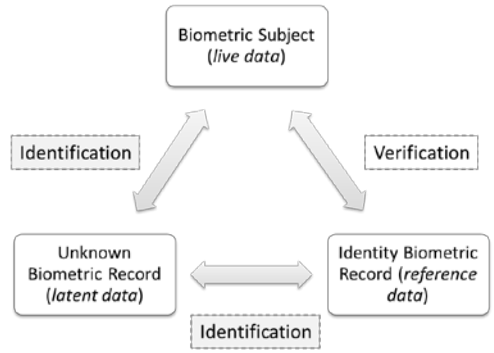


Figure 1. Overview of the biometric concept in the military domain

Verification (or authentication) and *Identification* are two key concepts used in the comparison of biometrics data. The scope of verification is to establish if a declared identity is valid. To answer this question a one-to-one comparison is used between (live subject) data that contain the identity declaration and reference data that contain a valid association between an identity and the biometric characteristics (thus yielding a one to one matching requirement without search).

In contrast the identification process tries to associate an identity to an unknown biometric record. In this case the comparison is conducted using the live sample (unknown identity) and the reference data set previously recorded (thus yielding a one-to-many matching search requirement) [2].

B. Modalities

Biometrics modalities refer to those human attributes that can be used to uniquely identify a person. Among the most popular modalities for ABIS applications are:

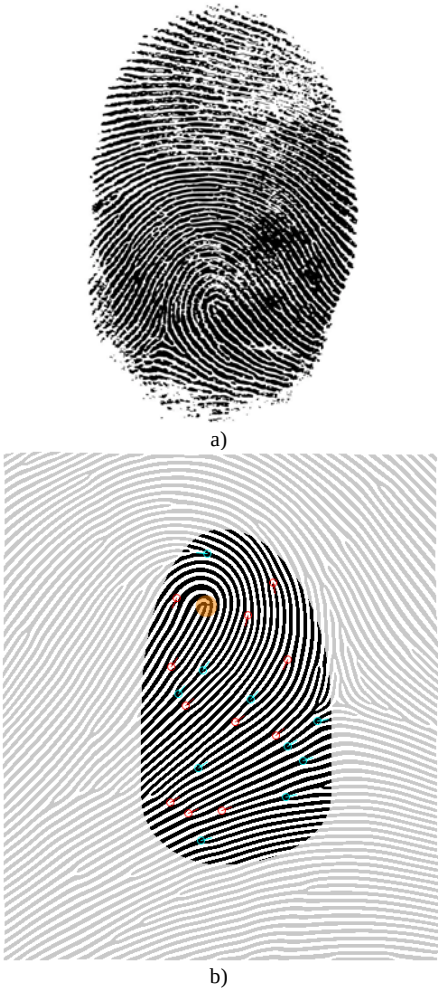
- Fingerprints
- Facial images
- Iris images
- DNA profiles
- Voice

These modalities are commonly used because they have a high probability to be unique for a given person and are relatively easy to collect and compare. Other modalities investigated in the biometrics domain include palm prints and voice. Soft modalities such as typing pattern, palm vein, gait or heart rate can also have been used in the military domain in specific scenarios.

The quality of biometric data is an important consideration that directly impacts on the performance of the matching process. Examples of biometric data with low and high quality are presented in Figure 2 for the fingerprint modality. The real test fingerprint presented in Figure 2.a. presents multiple scratches, has a high noise level and the intensity of the ridges is variable across the image (possibly due to variation of skin elasticity). All these features reduce the useful quality of this fingerprint when applied in a matching process.

An example of an ideal finger print (for matching) is presented in Figure 2.b. This image was generated using a theoretical model and some of the elements in this model are still visible in the picture. The minutiae are represented with small circles and they represent start/end or split points in the fingerprint ridge.

The quality of this theoretical print is also increased by the low noise and the fact that the ridges are uniformly distributed [2].



a)

b)

Figure 2. Fingerprints of different quality: a) real test fingerprint collected with an optical device; b) synthetic fingerprint generated using a theoretical model (capacitive sensor)

Biometrics modalities are collected using special equipment such as high resolution and infrared cameras and are stored in formats that optimize the required storage space whilst at the same time maintain a minimum quality for the data [2]. Common imagery formats such as JPEG and PNG are used for compressing biometric images.

C. Matching Techniques

Image processing provide the basis for most of the matching techniques used in the biometrics domain. These approaches are a consequence of the fact that common modalities such as fingerprints, faces and irises are collected using imaging systems.

One of the steps in the matching process is to detect the object of interest (e.g. face, iris, fingerprint) from the set of pixels containing an image. At this step it is common to use a simplified representation of the image that can be easily analyzed by computers. This simplified representation is constructed using special features that encode in a specific way the information included in the picture.

Haar-like feature are depicted in Figure 3. These types of features are used in classifiers to automatically detect and classify regions of interest in images [3].

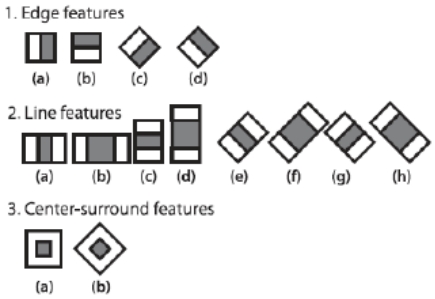


Figure 3. Haar-like features used in the face recognition applications

In case of fingerprint and iris images the image is segmented to identify features such as minutiae and circular patterns [3].

A good understanding of the matching process is essential for the correct interpretation of the results of an automated biometrics identification system. Although the matching algorithms are quite complex the general idea that should be well understood is that the results of the matching process are provided in a probabilistic sense. This observation is very important in preparing and operating ABIS systems and needs further study.

D. Tools

The collecting and processing of biometric data relies heavily upon the utilization of specialized equipment. The advances in the mobile computing technology have contributed to the expansion of biometrics into the military domain. Based on the operational utilization the equipment these tools can be grouped in three important areas, which are:

- *Enrolment devices*: used in the military operation to enroll biometric subjects in the field using three primary modalities – face, iris and fingerprint. Biometric data recorded on devices can be transferred to NABIS server where this information can be used in support of more elaborate identity exploitation activities and matching.
- *Forensic exploitation equipment*: forensic exploitation is often conducted at multiple levels and the tools used meet the requirements associated with these levels. The equipment used at *Level 1* is mainly used to collect latent biometric samples which will be transformed into biometric data record. *Level 2* and *Level 3* exploitation is conducted either at theatre level or out of theatre in specialized laboratories. Latent biometric records are developed through such exploitation and submitted to an ABIS system for storage and identification purposes [4].
- *Matching technologies*: The extent of the value added by the biometrics depends highly on the size and quality of the reference records stored into the ABIS server. Often, hundreds of thousands of biometric records are stored in operational ABIS servers. The matching algorithms are required to be able to compare a new enrolment with entire databases in real time. This previously challenging problem is being met by the modern systems and advancing over time. Two of the central server solutions analyzed in the design of NABIS are offered by *MorphoTrust* and *Neurotechnology* [5].

III. Design Consideration

A. Architecture

An overview of the design of the NATO ABIS systems is presented in this section. NABIS functionalities were thus selected to mainly support operational level and facilitate the exchange of biometrics data between Nations and at the same time to interact with the tactical level devices applied.

The architecture of the NABIS is based on NATO framework that has been used in multiple NATO intelligence tools and capabilities and enhance this framework with some new biometrics capabilities.

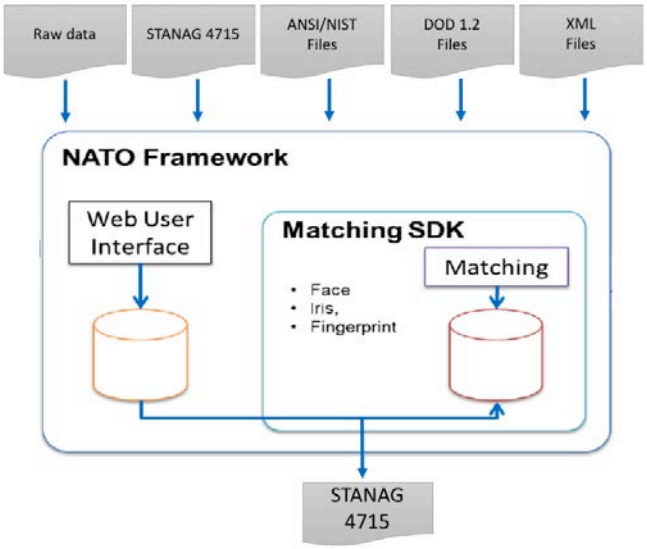


Figure 4. The NABIS Architecture

The biometric data can be received by NABIS from multiple sources, which include standard formats or simple images and store them in a local database similar to other types of intelligence information. The implementation of the biometric matching capability is based on the use of a commercial software provided by *Neurotechnology* [6]. Data stored in the NATO framework database is extended by the database of the matching engine (where the biometric templates are stored).

NABIS generates STANAG 4715 messages (within files) that can be automatically exchanged with other biometrics systems. This is an important design consideration given the broker role of NATO systems in operations.

B. Integration Framework

The NATO framework was developed in the past at the NCI Agency as a key part of the NATO Intelligence Toolbox.

The framework provides a web-based environment for storing and disseminating intelligence information. Synchronization of information across multiple databases, maintenance of links between information elements and user friendly interface are the key features which lead to the application of this NATO owned framework in the development of NABIS.

The generic user interface of the framework is depicted in Figure 5. On the left bottom side, the application area contains a few tabs representing the intelligence applications that a user has access to. Above the application switcher there is an information navigation panel where a “folder”

structure is defined to manage the records associated with a particular intelligence application. A list of records grouped on specific criteria is stored into a "folder" and displayed in the middle of the user interface. Details of the record are presented on the right hand side including a preview of the fully rendered record and a view of the metadata associated with the selected record.

Figure 5. Integration framework used to develop the NABIS prototype

On the top of this user interface a menu is available to facilitate the set-up of the system and the management of the intelligence object sets. This user interface is constructed with the assistance of database services that facilitate the actual storage of the data. An important component of this database infrastructure is the information service which facilitates the automated synchronization of information between multiple instances of the application deployed across a local or wide area network.

C. *Matching Engine*

The matching engines developed by *Neurotechnology* are used to compare biometrics records. The records are first uploaded into the NABIS as images augmented with metadata. STANAG 4715 is used to define the attributes that are associated with particular biometrics records. These records are then translated into biometrics templates and stored in the database associated with *Neurotechnology* matching engines by modality [6].

The matching engines operate on four modalities, namely: fingerprints, face, iris and voice. In the NABIS implementation only three of these modalities were tested, fingerprints, face and iris. The multimodal matching process uses these single modality engines and combines the results into a global result that is presented to the user.

The overall matching engine is constructed around a client-server architecture. The database containing templates of all recorded biometric data is installed and managed on the server side. On the client side, new records are converted to templates, which are then sent to the server for comparison with existing records, or for storage. The results of the comparison process are returned to the client as a matching score.

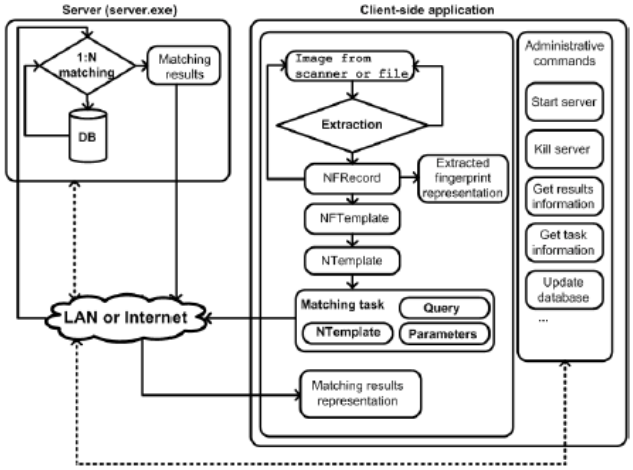


Figure 6. Flow of information in case of fingerprint matching application

An example of data flow in the case of a fingerprint matching application is presented in Figure 6. This diagram is illustrative for the client server architecture. The matching engine can also be used in developing stand-alone applications (of relevance for mobile devices used to enroll peoples) when both the reference data base and the client interface are installed on the same device. In the current NABIS implementation the client application is also a server. In the future true client applications can be developed, for example to support mobile devices that work like this.

D. *Enrollment*

Given this interoperability objective, most of the efforts were concentrated on generating STANAG compliant files from images, from records exported by the enrolment devices and from latent exploitation reports. Importing and exporting standard biometric files is another key functionality required to demonstrate the interoperability. Matching is performed using the Neurotechnology engine and therefore some data stored in NABIS had to be linked with the matching engine database as well [6]. The matching results received from the matching server are converted by NABIS into the format required by STANAG 4715 and submitted as a response to the requestor.

Biometric records are created in NABIS by combining metadata information with biometrics specific files stored as images.

STANAG 4715 defines a large set of attributes that can be stored with the biometric records. In the future developments of NABIS it would be necessary to extend the set of attributes in order to achieve a full compliance with the STANAG recommendations and that would be a more complex environment.

NABIS also offers a simple functionality to browse through the existing records on the data base and search on meta data attributes or simply through the related free text.

E. *Import/Export of STANAG 4715 files*

STANAG 4715 uses the ANSI/NIST ITL Logical Record Types to group biometric metadata as transaction entities. A STANAG compliant file contains two sections: one dedicated to subject area entities (also referred to as transaction types) and also an area reserved for biometric

intelligence reporting. Six STANAG 4715 transaction types have been implemented in NABIS [7]:

- *Type-1 Transaction Information Record*: Containing information regarding the purpose and thus operational context of transaction
- *Type-2 User-Defined Descriptive Text Record*: Contains key biometrics metadata such as identification, biographic, and descriptive, information regarding the subject of the transaction and situational information regarding the encounter.
- *Type-10 Facial, Other Body Parts and SMT Image Record*: Mainly used to exchange facial images and information.
- *Type-13 Variable-Resolution Latent Image Record*: Used for exchanging latent fingerprint image data with textual information.
- *Type-14 Variable-Resolution Fingerprint Image Record*: Contains fingerprint images and related information.
- *Type-17 Iris Image Record*: Used to exchange iris imagery and related data.

Each of these transaction types contains mandatory and optional fields. In the current NABIS implementation all the mandatory fields were implemented and the most representative ones can be controlled through the user interface.

STANAG 4715 also defines how the communication between multiple biometric systems shall be implemented in a standardized way by using these transaction types. The list of type of transactions used for submission and responses of biometric and latent enrolments is presented in Table 1. Most of these transaction types are implemented in NABIS.

TABLE I. TYPE OF TRANSACTION (TOT) SUBMISSIONS AND RESPONSES IMPLEMENTED IN NABIS [7]

ToT	Transaction Name	Notes	NABIS	
			Produce	Receive
Biometrics Enrolment Transactions				
NES	NATO Enrolment Submission	Biometric Submission for Enrolment	YES	YES
NSR	NATO Submission Result	Response containing an Identification/Non-Identification decision or status as Pending	YES	YES
NESE	NATO Enrolment Submission Error	Response in case of an error	YES	YES
Latent Enrolment Transactions				
NLS	NATO Latent Submission	Biometric Submission for Latent	YES	YES
NLR	NATO Latent Result	Response containing an Identification/Non-Identification decision or status as Pending	YES	YES
NLSE	NATO Latent Submission Error	Response in case of an error	NO	NO

F. *Transaction Structure*

NABIS transactions follow the transaction structure defined by the ANSI/NIST-ITL standards. A transaction is comprised of records containing information and biometric data concerning a particular individual (or individuals) that is stored and transmitted as a complete unit. Each record is comprised of a set of fields containing related transaction, contextual, or biometric data. An occurrence of a field is known as a subfield. Each subfield consists of one or more items used to transmit a particular datum or group of closely related data. An Item represents a single informational value and is the smallest representation of data within a transaction which may not be separated into further components [8].

Figure 7. Transaction Structure (Example)

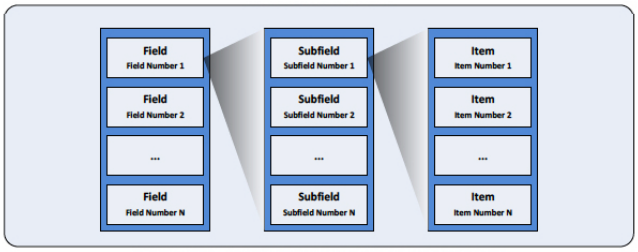


Figure 8. Record Structure (Example)

G. *Interoperability Module*

Functionality was developed in NABIS to import and export biometrics data to and from enrollment devices such as Crossmatch SEEK II, SEEK Avenger, SRI International and BIMA Kit, which do not use the STANAG 4715 fully compliant formats. Transaction files are in one of these formats: ANSI/NIST-ITL, DOD 1.2 SEEK II, EBTS, EFT, XML files in compliance with STANAG 4715.

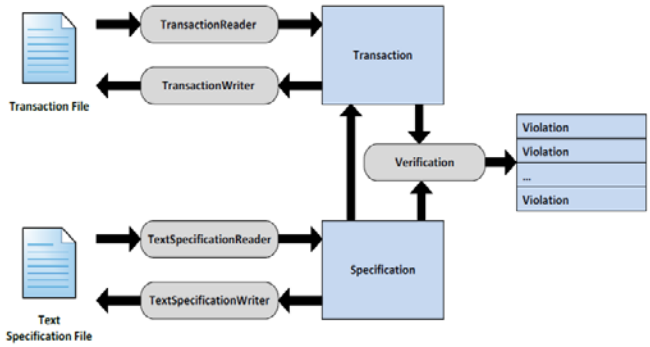


Figure 9. Interoperability Serialize/Deserialize process architecture

The popular format used is defined by the United States Department of Defense (DoD) Electronic Biometric Transmission Specification (EBTS), which is based on the American National Standards Institute (ANSI)/National Institute of Standards and Technology (NIST) Information

Technology Laboratory specification number 1-2011 (ITL 1-2011). The DoD's EBTS builds upon the ITL 1-2011 to meet DoD requirements via additions to and customizations of the ITL 1-2011 data format [9].

Although the EBTS format (.eft file extension) and STANAG 4715 are using the same core data format defined in the ANSI/NIST standard, additional effort was needed to convert data between these formats.

IV. Conclusions and Future Work

A NATO Automated Biometric Identification System (NABIS) was developed as part of the Defense Against Terrorism Program of Work (DAT POW). The capability was requested and authorized by the NATO Biometrics Program of Work Coordination Group, mainly to support the interoperability in the biometrics domain.

NCI Agency developed the NABIS system by using an intelligence application framework available within NATO and a commercial matching engine. This approach enhances the architecture interoperability of NABIS with NATO systems. NABIS has functionality to indicate if a person belongs to a biometric enabled watch list (BEWL). The commercial engine offers an integrated solution for multimodal matching of biometrics data including fingerprints, face and iris modalities. NABIS is able to read and produce enrolment/latent submission and response messages which were disseminated in accordance with predefined technical business rules.

Records can be created in NABIS from raw image information imported from a number of enrolment devices (mainly formatted in accordance with Department of Defense (DoD) Electronic Biometric Transmission Specification (EBTS)) and from STANAG 4715 files. The compliance to STANAG 4715 was verified by exchanging information with a similar ABIS system.

No formal operational concept exits for NABIS at the moment and this is mainly because of its development status. However, initial thought was given on how such a capability will be used by NATO in operations. Two use cases relevant for NABIS usage in operations are represented by:

- Storage of subsets of biometric records in specific galleries supporting specific domains under the responsibility of NATO
- Provide a transition repository that facilitates the exchange of biometrics data between Nations military and nations/international law enforcement agencies.

Of note is the fact that biometric information can also be utilised and stored in applications supporting specific communities. The biometrics information used by specialized functions can be seen as subsets of the overall biometric data that needs to be managed in support to operations.

Future development of NABIS is required to enhance the compliance with STANAG 4715 and implement functionalities relevant for biometric operations into a multinational domain.

A few additional topics that need to be considered in the future are listed in the following:

- This application framework may be assessed by functionalities associated with existing national ABIS/Intelligence architectures to ensure NABIS interface functions are useful for national intelligence purposes in particular the interface with existing ping-and-ring concepts.
- Integration of the NABIS within intelligence toolsets needs to be further investigated from an operational perspective. The transmission of data to the ABIS and the sharing of data from ABIS to other data repositories may become difficult when it is integrated directly into an intelligence toolset.
- Integration of the NABIS with an Interchange System such as PING and RING and share content with multiple ABIS systems.

References

[1] North Atlantic Military Committee, "Concept for Biometrics in Support of NATO Operations," MCM-0050-2012, 17 Sep. 2012.

[2] Nord Atlantic Treaty Organization Technical Report, TR2014, NAT009621/01, 1 Aug. 2014.

[3] Duan-Sheng Chen and Zheng-Kai Liu, "Generalized Haar-Like Features for Fast Face Detection," presented at the 2007 Machine Learning and Cybernetics International Conf., Hong Kong, China, Nov. 9–12, 2007.

[4] Alliance Joint Publication 3.15(B), "Allied Joint Doctrine for Countering-Improvised Explosive Devices," STANAG 2295, Brussels, Belgium, May 2012.

[5] Anush Sankaran, Tejas I. Dhamecha, Mayank Vatsa, and Richa Singh, "On Matching Latent to Latent Fingerprints," IIIT Delhi, India.

[6] http://www.neurotechnology.com/

[7] NATO AEDP-15, "NATO Biometrics data, Interchange, Watchlisting and Reporting," 4 Oct. 2013.

[8] Lakota Software Solution, "ANI Developer's Guide," Version 6.0, Dec. 2016.

[9] Department of Defense (DoD) Electronic Biometric Transmission Specification, "Version 4.0 Amendment 1 (DoD EBTS v4.0 Amd 1)," May 2016.