ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

The Standards in Data Structure for Biometric Applications

Girish Rao Salanke N S[1], Dr. Maheswari N[2], Shivakumar Dalali[3], Dr. Suresh L[4]

Research Scholar, Department of SCSE, VIT University, Chennai, India[1]

Professor, Department of SCSE, VIT University, Chennai, India[2]

Research Scholar, Cambridge Institute of Technology, Bangalore, India[3]

Principal, Cambridge Institute of Technology, Bangalore, India[4]

ABSTRACT: Security solutions will play an important role in diversifying the applications of IT in the future world. With the increase in the application of information technology the need for specific security solution is also increasing. The present technologies can help, but there is always a need for more enhancements. Using Biometrics as a component in security solution will play an important role. The fundamental of Biometric technology is to use god-gifted traits of a living being as security keys. There are a large number of studies and research in this area and this paper attempts to present the fundamentals involved in biometric system and an implementation framework.

KEYWORDS: Biometric, BioAPI, False acceptance Rate(FAR). False Rejection Rate(FRR)

I. INTRODUCTION

Information technology has changed the world dramatically over the past few years. People have started using computer systems at their offices, homes and are also connected to the internet round the clock. This makes them available around the world as well making them vulnerable to security attacks. The need is to identify the correct user of the information that is available either on the computer or on the network. The process of establishing the validity of the user attempting to gain access to a system is called authentication. The primary authentication methods used are mostly non biometric such as access passwords (i.e. on the basis of something the user knows) and access tokens (i.e. on the basis of something the user owns).

Biometrics is the term given to the use of biological traits or behavioral characteristics to identify an individual. The traits or characteristics are any biological characteristics like retina, DNA, fingerprints, hand, face, voice etc that are unique to each human. The use of biological characteristics provides a better and reliable way of providing authentication as they are immune to threats like stealing, forgetting, change etc as was the case with non-biometric methods.

Security solutions have been developed involving non – biometric and biometric technology. An example of such system is given by [5]. It proposes a system that uses a non-biometric method for initial authentication and uses two randomly chosen biometric methods to further establish the identity of the user. The user is given access only when he passes the entire test.

II. RELATED WORK

Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of these characters. Biometric system can work on any human physiological and / or biological characteristics as long as it satisfies the requirements of Universality, Distinctiveness, Permanence and Collectability [3]. [2] shows a comparative study of different biometric characteristics.

A Biometric system can be developed either for verification or identification of a user. In verification the user is authenticated by matching by matching his / her input biological characteristic with his / her similar previously stored characteristics in the database. In identification the system matches the input characteristics with the database to establish the identity of the person. Verification is one -- one matching whereas identification is one -- many matching.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

A biometric system could be either an online or offline. Typically on-line systems are fully automatic and the identification / verification has to done faster. The offline systems are semi-automatic and can afford have some delay in the identification or verification process. An example of online biometric system would be restricted access system (using fingerprint to usea laptop, using eye retina to enter a secured area etc.). An example of the offline biometric system would be a system identifying a criminal / terrorists.

A biometric system can operate in a positive or a negative identification mode. Both these modes require user cooperation. In a positive identification the user is interested to be identified, for example getting an access to one's own office. In the negative identification mode the user tries to avoid successful identification, for example, the thief is not interested in being identified. Here the user is not willing to cooperate hence often needs observation.

III. BASIC MODEL OF A BIOMETRIC SYSTEM

A simple biometric system broadly has four components [8]:

a) Sensor module,
b) Feature extraction module,
c) Matching module and
d) Decision-making module.

The sensor module in figure 1 contains hardware like scanner to capture the biometric characteristics. The feature extraction module extracts distinguished features of the scanned biometric characteristics, ex. the features like width of the fingers at various locations, width of the palm, thickness of the palm, length of the fingers, etc. in case of hand geometry been scanned. The matching module performs the matching of the user characteristics with the previously stored sample. The decision-making module accepts or rejects the person based on the matching module.

The Biometric recognition of any type (fingerprint, hand, retina etc) requires feature extraction and storing of biometric data / template of the user in a database. The matching module work on this stored template. This initial data template is made by collecting a number of samples with the help of devices and then extracting some pre-determined features form the samples. This process is called as registration. Matching is done with the registered users.

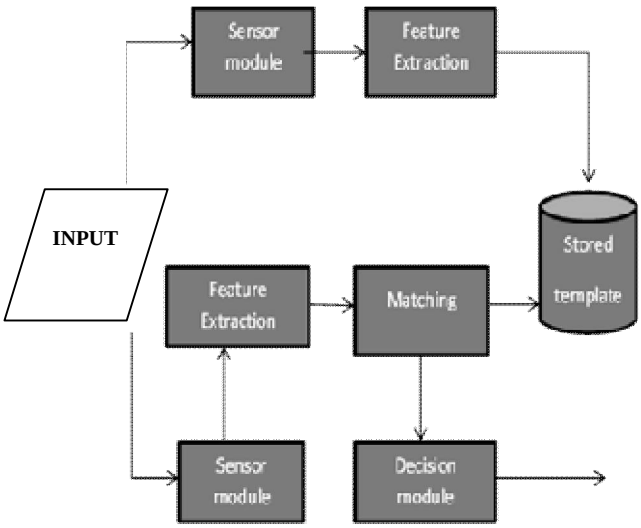

Figure 1: Basic model of a biometric system

IV. DATA STRUCTURES FOR BIOMETRIC DATA

The biometric data collected by any biometric system and application are stored in a universally accepted Common Biometric Exchange File Format (CBEFF). This format supports the interoperability and exchange of biometric data across different vendors. The CBEFF describes a common set of data structures require to support the biometric technologies. Any biometric data stored in a biometric application may use CBEFF format shown in figure 2.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Standard Biometric Header	Biometric Specific Block	Signature Block

Figure 2: CBEFF format for biometric data

The *Standard Biometric Header*contains information as biometric type, security options, id of the vendor, type specified by the format owner etc. The values of format owner are assigned and registered by the International Biometric Industry Association (IBIA), which ensures uniqueness of these values.
The *Biometric Specific memory block*contains the biometric data. This block contains either raw, intermediate or processed data that can be used for verification or identification. The *Signature Block*is optional and is used for encrypting the biometric data.
The *BioAPI consortium and X9.F4*have developed their biometric data standards based on the recommendations of CBEFF. These standards are intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology.
The BioAPI[1] consortium uses a Biometric Identification Record (BIR) to represent any biometric data (either taken as a data template to store or taken as a sample to match). The data structure provides data exchange,interoperabilityand flexibility to the vendors of biometric technology. The BioAPI Consortium has published two specifications named BioAPI v1.1 and the latest one as BioAPI 2.0. BioAPI 2.0 is the result of a series of simplifications and enhancements made to BioAPI 1.1.

The main difference [7] between the two versions of BioAPI is in the component model. The component model of BioAPI 1.1 is comprised of a framework, one or more biometric service providers (BSP's) "below" the framework, and one more applications "above" the framework. The component model of BioAPI 2.0 is similar, but there is an additional layer of components below the BSPs, called biometric function providers (BFP's). The purpose of a BFP is to take over a part of the functionality of a BSP, enabling a division of work between the two kinds of components. There are four categories of BFPs named as Sensor BFPs(responsible for managing sensors), Archive BFPs(responsible for managing access to a template database), Processing-algorithm BFPs (responsible for processing biometric samples) and Matching-algorithm BFPs.

The high level structure of the BIR remains same in BioAPI 1.1 and BioAPI 2.0 and is shown in figure 3.

Header	Biometric Data	Signature(optional)

Figure 3: BIR [BioAPI 1.1 & 2.0]

As per the BioAPI 1.1 the Header contains the field like header version, BIR data type, format owner, format ID, quality etc. The BIRs are handled using either a reference or using key value or in some cases the BIR itself. Following are the few data structures defined in BioAPI 1.1[BioAPI specification version 1.1]:

BioAPI BIR structure:

```
typedefstructbioapi_bir
{
BioAPI_BIR_HEADER Header;

BioAPI_BIR_BIOMETRIC_DATA_PTR
BiometricData;
BioAPI_DATA_PTR Signature;
/* NULL if no signature*/
```

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

}

BioAPI_BIR_BIOMETRIC_DATA_FORMAT:

typedefstructbioapi_bir_biometric_data_format
{
uint16FormatOwner;
uint16FormatID;
}

BioAPI_BIR_DATA_TYPE:
typedef uint8 BioAPI_BIR_DATA_TYPE;
#define BioAPI_BIR_DATA_TYPE_RAW (0x01)
#define
BioAPI_BIR_DATA_TYPE_INTERMEDIATE
(0x02)
#define
BioAPI_BIR_DATA_TYPE_PROCESSED
(0x04)

#define
BioAPI_BIR_DATA_TYPE_ENCRYPTED(0x10)
#define BioAPI_BIR_DATA_TYPE_SIGNED

The **X9.84**[6**]**is an American National Standards Institute (ANSI) standard, which focuses on developing biometric standards for financial services industry. The X9.84 standard also addresses the security issues related with the storing and matching of the biometric data. The X9.84 standard uses a Biometric object,which meets the CBEFF requirements to store the biometric data. The structure of the Biometric object is shown in figure 4.

Biometric Header	Biometric data

Figure 4: Structure of Biometric Object

The biometric object contains biometric header and biometric data. The structure of these based on 1.1 specifications is shown below[8]:

BiometricHeader1.1 ::=
SEQUENCE
{
version INTEGER (…),
recordTypeRecordType OPTIONAL,
dataTypeDataType OPTIONAL,
purposePurpose OPTIONAL,
qualityQuality OPTIONAL,
validityPeriodValidityPeriod OPTIONAL,
format Format OPTIONAL
}
BiometricData ::= OCTET STRING (…)

In BioAPI 2.0, the header of the BIR has following additional information[9]:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

BiometricHeader2.0 ::=
SEQUENCE
{
BiometricHeader1.1
ProductOwner_TypeSTRING(…),
Create_Date_TimeDate_Time,
ExpirationDate date,
SecurityBlockFormatOwner Format,
Index Integer(…)
}

The first BioAPI 2.0 reference model has been developed by OSS Nokalva [9].

V. FRAMEWORK AND PERFORMANCE ISSUES FOR DEVELOPING A BIOMETRIC SYSTEM

The biometric system uses client server model to share the workload. APIs have been defined to allow the biometric application developer to share the processing between client and server. The client has the biometric device that enables the process of acquiring the biometric data and creating a template to be stored. The algorithms for verification and the implementation of databases to store the template are at the server side. As for example the BioAPI specification provides four primitive functions on client and server sides as Capture (client), Processing algorithms (server/client), Match (server / client), and CreateTemplate (client/server). The API's normally does not maintain the user databases as they may already exist, but it associates a biometric data template with each user in the database. The API does also give the biometric application vendor the flexibility to design the user interface. The framework for the development of a biometric application is shown in figure 5.

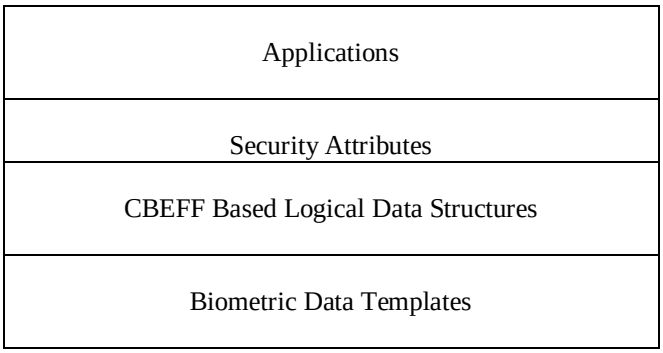

Figure 5: Biometric Application framework [BioScrypt Inc.]

Determining the effectiveness of the underlying security mechanisms in biometric systems is dependent on performance testing. The behavior of a biometric systemdepends on components that include the capture device, the biometric algorithms, the environmental conditions, and also the distribution of the biometric features among the user and impostor populations.

The overall system performance is expressed as probabilistic measures as two samples of the same person taken at different time will not correspond exactly due to factors like different positioning on the acquiring sensor, environmental changes, noise etc. Some of these measures are:

*False Acceptance Rate (FAR):*It gives the probability of accepting an unauthorized user by the system
*False Rejection Rate (FRR):*It gives the probability of rejection of an authorized user of the system.
*Failure to Enroll rate (FTE, also FER):*It gives the proportion of people who fail to be enrolled successfully.
*False Identification Rate (FIR):*It gives the probability of an identification that the biometric features are falsely assigned to a reference.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Other methods such as False Match Rate (FMR), False Non-Match Rate (FNMR), equal error rate, zeroFAR and zeroFRR are also used to evaluate the performance of a biometric system. Depending on the conditions, the biometric application may be more interested in one than the other. FAR and FRR works on a match threshold, which are fixed by the biometric application provider. Testing of these rates must include an appropriate and statistically representative data set that validates the rates. Testing may be done from a collected biometric database or by enrolling and testing a representative sample population. To analyze the performance of a biometric verification system, one has to look at how the system reacts to a large number of inquiries for biometric features from authorized as well as unauthorized users. The higher the total numbers of measurement, the more accurate the estimation.

VI. CONCLUSION

Biometric systems that are currently available today examine fingerprints, handprints, and retina patterns. Systems that are close to biometrics called as behavioural systems such as voice; signature and keystroke systems are also available in the market. As per some market research biometric systems are going to be billion-dollar market in the near future and financial institutes like banks will be major user. The biometric technology is also spreading its presence in university campus, police system and airport security. Biometrics is still relatively new technology and faces many challenges involving accuracy of probabilistic measure, acquiring features and scaling.

REFERENCES

1. BioAPI Consortium: http://www.bioapi.org, BioAPI Consortium BIOAPI Specification, Version 1.1 March 16, 2001.
2. Jain, A.K. Bolle, R. and Pankanti S. (eds.). Biometrics: Personal Identification in Networked Society. Kluwer, New York, 1999. IEEE, Biometrics, Vol. 4, 2004.
3. A.K. Jain, L.Hong, Y. Kulkarni, "A Multimodal Biometric System using Fingerprints, Face and Speech", *2nd Int`l Conference on Audio- and Video-based Biometric Person Authentication*, Washington D.C., pp. 182-187, March 22-24, 1999.
4. R. Moona, B V Kumar, S V Subramanya,"Methods and System for secured access to Devices and systems"., applied for Indian and US Patent.
5. Common Methodology for Information Technology Security Evaluation – "Biometric Evaluation Methodology Supplement [BEM]". v1.0
6. Biometrics standards and interoperabilty issues, "ANS X9.84", 2001 BIMS
7. Alessandro Triglia, "BioAPI 2.0 and the Biometric Interworking Protocol", OSS Nokalva, Inc., Mitretek Biometric Cluster Group, 2005
8. Anil K. Jain , David Maltoni, "Handbook of Fingerprint Recognition" Springer-Verlag, 2003