BIOMETRICS STANDARDS AND FACE IMAGE FORMAT FOR DATA INTERCHANGE - A REVIEW

Nita M. Thakare [1] and V. M. Thakare [2]
[1]Department Computer Science and Engg., S.S.G.M. College of Engg., Shegaon (M.S.), India
[2] Department of Computer Science and Engg., S.G.B.A. University, Amravati (M.S.), India

ABSTRACT

A biometric system is essentially a pattern recognition system. It compares the feature set data against the set of templates. Initially the biometric data is acquired from the subject, and from the acquired data the feature sets are extracted, these feature sets are used for comparison. With the ever-growing use of biometrics, it is the utmost need to use standard biometric systems. The biometric standards simplifies otherwise complicated choices, enables large scale integration, promote longevity and enables interoperability of the biometric systems. ISO/IEC has developed the biometric standards for all modalities. The part-5 of it contains the Face-Image Format for Data Interchange. It defines specifically a standard scheme for codifying data, describing human faces within a compliant data-structure. In order to enable applications that run on a variety of devices, including those with limited resources and to improve face recognition accuracy; the specification describes not only the data format, but also additional requirements, namely: scene constraints; photographic properties; digital image attributes.

KEYWORDS: *Biometric standards, Biometric modalities, Face recognition.*

I. INTRODUCTION

Biometric is the technique used to identify or verify a person by using the biological and behavioural characteristics of a person. The main objectives to implement the biometric system are to provide security towards the access of data, prohibit the entry of the unauthorised person in the restricted area, identify a person with criminal record or maintain the working time-record of an employee. It is the automated system which recognizes the individual based on the measurable biological and behavioural characteristics. The characteristics must be any automatically measurable, robust and distinctive physical trait. Biometrics' which are commonly used includes: Fingerprint Recognition, Iris Recognition, Face Recognition, Hand Geometry Recognition, Vein Recognition, Voice Recognition and Signature Recognition. In other words the biometrics can be referred to an automated system that can identify an individual by measuring their physical and behavioral uniqueness or patterns, and comparing it to those on record, instead of requiring personal identification cards, magnetic cards, keys or passwords, biometrics can identify fingerprints, face, iris, palm prints, signature, DNA, or retinas of an individual for easy and convenient verification [1][2]. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

The overall process can be implemented in two phases; Enrolment phase and Authentication phase. At the enrolment end a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. And at the authentication or recognition end biometric system recognizes a person or authenticates a person's claimed identity from their previously enrolled pattern as shown in figure 1. In this process the comparison is carried out by one of two types of searches. They provide either a one-to-one (A sample is compared with single stored template) or a one- to-many (A sample is searched against database of templates) search capability. One-to-one process which is also known as verification or authentication checks the validity of a claimed identity by comparing a verification template to an enrolment template. One-to-many search is known as identification or recognition, is designed to determine identity of a person based on biometric information only. The template of one person is compared against all biometric templates enrolled in the system.

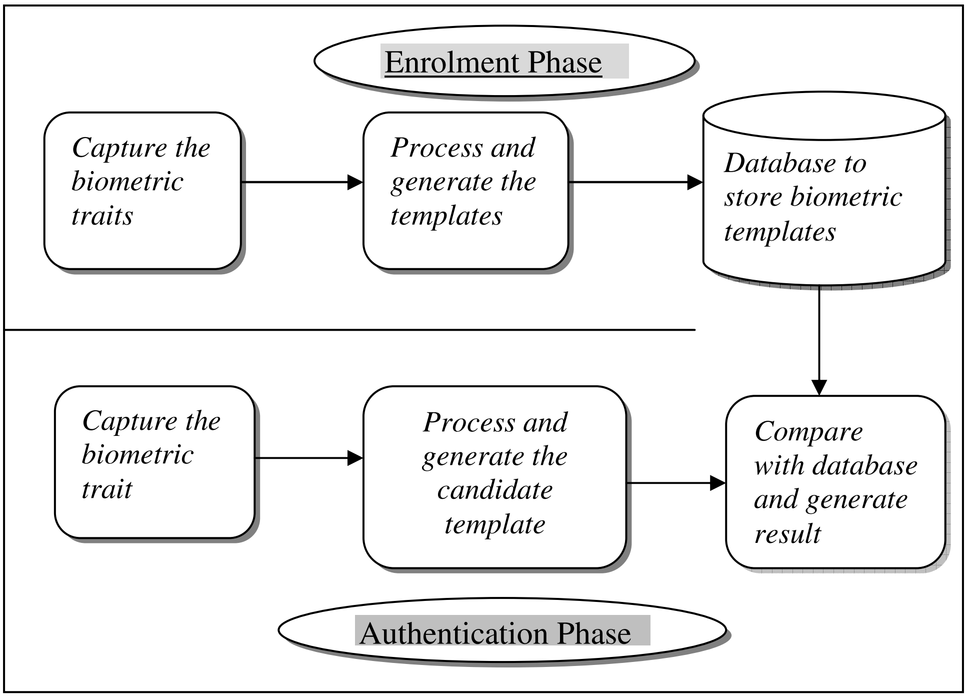
Enrolment Phase
Capture the biometric traits
Process and generate the templates
Database to store biometric templates
Capture the biometric trait
Process and generate the candidate template
Compare with database and generate result
Authentication Phase

Figure 1: *Biometric process*

II. THE MEASURES OF MODALITY

The modalities that are being commonly used can be classified into two categories; physiological and behavioural. Physiological biometrics includes fingerprint recognition, iris recognition, retina scan, face recognition, DNA biometrics whereas the voice recognition, signature verification, keystroke verification and gait recognition are considered as behavioural biometrics. For every biometric technique the four possible outcomes are Genuine Accept, False Accept (Error), Genuine Reject, False Reject (Error). The performance of biometric system is evaluated by considering two factors; False Accept Rate (FAR) and False Reject Rate (FRR). The FAR is the chance that someone other than you is granted access to your account. Low false acceptance rate is most important when security is the priority. The FRR is the probability that the genuine user is not authenticated to access his/her account. Low FRR is required when convenience is the important factor. Therefore the balance between these two errors is required to implement an efficient biometric system. To enhance the performance of biometric system as well as to answer the accessibility issues the multimodal biometric is the widely accepted solution. The multimodal biometric system makes use of multiple biometrics like face recognition with signature verification, fingerprint recognition with iris scan, gait recognition with retina scan. The multimodal biometric systems are rapidly progressing. As far as biometrics for personal recognition is concerned, any biological or behavioural characteristic can be used as a biometric identifier providing it satisfy the basic requirements [3]. These requirements are considered as measures of modality.

Universality: Every person should have the characteristic which is considered as the biometric trait for the recognition. The dumb candidate or a person without a fingerprint, need to be accommodated in some other way.

Uniqueness: Generally, no two people have identical characteristics. However, identical twins are hard to distinguish. The combination of physiological and behaviour traits can help to improve identification performance.
Permanence: The characteristics should not vary with time. A person's face, for example, may change with age. In such cases the registration/ enrolment should be repeated after certain period.
Collectability: The characteristics must be easily collectible and measurable.
Performance: The method must deliver accurate results under varied environmental circumstances.
Acceptability: The general public must accept the sample collection routines. Nonintrusive methods are more acceptable.

III. BIOMETRIC STANDARDS

Biometric systems work on images to measure and record biological characteristics. The enrolled/ trained images are converted into templates using image processing algorithms. These templates further are used to verify, recognize or identify individuals. These systems are implemented in mainly four phases; these phases are implemented to collect, store, analyze and exchange data efficiently and securely (see Figure 2). This figure is reconstructed from Biometric Standards for DoD Operational Requirements by [4], it depicts the generalized method of biometric standardization. Biometric standards allow the systems to implement the standardization of various components. It allows ease of maintenance, interoperability, and longevity of systems.

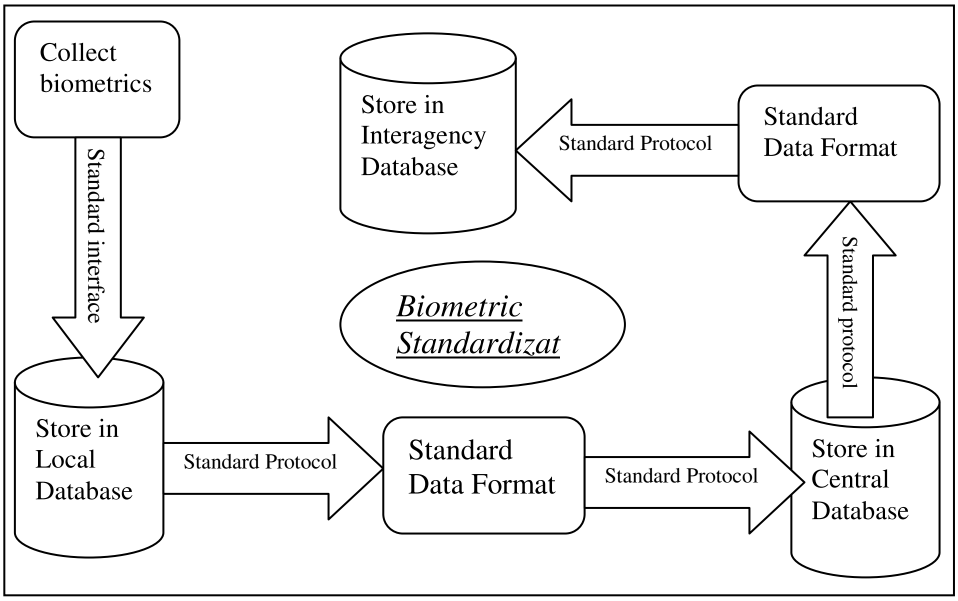

Figure 2. *Biometric Standardization*

International Organization for standardization (ISO)/ International Electrotechnical Commission (IEC) guide 2:2004 defines a standard as "a document, established by consensus that provides rules, guidelines or characteristics for activities or their results" [5]. As shown in the figure-2 biometric standardization uses the standard interfaces, standard protocols and standard data format which makes the biometric system as a standard system. These standards-based interfaces and data formats enable the system to be vendor independent, it incorporates interoperability and data sharing among various subsystems. It also helps to review the existing standards and, if required, modify or extend, to specify the design parameters of the standards and to generate the standard performance results.

The biometric standards support standardized performance and conformance testing which results into uniform test results and predictable matching performance also the standards-based sample quality assessment generates the uniform quality scores, it also help consistent design of quality measurement tools which results into improved matching performance**.** The four basic types of standards are:

3.1 Interfaces for Technical Information

Technical interface standards are specific to interactions between subsystems and components within one system. These standards include possible mechanisms to store data securely and protect data as it's exchanged between subsystems and components. They specify the need for architecture and operations necessary to identify additional standards required to support multi-vendor systems and applications.

3.2 Formats for Data Interchange

Standards of data interchange formats are mode specific and specify meaning, representation and content of formats. These standards are used for the interchange of data between multiple systems. They identify specific formats for transfer and notation that separate transfer syntax from content definition, providing independent platforms. There are modality specific formats for biometric systems such as Finger Minutiae Format for Interchange, Face Recognition Format for Data Interchange, Iris Interchange Format and Finger Image Based Interchange Format.

3.3 Standards of Application Profiles

The standards of application profiles are developed to enable interoperability of information within system applications. These are specifications for at least one base standard relative to other standardized profiles. When necessary, they identify options, parameters, chosen classes and conforming subsets of base standards and other relevant profiles. These special applications of these standards are Verification of Transportation Workers and Border Management, as well as Point of Sale applications.

3.4 Standards for Testing and Reporting

Standards of performance testing and reporting define testing methodology and the requirements of reporting test results. These standards specify methods of calculations, definitions of metrics used, testing protocols and scenario testing protocols.

IV. THE DEVELOPERS OF BIOMETRIC STANDARDS

The Biometric standards are developed by the government agencies and the standard development organizations (SDOs). The committees and institutes who are involved in development of biometric standards are;

i. National Institute of Standards and Technology (NIST)
ii. International Committee for Information Technology Standards (INCITS) M1
iii. Joint Technical Committee 1 (JTC1)/Subcommittee 37(SC37)
iv. Organization for the Advancement of Structured Information Standards (OASIS)

The brief description of standard development organizations is included in table-1. This table contains the names of SDO, The basic information about SDO, The tasks these SDOs deal with, and the deliverables of each SDO. All this information is extracted from [5][6].

Table 1. A brief description of each SDO .

SDO	About SDO	Deals with	Standard Task Group/ Works groups/Deliverables
NIST	Secretary of Commerce Under information of technical management reform act.	Standards and Guidelines for Federal Computer Systems. Specially handles security and interoperability.	*DELIVERABLES* NISTIR- NIST interagency report- NISTIR6529-A (CBEFF) NIST special Publications SP-500-245 ANSI/NIST-ITL 1-2000 data formats for interchange of fingerprint, facial & scar mark and tattoo information.
INCITS M1 (Membership Open to any Organization) It also serves as	Established in November 2001 by ANSI	Information and communication Technology (ITC), Store, Process, Transfer,	*STANDARDTASK GROUPS* M1.2 (Biometric technical Interfaces) M1.3 (Biometric Data Interchange Formats)

technical Advisory Group(TAG) for ISO/IEC (JTC1)		Display and manage information	M1.4 (Biometric profiles) M1.5 Biometric performance Testing and Reporting) M1.6 (Societal Aspects of Biometric implementation)
JTC1/ SC 37 (Has twenty-one participating countries, six observer countries, and eleven liaison organizations)	Established in June 2002, By by JTC1	The international standardization projects for generic biometric technologies to support data interchange, interoperability, and testing	*WORKING GROUPS* WG1-Harmonized Biometric Vocabulary WG2- Biometric Technical Interfaces(standards for BioAPI and CBEFF) WG3- Biometric Data Interchange Formats WG4- Biometric Functional Architecture and related profiles WG5-Biometric Testing and Reporting WG6-Cross jurisdictional and societal aspects
OASIS (Not-for-profit, international consortium)	Founded in 1993 (has more than 5000 participants, from 600 organizations and 100 countries)	Web services standards for security, e-business and standardization efforts in the public sector and for application specific market.	OASIS XCBF- Standard way to describe identity OASIS TC defined a XML encodings based on ASN.1 schema of ANSI X.84:2003 They confirm XER-XML encoding rules. SAML- Security Assertion Markup Language developed by OASIS-SSTC

V. Face Biometric Standards

Face recognition is the automated process for recognizing individual by using facial characteristics. It is considered as the most challenging biometric method because of the perceptually identical structure of human faces, the possible environmental changes and variance in image capture conditions. ISO standards 19794-5 is the international standard for face recognition [7], it describes interchange formats for several types of biometric data. ISO/IEC 19794-5 defines specifically a standard scheme for codifying data describing human faces within a CBEFF-compliant data structure for use in facial recognition systems; it implements interoperability among vendors [8]. This international standard is intended to provide a face image format for face recognition applications requiring exchange of face image data. It has significant impact on both government and civilian biometric implementation such as E-passport, personal identity documents and access control systems.

The four main requirements in ISO 19794-5 are:

Photographic Specifications.

This standard specifies the photographic conditions such as lighting conditions, positioning of cameras as well as focus set by cameras.

Scene Constraint Specifications.

This standard specifies the scene constraints such as pose and expressions.

Digital Specifications

It also specifies the digital image attributes so as to have standard image resolution and image size. It helps to verify some identification marks and will also work on the devices with limited memory space.

Image Data Format Specifications.

The face image data format should follow specific format provided by the ISO standard to specify all details.

These four requirements help in improving face recognition accuracy.

VI. THE FACE IMAGE TYPES AND RECORD FORMAT

The ISO/IEC 19794-5 standards provide four face image types these types are Basic, Frontal, Full Frontal and Token Frontal. The Basic image is the fundamental face image type which specifies a record format including header and image data. There are no mandatory scenic, photographic and digital requirements for this image type. The Frontal is a kind of basic face image type that adheres to additional requirements appropriate for frontal face recognition. The frontal images are also used for human examination. The fundamental requirements are the limitation on head rotation angle, shadows over the face, subject lighting, scene lighting. Another type is Full Frontal type. In this type frontal images are specified with sufficient resolution for human examination as well as reliable automated face recognition. These types of images also include the full head as well as the neck and shoulders. These images are used to store the facial information permanently. Token Frontal is the fourth face image type which specifies frontal images with a specific geometric size. The main specification is regarding eye positioning based on the width and height of the image. The most important use of this type of image is to minimise the storage requirements on automated face recognition.

Another important specification is regarding image record format. The detail implementation of this format is as shown in the Figure 3 which is extracted from ISO/IEC 19794-5: Biometric Data Interface Format - Face Image Data [5]. This organization of the record format includes fixed-length (14 byte) *Facial Record Header* containing information about the overall record, including the number of facial images represented and the overall record length in bytes and a *Facial Record Data block* for each facial image

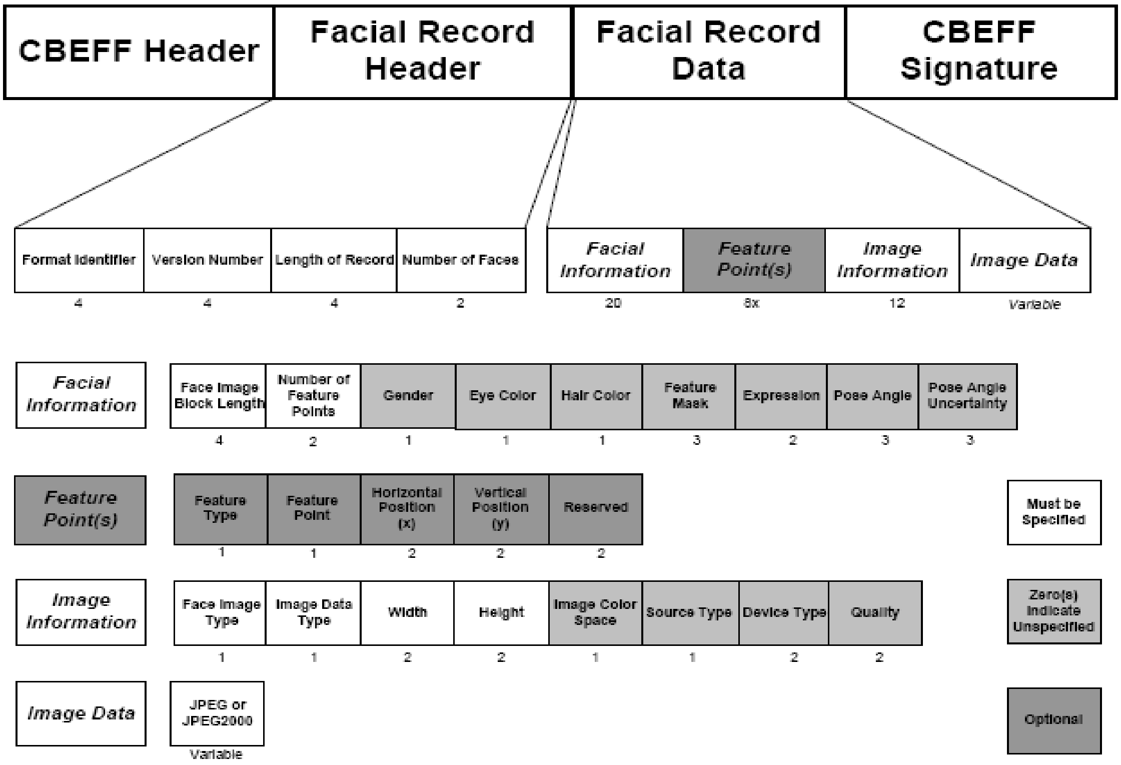

Figure 3: Face Image Record Format source: ISO/IEC 19794-5

This data consists of fixed length (20 byte) *Facial Information block* describing discernable features of the subject such as gender, multiple (including none) fixed length (8 byte) feature points block describing feature points in a facial image, A fixed length (12 byte) *Image Information block* describing digital features of the image such as face image type and dimensions such as width and height.

The standard provides the normative requirements for all the four types of face images; basic, frontal, full frontal and token frontal. These image-type specific requirements includes expected specification of facial image like its encoding format, degree of rotation, camera position, lighting condition, resolution of the image. The face image provider and vendors should ensure that the normative requirements for the chosen image type are met [9]. While face image captured is normally handled by third party, it is logical for the biometric system integrator or biometric solution provider to implement automated conformance testing of ISO/IEC 19794-5 to ensure that input face images are compliant with the respective requirements of face image types.

By establishing standard formats for facial images the following objectives can be achieved[11]:

. Allow interoperability among facial recognition vendors

. Minimize the amount of data necessary to store face information with applications that have limited storage

. Ensure that enrolled images will meet a quality standard needed for face recognition

. Improve system throughput by saving the intermediate data instead of the raw data

VII. THE END-USER ADOPTION OF THE BIOMETRIC STANDARDS.

Standards are useful only if they are adopted. There is generally a lag time between the availability of standards and the availability of compliant products [10]. Further, many times vendors delay implementing the standards until they see customer demand for compliance. Some of the examples of end-user adoption of standards are listed below.

Table 2 . Examples of end-user adoptions

End user adoptions	**Application**
E-Passports	The International Civil Aviation Organization (ICAO) of the UN sets the requirements for machine readable travel documents (MRTDs), including e-passports and visas. ICAO has required that the biometrics stored within the e-passport conform to the requirements of the SC37 biometric data interchange format for face, fingerprint, and iris data.
Seafarer Identification.	The International Labour Organization (ILO) of the UN has a program for issuing a common identification credential for seafarers. This program has required that the fingerprint minutiae templates stored on the seafarer ID card conform to ISO/IEC 19794-2.
US Department of Homeland Security	DHS has required the use of INCITS biometric standards in several of its large biometric projects to include: • US Visitor and Immigration Status Indicator Technology (US VISIT) border management program • Transportation Worker Identification Credential (TWIC) • TSA Registered Traveler program
US Department of Defense	A number of INCITS standards have been adopted within the DoD Joint Technical Architecture and the Defense Information Standards Registry.
US Federal Employee Personal Identity Verification.	To comply with Homeland Security Presidential Directive (HSPD) 12, NIST developed technical specifications for the associated biometric-based credentialing system. Included in these specifications are requirements for compliance with the INCITS biometric data format specifications for finger images, minutiae templates, and facial images. Product availability is in progress, particularly since most of the standards are so recent, but a good example is the availability of BioAPI compliant products. BioAPI was released in 2001 and became an official ANSI standard in 2002. At this point, approximately 40 products have been announced

VIII. Conclusion

Biometric recognition can be described as automated methods to accurately recognize individuals based on distinguishing physiological and/or behavioural traits. The biometric traits plays vital role in making the biometric systems robust and performance efficient it is an increasingly critical component in the protection of information, infrastructure and personal identity, the continued development of comprehensive biometric standards is essential to ensure reliability, security, interoperability, usability and scalability.The International biometric standards are being widely used in both government and civilian applications. Especially the face recognition standards help in improving performance accuracy for identity and passport verification. Besides making the biometric system interoperable it also help in reducing the computational cost because of the less requirement of image pre-processing and image registration task. The Image database containing the images in standard format improves efficiency, robustness and interoperability of the biometric system.

References

[1] Biometrics.gov: Biometrics history (2006).
http://www.biometrics.gov/Documents/BioHistory.pdf

[2] Biometrics and its application, BioEnable technology private Ltd.
www.bioenabletech.com

[3] Emilio Mordini and Sonia Massari (2009) , Body, Biometrics and Identity, *Bioethics*
ISSN 0269-9702 (print); 1467-8519 (online) doi:10.1111/j.1467-8519.2008.00700.x
Volume 22 Number 9

[4] Mr. Enji Hutchinson (2008),Biometric Standards for DoD Operational Requirements,
Biometrics task force

[5] NSTC-Biometric standards.

[6] Fernando Podio, Overview of National and International Biometric Standards Activities
NIST Biometric Standards Program Computer Security Division ,NIST/ITL

[7] ISO/IEC 19794-5: Biometric Data Interface Format - Face Image Data.

[8] Lim Eyung,Lum Jia Jun Brandon,Dai Zhong Min, Face Biometric Standards and Conformance, Temasek Polytechnic/Cyber and Digital Security

[9] NSTC Policy for Enabling the Development, Adoption and Use of Biometric.
Standards (2007), *NSTC* Subcommittee on Biometrics and Identity Management.

[10] Creed Jones, et all , Description of Biometric Data Interchange Format Standards, INCITS M1 Technical Editors

[11] Cathy Tilton**,** Biometric Standards – An Overview, January 2006

Authors

N. M Thakare is an Assistant Professor, working in the department of computer Science and Engg at Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Amravati, Maharastra (India).She has completed ME in Computer Science and Engineering. Currently she is pursuing Ph.D. under the supervision of Dr. V. M. Thakare. Her Area of research is Computer Vision. She has published and presented 17 papers at National and International level. Currently she is working on pattern recognition algorithms and the face recognition methodologies

V M Thakare is Professor and Head of PG department of computer Science and Engg in SGB Amravati University Amravati, Maharastra(India) and has completed ME in Advance Electronics and Ph.D. in computer Science/Engg. His Area of Ph D is Robotics and Artificial Intelligence. Currently he is working in area of wireless computing, mobile computing, Information Technology. He is Recognized supervisor for computer science and computer engineering in this University and also in other universities .He has also received national level Award for excellent paper. More than 10 candidates are working for Ph D Under his supervision. He has published and presented more than 115 papers at National and international level.