International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:4, 2009

Biometric Methods and Implementation of Algorithms

Parvinder S. Sandhu, Iqbaldeep Kaur, Amit Verma, Samriti Jindal, Shailendra Singh

***Abstract*—**Biometric measures of one kind or another have been used to identify people since ancient times, with handwritten signatures, facial features, and fingerprints being the traditional methods. Of late, Systems have been built that automate the task of recognition, using these methods and newer ones, such as hand geometry, voiceprints and iris patterns. These systems have different strengths and weaknesses. This work is a two-section composition. In the starting section, we present an analytical and comparative study of common biometric techniques. The performance of each of them has been viewed and then tabularized as a result. The latter section involves the actual implementation of the techniques under consideration that has been done using a state of the art tool called, MATLAB. This tool aids to effectively portray the corresponding results and effects.

***Keywords*—**Matlab, Recognition, Facial Vectors, Functions.

I. Introduction

TRUSTED and faithful systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting for their services and corresponding applications. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. The purpose of establishing the identity is to ensure that only a legitimate user, and not anyone else, accesses the rendered services. Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. Biometrics identify people by measuring some aspect of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such as your handwritten signature), or something that is a combination of the two (such as your voice). Biometrics allows us to confirm or establish an individual's identity based on who he/she is, rather than by what he/she possesses as from ID card or what she knows for example password (cryptal or non-cryptal) [7]-[10]. In much simpler way Biometrics refers to the automatic identification of a living person based on physiological or behavioral characteristics. There are many types of biometric technologies on the market: face-recognition, fingerprint recognition, finger geometry, hand geometry, iris recognition, vein recognition, voice and signature. The method of biometric identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: The person to be identified is required to be physically present at the point-of-identification or the identification based on biometric techniques obviates the need to remember a password or carry a token or a smartcard. With the rapid increase in use of PINs and passwords occurring as a result of the information technology revolution, it is necessary to restrict access to sensitive/personal data. By replacing PINs and passwords, biometric techniques are more convenient in relation to the user and can potentially prevent unauthorized access to or fraudulent use of ATMs, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports, driver's licenses and insurance cards may be forgotten, stolen, or lost. Various types of biometric systems are being used for real-time identification; the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan, speech, face, and hand geometry.

Parvinder S. Sandhu is Professor at Rayat & Bahra Institute of Engineering & Bio-Technology, Mohali-Sahauran 140104. E-Mail: parvinder.sandhu@gmail.com.

Samriti Jindal is Lecturer with Swami Vivekananad Institute of Engineering & Technology, Banur Punjab.

Shailendra Singh is associated with Deptt. of Information Technology at Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India

Amit Verma and Iqbaldeep Kaur are Assistant Professors at Rayat & Bahra Institute Of Engineering & Bio-Technology, Mohali, India. E-Mail:eramitverma@rediffmail.com, er_iqbaldeep@yahoo.com

II. Identification versus Verification

Sometimes Identification and Verification are used as similar terms, but they have two different meanings. Identification means determining a person by presenting his biometric feature. For this purpose a database of templates is searched and matched against the biometric sample until the best fitting (most similar) template is found. This method also known as "1:N" or "one-to-many comparison". In comparison to identification, verification (as shown in Fig. 1) [17] means testing, if the user is really the person he/she claims to be. The presented biometric feature is compared against the previously stored biometric reference data either on a smartcard or in a database.

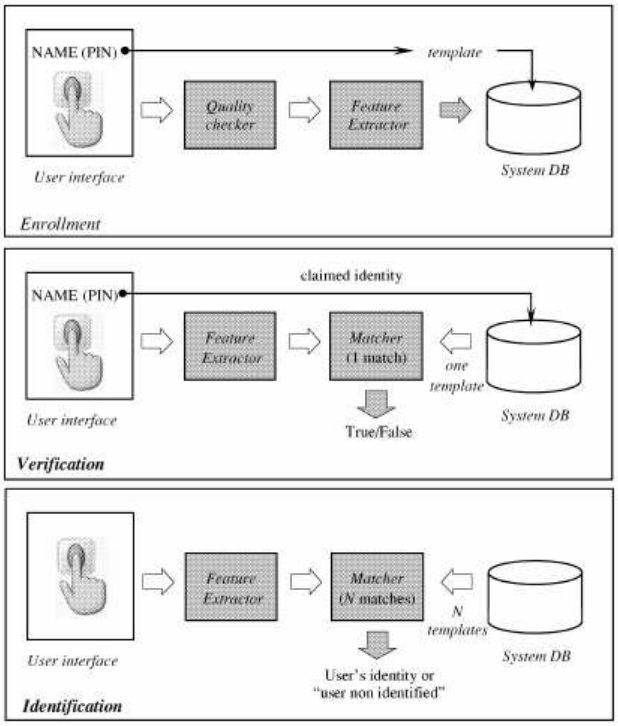

Fig. 1 Identification and Verification Unit

In contrast to the identification method only one biometric comparison is being performed.

III. False Rejection Rate / False Acceptance Rate

In contrast to methods based on knowledge or possession like PINs/passwords or tokens, biometric systems work with probabilities, because biometric features are invariably caused by noise in the measurement – therefore biometric systems are not exact methods. A second point is that for example, fingerprint systems can suffer from accuracy problems created by limitations of sensors and algorithms. These limitations result in two problems called False Acceptances and False Rejections. The False Acceptance Rate (FAR) is the success probability for an unauthorized user or a user that does not exist within a biometric system to be falsely recognized as the legally registered user. A low tolerance threshold for the biometric data to be matched leads to a lower FAR value, but to higher values of the False Rejection Rate (FRR). In contrast, the False Rejection Rate (FRR) rate is the probability of the legally registered user to be falsely rejected by the biometric system when presenting his biometric feature. High tolerance limits for the biometric data to match lead to a very low FRR value, but to higher values for the False Acceptance Rate (FAR). Both values FAR and FRR are negatively correlated. However, these measures can vary significantly depending on how one adjusts the sensitivity of the mechanism that matches the biometric. If the tolerance thresholds for the biometric data to be matched for a successful verification are chosen, so that the values for a false acceptance rate and false rejection rate are equal, this common value is called the equal error rate (EER). The equal error rate is also known as the crossover error rate (CER). The lower the equal error rate is, the higher the accuracy of the biometric system. For applications where convenience and general user acceptance are more important than security (i.e. hotel room access, automatic teller machine authentication), administrators have to settle for a high FAR in order to ensure that authorized individuals are always granted access. The disadvantage of a low FRR is a greater likelihood of granting access to unauthorized individuals.

IV. Methods

A. Handwriting Signatures

Handwritten signatures had been used in China, but carved personal seals were considered to be upper status, and are still used for serious transactions in China, Japan, and Korea . Over time, the signature became accepted as the standard way of doing transactions. Every day, billions of dollars' worth of contracts are concluded by handwritten signatures on documents, and how these can be replaced by electronic signatures is a hot policy and technology issue.

B. Face Recognition

The face is the commonly used biometric characteristics for person recognition. The most popular approaches to face recognition are based on shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. Recognizing people by their facial features (or vectors) is the oldest identification mechanism of all, going back at least to our early primate ancestors. Biologists believe that a significant part of our cognitive function evolved to provide efficient ways of recognizing other people's facial features and expressions. For example, we are extremely good at detecting whether another person is looking at us or not. In theory, humans' ability to identify people by their faces appears to be very much better than any automatic system produced to date.

The human ability to recognize faces is also important to the security engineer because of the widespread reliance placed on photo IDs.

C. Fingerprints

Fingerprints are important. By 1998-99, fingerprint recognition products accounted for 80% of the total sales of biometric technology. These products look at the friction ridges that cover the fingertips and classify patterns of minutiae, such as branches and end points of the ridges. Some also look at the pores in the skin of the ridges.

D. Iris Codes

Iris code is a very traditional Technique of identifying people to the modern and innovative way . Recognizing people by the patterns in the irises of their eyes is far and away the technique with the best error rates of automated systems when measured under lab conditions. Voice recognition—it is also

known as speaker recognition—is the problem of identifying a speaker from a short utterance. While speech recognition systems are concerned with transcribing speech and need to ignore speech idiosyncrasies, voice recognition systems need to amplify and classify them. There are many sub problems, such as whether the recognition is text-dependent or not, whether the environment is noisy, whether operation must be real time, and whether one needs only to verify speakers or to recognize

E. Other Systems

A number of other biometric technologies have been proposed. Some, such as those based on facial thermograms (maps of the surface temperature of the face, derived from infrared images), the shape of the ear, gait, lip prints, and the patterns of veins in the hand, don't seem to have been marketed as products. Other technologies may provide interesting biometrics in the future. For example, the huge investment in developing digital noses for quality control in the food and drink industries may lead to a "digital doggie," which recognizes its master by scent.

V. Tabularized Representation Of Method

The various method [1] [2] discussed above are given under in the tabularized form with performance, universality, ease of use and approx template size as parameter for [11]-[15] comparison.(As shown in Table I)

TABLE I
COMPARISON OF DIFFERENT METHOD OF RECOGNITION

Type	Performance	Acceptability	Universality	Ease of Use	Approx Template Size
Facial	Moderate	High	Moderate	High	84 byte - 2k
thermo gram	Moderate	Moderate	Moderate	Moderate	---------
Hand Vein Gait	Moderate	Moderate	Low	Moderate	9 byte
Keystroke	Low	Low	Low	low	---------
Odor	High	Moderate	Moderate	Moderate	---------
Ear and Finger and Face	Moderate	High	Moderate	High	256 byte-1.2k
Iris	Moderate	Moderate	Moderate	Moderate	256 byte
Retina	Moderate	High	Moderate	Moderate	96 byte
Voice	Moderate	Moderate	High	Moderate	70-80k
Signature	Moderate	Moderate	High	High	500 byte-1000 byte
DNA	High	High	High	Moderate	------

The work flow of the methods is as given below:

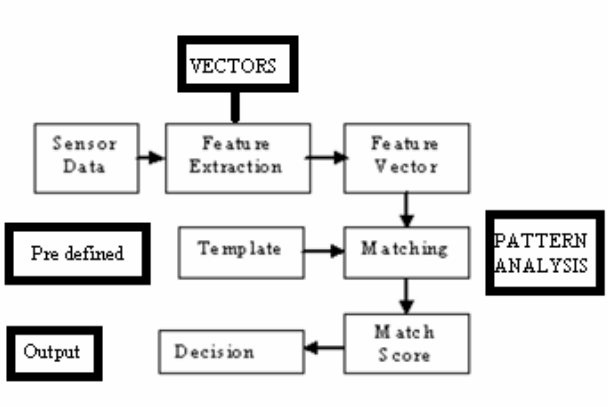

Fig. 2 Flow Diagram

As shown in fig. 2, Feature extraction [1] [6] referred as vectors or feature vectors. Templates are predefined and matching is done according to pattern as the part of analysis.

VI. Algorithms of Biometrics

The categorization of bio-metric (As from Fig. 3) is as given below:

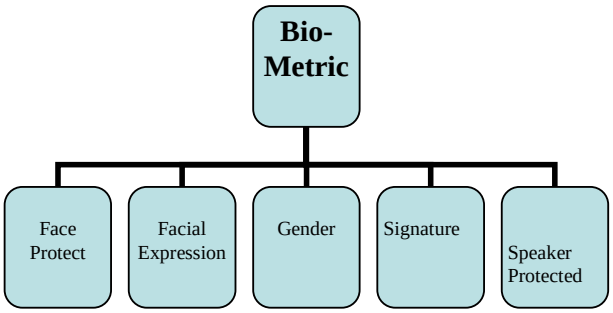

Fig. 3 Bio-Metric Recognition

A. Face Protect[3][5]

First, select an input image as shown in Fig. 2 & Fig. 3, then clicking on Select image icon (As shown in Fig. 4). Then we can add this image to database by click on Add selected image to database and image selected as part of database. We can perform face recognition by clicking on Face Recognition icon. If we want to perform face recognition database has to include at least one image. If we choose to add image to database, a positive integer (vector ID) is required. This positive integer (As from Fig. 5) is a continuous number which identifies a person or image under test and each person corresponds to a particular class.

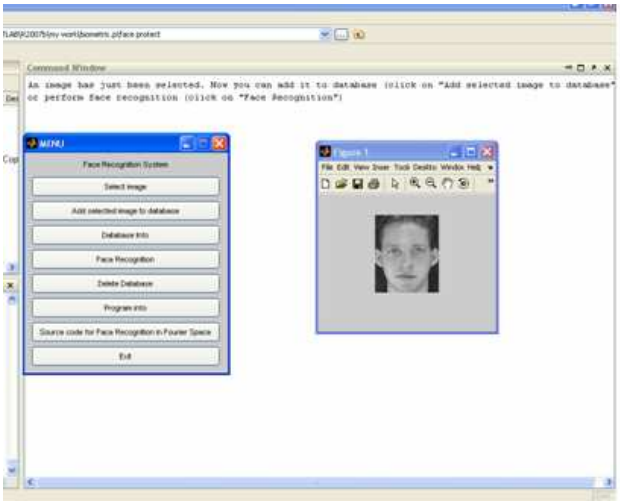

Fig. 4 Selection of An Image

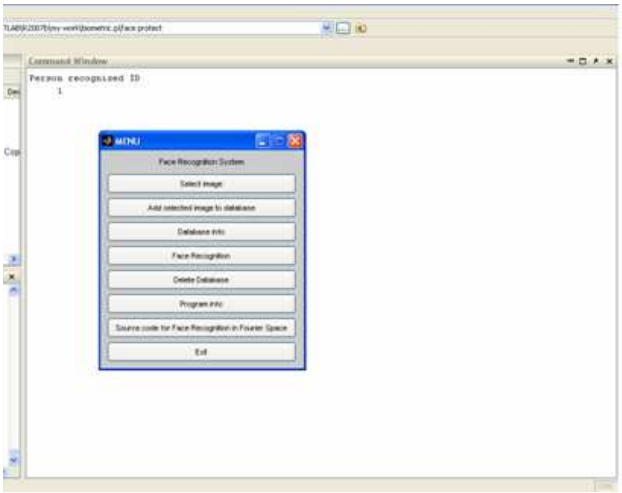

Fig. 5 Recognition by Positive Number

B. Facial Expression [3][5]

Select an input image clicking on Select image icon. We can select any image any face. Then add this image to database by click on Add selected image to database under test. Perform facial expression recognition by clicking on Facial Expression Recognition icon. If we want to perform facial expression recognition; database has to include at least one image. If we choose to add image to database (As from Figure 6), one have also to insert the corresponding facial expression [4] 'Happiness', 'Sadness', 'Surprise', 'Anger', 'Disgust', 'Fear' or 'Neutral'. Functions are discussed in Table II.

C. Gender[3][5]

Select an input image clicking on Select image (face taken from [16]) icon as shown in Fig. 7. We can select any image any face. Then add this image to database by click on Add selected image to database under test. Perform gender recognition by clicking on gender recognition icon (As from Table III). If it is required to perform gender recognition (Fig. 4 & Fig. 5), database has to include at least one image. After that we have to specify the gender of the image under test type "1" if female, "0" if male. Functions are discussed below (As from Fig. 8).

TABLE II
FUNCTION OF FACIAL EXPRESSION

Select image	read the input image
Add selected image to database	The input image is added to database and will be used for training
Database Info	Show information's about the images present in database.
Facial Expression Recognition	Facial Expression recognition. The selected input image is processed
Delete Database	Remove Database from the current directory
Exit	Quit Program

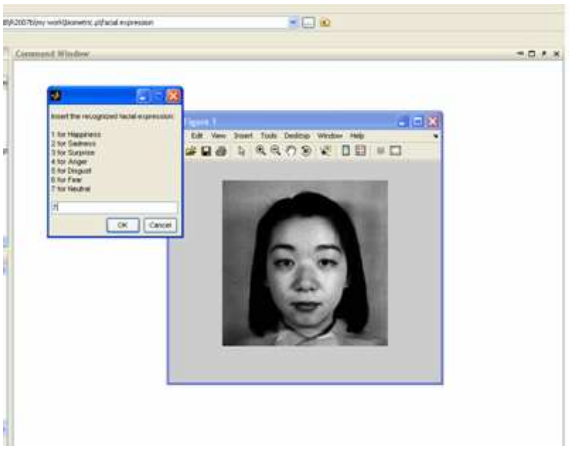

Fig. 6 Selecting Face and Perform Recognition

TABLE III FUNCTION FOR GENDER RECOGNITION

Select image	read the input image
Add selected image to database	the input image is added to database and will be used for training
Database Info	show informations about the images present in database.
Gender Recognition:	The selected input image is processed
Delete Database Exit	remove database from the current directory and quit program

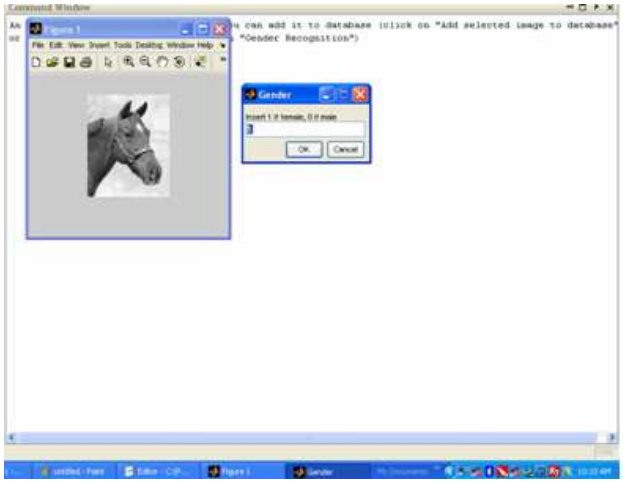

Fig. 7 Selection of An Image

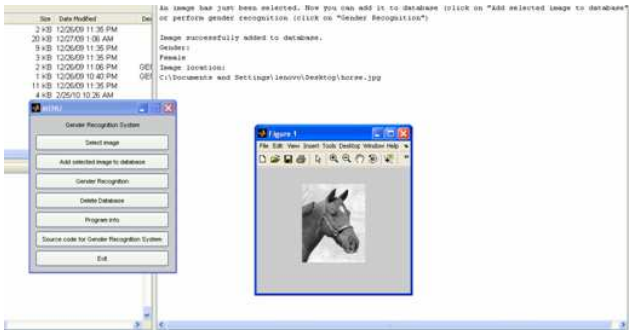

Fig. 8 Performing Gender Recognition

D. Signature Recognition [3][5]

Select an input image clicking on.Select image icon. One can select any image any face. Then add this image to database by click on Add selected image to database under test. Perform Signature recognition by clicking on Signature recognition icon. If we want to perform Signature recognition, database has to include at least one image. Then assign class to that signature by any positive number (Fig. 6). When ever one process the signatures they are recognition by corresponding class (As from Fig. 9)

VII. Conclusion

In this world of globalization where the whole world is connected to each other for sharing of resources in one way or the other, the following statement holds true. The only system which can be relied upon to be safe is the one that is powered off! So, the crux of the story lies in the strength of the security feature of the system. There are two sides of every coin. Biometric systems are no exception. There also exists the flop side. To be more specific, we may find the usual cropping of failures due to bugs, blunders, and complacency. Biometrics are like many other protection mechanisms (alarms, seals, tamper sensing enclosures,) in which environmental conditions can cause havoc. Noise, dirt, vibration, and unreliable lighting conditions all take their toll. Some systems, like speaker recognition, are vulnerable to alcohol intake and stress. Changes in environmental assumptions, such as from closed to open systems, from small systems to large ones, from attended to standalone, from cooperative to recalcitrant subjects, and from verification to identification—can all undermine a system's viability. There are a number of more specific and interesting attacks on various biometric systems. There have been some attacks on the methods used to index biometric data. Apart from the possibility that a fingerprint or DNA sample might have been planted by the security, it may just be old. So the need is to implement a powerful biometric system. Biometrics is usually more powerful in attended operation, where, with good system design, the relative strengths and weaknesses of the human guard and the machine recognition system may complement one another.

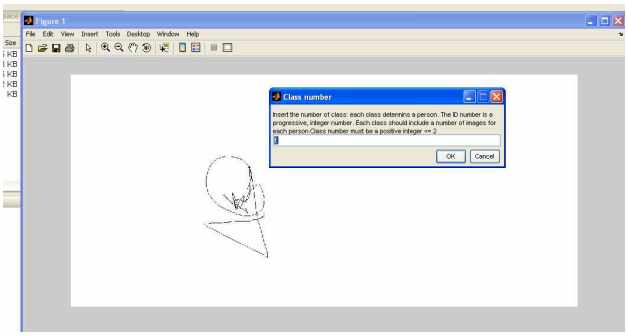

Fig. 9 Signature Recognition

References

[1] A Survey of Unimodal Biometric Methods Nimalan Solayappan and Shahram Latifi Department of Electrical engineering, University of Nevada at Las Vegas, USA
[2] A SURVEY OF BIOMETRIC RECOGNITION METHODS Kresimir Delac , Mislav Grgic HT - Croatian Telecom, Carrier Services Department, Kupska , Zagreb, CROATIA University of Zagreb, FER, Unska 3/XII, Zagreb, CROATIA, 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia 184
[3] http://scien.stanford.edu/class/ee368/projects2001/dropbox/project16/
[4] http://www.irc.atr.jp/%7Emlyons/pub_pdf/fg98-1.pdf
[5] http://www.kasrl.org/jaffe.html
[6] Natalia A. Schmid, Joseph A.O'Sullivan,"Performance Prediction Methodology for Biometric Systems using a Large Deviations Approch", IEEE Transaction of Signal Processing, October 2004.
[7] Li Ma , Tieniu Tan , Yunhong Wang , Dexin Zhang , " Personal Identification Based on Iris Texture Analysis" , IEEE Transactions on Pattern Analysis and Machine Intelligensce , Vol. 25 No. 12, December 2003.
[8] John Carter, Mark Nixon, "An Integrated Biometric Database" Department of Electronics and Computer Science, University of Southampton, Highfield, Southanpton,
[9] A Survey of Unimodal Biometric Methods Nimalan Solayappan and Shahram Latifi Department of Electrical engineering, University of Nevada at Las Vegas, USA
[10] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(7), 1997.
[11] R. Chellappa, C. L. Wilson, and S. Sirohey. Human and Machine Recognition of Faces: A Survey. Proceedings of the IEEE, 83(5), 1995.
[12] E. Hjelmås and J. Wroldsen. Recognizing Faces from the Eyes Only. In Proceedings of the 11th Scandinavian Conference on Image Analysis, 1999.

[13] A. Jain, L. Hong, and S. Pankanti. Biometric Identification. Communications of the ACM, 43(2), 2000.
[14] M. Lades, J. C. Vorbrüggen, J. Buhmann, J. Lange, C. von der Malsburg, R. P. Würtz, andW. Konen. Distortion Invariant Object Recognition in the Dynamic Link Architecture. IEEE Transactions on Computers, 42(3), 1993.
[15] B. S. Manjunath, R. Chellappa, and C. von der Malsburg. A Feature Based Approach to Face Recogntion. In Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1992.
[16] Coding Facial Expressions with GaborWavelets Michael Lyons and Shigeru Akamatsu ATR Human Information Processing Research Laboratory 2-2 Hikaridai, Seika-cho Soraku-gun, Kyoto 619-02, Japan Miyuki Kamachi and Jiro Gyoba Psychology Department, Kyushu University Proceedings, Third IEEE International Conference on Automatic Face and Gesture Recognition, April 14-16 1998, Nara Japan, IEEE Computer Society, pp. 200-205.
[17] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE An Introduction to Biometric Recognition IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, JanuarY 2004