RESEARCH PAPER | Computer Science | Volume : 4 | Issue : 4 | Apr 2014 | ISSN - 2249-555X

Face Recognition System Techniques and Approaches

KEYWORDS: Biometrics, face databases, identical twins, Face recognition techniques

B. Lakshmi Priya
PhD Research scholar in Computer Science, Mother Teresa Women's University,Tamil Nadu, India

Dr. M. Pushpa Rani
Professor & Head, Dept. of Computer Science, Mother Teresa Women's University, Tamil Nadu, India

ABSTRACT *A facial recognition method is a computer application for robotically identifying or verifying a person from a digital image or a video frame. The security system recently boomed in safe & security industry in biometric system which is using face, ear, retina, iris, fingerprints, gait and so on recognition. One of the ways to do is by comparing selected facial features from the image and a facial database. Variations in pose, expression, aging and mask are considered as basic challenges in face recognition systems and several standard databases have been built to address these challenges. Classifying identical twins is another challenging problem. The twin's database images were collected from different twin's festivals in Twinsburg from the World Wide Web. In this paper description of a general review and study of recent face recognition techniques.*

1. INTRODUCTION

The human face plays an important role in our social interaction, conveying people's identity. Using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years due to its potential for a wide variety of applications in both law and non-law enforcements. As compared with other biometric systems using fingerprint, palm print and iris, face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrent purpose because face images that have been recorded and archived can help later to identify a person. However it is still suitable for many applications especially when taking into account its convenience for user as shown in Figure 1. Human often uses faces to recognize individuals. Today many face recognition systems have been proposed and their accuracy have been evaluated on various face-databases. Yet there are some existing essential problems that affect the performance of these systems, illuminations, poses, occlusions, aging, masked and expressions are among these problems. For several years researchers have proposed different approaches to address these problems [1,2,3] but there still remains some other new challenges such as studying the groups with the most common features like twins. Few twins studies have been already carried out in biometrics. They include various biometric systems such as finger prints [4] hand writing [5] palm prints [6], and iris [7], have been proposed, implemented and deployed. However, identical twins having the closest gene based relationship are expected to have maximum similarity between their biometrics. Classifying identical twins is a challenging problem for some automatic biometric systems. So there is a need for a new database containing twins face images which is capable of addressing various problems in face recognition systems. The major motivation of this work is to assess the accuracy of current generation of facial recognition systems on a particularly challenging data set, containing twins.

The twins data used in our study were obtained from data collection sessions at the Twins Days Festival in Twinsburg, Ohio in August 2009 and August 2010 [8]. The dataset consists of 186 subjects, of which 34 are male and the remaining 152 are female. The twins participating in the data collection self reported themselves as identical twins. All data collected at the festival followed a data collection protocol approved by the Human Subjects Institutional Review Board (HSIRB). Humans are very good at identifying people from their images, and so human face recognition performance is often considered as a guideline for assessing face recognition algorithms [9]. To the best of our knowledge, there is no study that considers twins facial impacts on face recognition systems. The main motivation for this paper is to present a new database which provides a large set of clear face images of twins and systematically evaluate the performance of existing face recognition algorithms. All the faces are the result of Viola-Johns face detection [10] and poses lower than 25° are considered in different subset grouping.

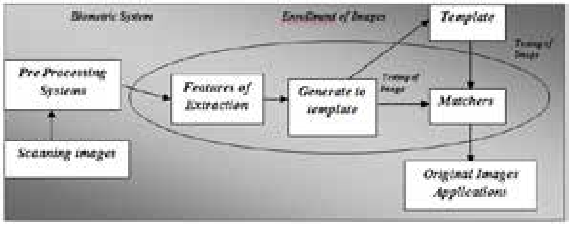


Figure.1 "The Biometric System Processing diagram"

The remainder of the paper is structured as follows: Section 2 presents an overview of biometric Systems operating modes and errors. Section 3 describes face recognition approaches of databases, twins face recognition challenges and combining twins face recognition with other biometric modalities. Section 4 concludes the paper with directions for future work.

2. AN OVERVIEW OF BIOMETRIC SYSTEM

Biometric systems have the following stages of operation: 1) capture biometric sample of the person, 2) extract set of relevant features from captured sample, 3) and compare the extracted feature set against the template set in the database. Biometric systems operate in two modes, verification (also called authentication) and identification. In the verification mode, the system performs a one to one comparison and the system's decision is either to accept or to reject a claimed identity. In the identification mode, the system performs one to many comparisons and the system's aim is to assign an identity to one of the user templates or to announce no match. In other words, the verification modes seeks an answer to the question"Am I who I claim I am?" while the identification searches for the question"Who am I?". Biometric systems are not perfect. There are two important types of errors associated with biometric system, namely a false accept rate (FAR) and a false reject rate (FRR). The FAR is the probability of wrongly accepting an impostor user, while the FRR is the probability of wrongfully rejecting a genuine user. System decisions (i.e. accept/reject) is based on so-called thresholds. By changing the threshold value, one can produce various pairs of FAR and FRR. For reporting performance of biometric system in verification mode, researchers often use a decision error trade-off (DET) curve. The DET curve is a plot of FAR versus FRR and shows the performance of the system under different decision thresholds [11], shown in Figure 2. Using machine learning terminology, FAR and FRR are analogues to False Negative and False Positive, respectively. A modified version of the DET curve is a ROC (Receiver Operating Characteristic) curve, which is widely used in the machine learning community. The difference between DET and ROC curves is in ordinate axis. In the DET curve the ordinate axis is FRR, while in the ROC curve it is 1-FRR (i.e. probability of correct verification). Usually, to indicate the performance of biometric system by a single value in verification mode, an equal error rate (EER) is used. The EER is the point on the DET curve, where FAR=FRR, shown in Figure 2. To evaluate the performance of a biometric system in identification mode, a cumulative match characteristics (CMC) curve can be used. The CMC curve is a plot of rank versus identification probability and shows the probability of a sample being in the top closest matches [12], shown in Figure 3. In identification mode, to indicate performance of the system by a single number, the recognition rate (i.e. identification probability at rank 1) is used. In the next sections, when performance of the method is referred to the recognition rate the system is evaluated in the identification mode, and when it is referred to the EER the system is evaluated in the verification mode. It should be also noted that the given performances (i.e. EER, recognition rates) in next sections are not intended for direct comparisons mainly due to differences in data sets and classification methods. They are intended to give an impression of overall performance of face recognition biometrics.

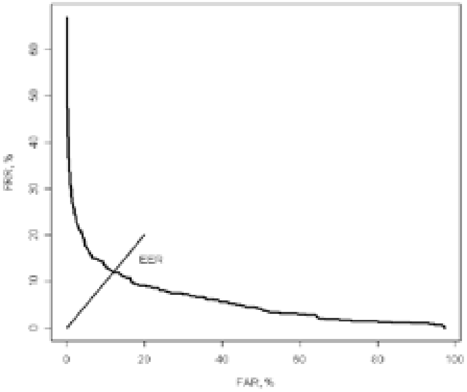


Figure 2: An example of DET curve

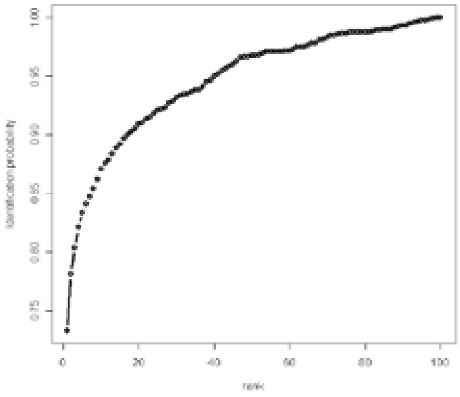


Figure 3: An example of CMC curve

3. DATABASES FOR FACE RECOGNITION

This researcher reviewed some of the databases for face recognition are noted herewith.

The AR Face Database

The AR database [13] was collected at the Computer Vision Center (CVC) at the U.A.B. It contains over 4,000 color images corresponding to 126 people's faces (70 men and 56 women). The imaging and recording conditions (camera parameters, illumination setting, and camera distance) were carefully controlled and constantly recalibrated to ensure that settings are identical across subjects. The resulting RGB color images are 768 × 576 pixels in size. The subjects were recorded twice at a 2–week interval. During each session 13 conditions with varying facial expressions, illumination and occlusion were captured. Figure 4, shows an example for each condition. So far, more than 200 research groups have accessed the database.

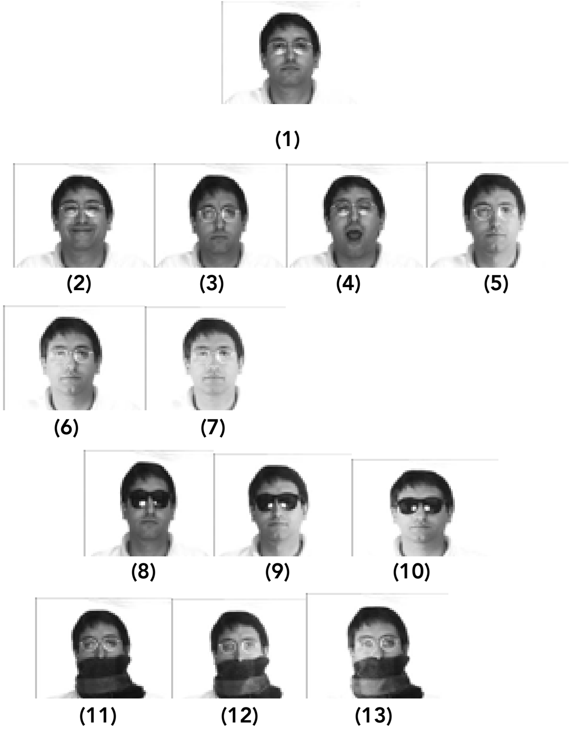


Figure 4: AR database - The conditions are (1) neutral, (2) smile, (3) anger, (4) scream, (5) left light on, (6) right light on, (7) both lights on, (8) sun glasses, (9) sun glasses/left light (10) sun glasses/right light, (11) scarf, (12) scarf/left light, (13) scarf/right light

BANCA Database

The BANCA[14] multi-modal database was collected as part of the European BANCA project, which aimed at developing and implementing a secure system with enhanced identification, authentication, and access control schemes for applications over the Internet. The database was designed to test multimodal identity verification with various acquisition devices (high and low quality cameras and microphones) and under several scenarios (controlled, degraded, and adverse). Data were collected in four languages (English, French, Italian, and Spanish) for 52 subjects each (26 men and 26 women). Each subject was recorded during 12 different sessions over a period of 3 months. Recordings for a true client access and an informed imposter attack were taken during each session. For each recording the subject was instructed to speak a random 12-digit number along with name, address, and date of birth (client or imposter data). Recordings took an average of 20 seconds. Figure 5, shows an example of images for all three recording conditions. The BANCA evaluation protocol specifies training and testing sets for a number of experimental configurations, so accurate comparisons between algorithms are possible.

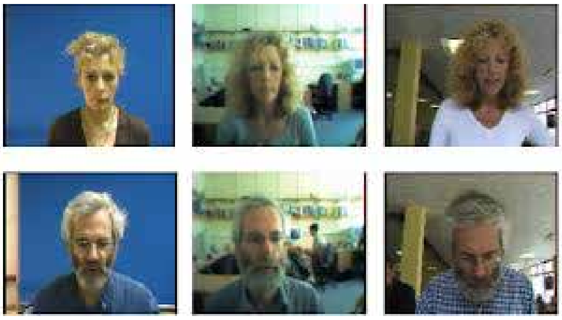


Figure 5: Images for the three recording conditions in the BANCA database.

EQUINOX Infrared Face Database

Equinox [15] Corporation collected a database of long-wave infrared (LWIR) imagery in the spectral range. The database is unique in that the sensor used for the collection simultaneously records video sequences with a visible CCD array and LWIR micro bolometer. The resulting image pairs are 240 × 320 pixels in size and co-registered to within 1/3 pixel. All LWIR images were radio metrically calibrated with a black-body radiator. The database contains 91 subjects. For each subject, a 4-second (40 frames) video sequence was recorded while the subject pronounced the vowels. Additional still images were obtained in which the subjects display the facial expressions "Smile." These images were recorded under two illumination conditions: The categories are (a) vowel (frontal illumination) and (b) "smile" (right illumination), Figure 6, Shows an Example image of the Equinox IR database. The upper row contains visible images and the lower row long-wave infrared images.

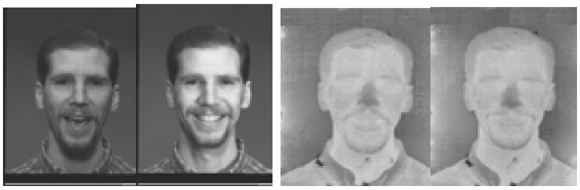


Figure 6: Example images of the Equinox IR database.

Face Disguise and Synthetic Database:

Physical appearance with disguise is one of the ways frauds try to penetrate to security systems. Face recognition systems should be capable of identifying these appearance alterations. Face disguise and synthetic database [16] were organized to cover some of these real variations an individual can make. This database contains 10 disguise variations of 15 individuals which are generated using synthetic disguise template such as beard, moustache, hat and scars. As shown in Figure 7, the inter-personal and intra-personal characteristics can be modelled using disguise accessories to alter the appearance of an individual, to impersonate another person, or to hide one's own identity. The database organizers also built a synthetic face database to make variations in disguise by using the Face Software which is widely used for face generation in crime scene investigations. For example, a criminal can alter facial features and appearance using makeup tools and accessories to remain elusive from law enforcement. The challenges due to disguise cause change in visual perception alter actual data, make pertinent facial information disappear, mask features to varying degrees, or introduce extraneous artifacts in the face image. Existing face recognition algorithms may not be able to provide the desired level of security for such cases.

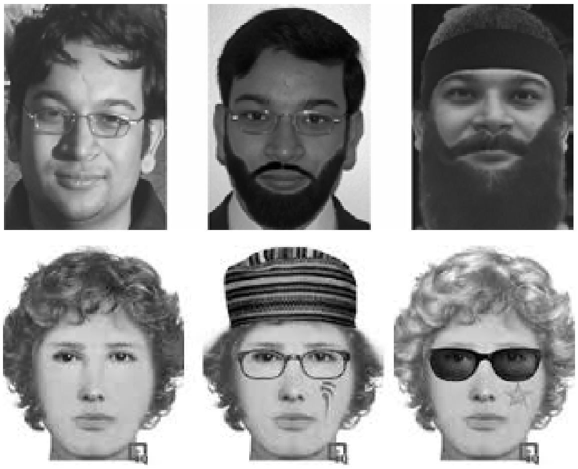


Figure.7 Face Disguise and Synthetic Database: "use of makeup tools and accessories to alter facial features and appearance of the same individual."

Plastic Surgery Database

Facial plastic surgeries [17] have become increasingly popular in the recent past, especially for aesthetic improvement purposes. A report from the American Society of Plastic Surgery states that a total of 13.8 million cosmetic and reconstructive plastic surgeries were performed just in the year 2014. Some of the major facial plastic surgeries include: rhinoplasty (nose surgery), blepharoplasty (eyelid surgery), brow lift (eyebrow surgery), otoplasty (ear surgery), and rhytidectomy (face lift surgery).Figure 8, shows an example images of the plastic surgery databases. Only recently, have researchers from the biometric community begun to study the effect of plastic surgery on face recognition algorithms. Prior to that, research on this topic was stymied by the lack of databases containing pre- and post-surgery face images. The low recognition accuracies that have been reported on this database seem to suggest that the task of face recognition on plastic surgery images is a challenging problem. Based on the results, it is opined that the problem of face recognition using the publicly available plastic surgery database could be further improved if the non-ideal factors (e.g., duplicate entries, low image resolutions, etc.) of the database are accounted for. Future work would include an adaptive fusion scheme (face only, or a combination of face and ocular) for improved identification performance.

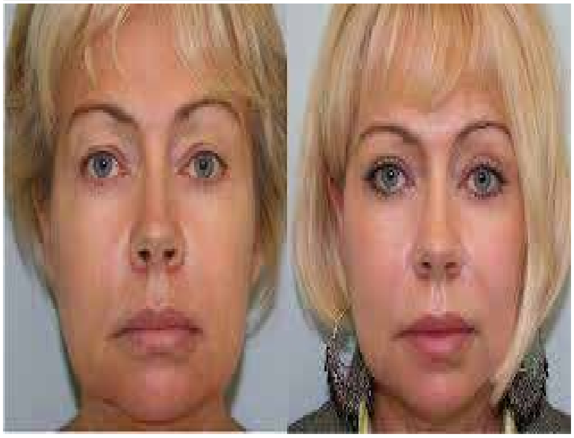
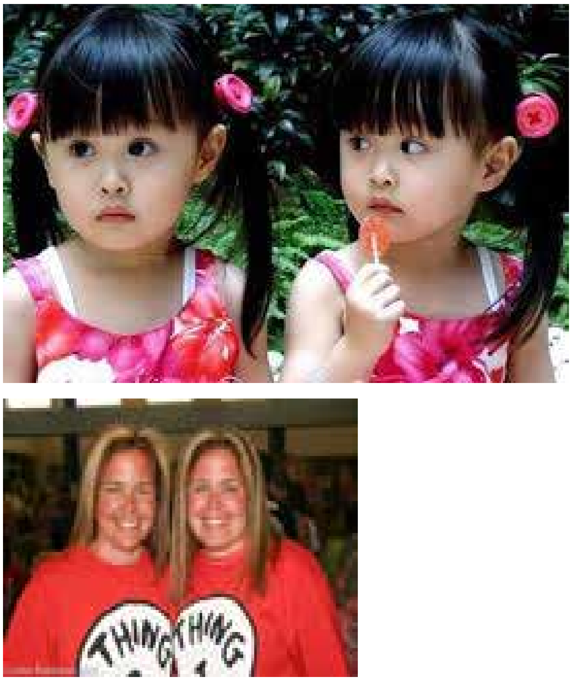


Figure 8: Example images of the Plastic Surgery Database

Challenges

Researchers recently concluded " the facial biometric technologies were not accurate enough to distinguish between pairs of identical twins" ; researchers took photos of over 126 pairs of identical twins in a variety of conditions of varying quality to provide different test conditions for biometric scanners; the photos were tested against three of the highest performing facial recognition and found that under real world circumstances the systems could not accurately distinguish twins; researchers recommend calibrating facial recognition algorithms to analyze minute facial characteristics as well as high-resolution photos to increase accuracy[18]. Researchers recently concluded that facial biometric technologies were not accurate enough to distinguish between pairs of identical twins. Still, the amount of performance improvement so many techniques are uses to researchers like facial mark, facial features an optical recognition principle, facial components, ect.,[19,20,21] features in Twin Vs Twin. Show in Figure.9, an example of twin's images. Future work should involve expanding the twin's similarity datasets to improve for twin identification. New research ideas are needed to help improve performance on recognition of identical twins in realistic imaging contexts. One needs to cope with such factors in order to develop robust twins face recognition systems.



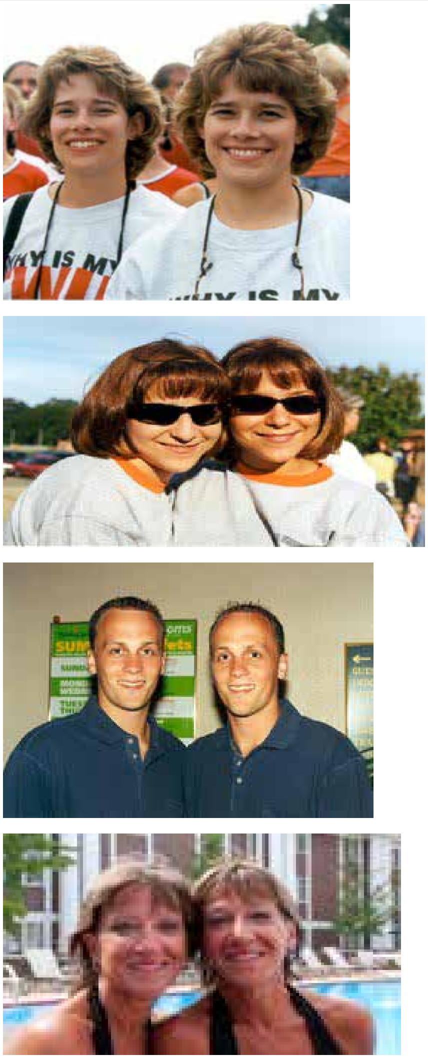


Figure 9: Example images of the identical twins database

Combining twins face recognition with other biometrics

Multi-modal biometric systems, show in Figure.10, flow chart of multi-modal biometric identification- combine evidences from several biometric modalities to establish more reliable and accurate identification. In a multi-modal biometric system [22] (fingerprint, ear, palm print, iris, retina, gait and so on) twins face recognition helps in improving the accuracy of the system when it is integrated with other biometrics. There is no significant difference in the performance a biometric system for the identical twin data and for the general data. So the multimodal can be used to distinguish identical twins as much as it can be used to distinguish any unrelated individuals.

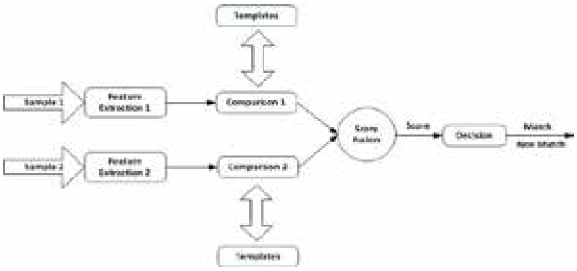


Figure 10: Flow Chart of Multi-Modal biometric identification.

Volume : 4 | Issue : 4 | Apr 2014 | ISSN - 2249-555X

Apart from accuracy improvement, another important benefit of the multi-modal biometric systems is in being more robust against attacks. Indeed, it requires more effort to forge or spoof several biometrics simultaneously compared to only one modality.

4. CONCLUSION

In this paper, the researcher reviewed the main approaches in face recognition databases and recent challenges which are evolved to distinguish between pairs of identical twins. The existing reports about face recognition for identical twins give some encouraging results. The researchers showed that face recognising technology and algorithms are possibly to be a fool proof way to tell the differences between identical twins. The further trends of face recognition in distinguishing between pairs of identical twins must be more accurate in recent machineries. We hope that this design of database will rise up a new era in face recognition techniques and researches.

REFERENCE

1. V. Blanz, S. Romdhami, and T. Vetter, “Face identification across different poses and illuminations with a 3d morphable model,” in Proceedings of Int. Conf. on AutomaticFace and Gesture Recognition, 2002, pp. 202–207. || 2. S. Kumano, K. Otsuka, J. Yamato, E. Maeda and Y. Sato, “Pose-Invariant facial expression recognition using variable-intensity templates,” Int. J. of Computer Vision, 2007, vol. 4843/2007. || 3. N. Ramanathan, R. Chellappa and A.K. Roy Chowdhury, “Facial similarity across age, disguise, illumination and pose,” in Proceedings of Int. Conf. on image Processing, 2004, vol. 3, pp. 1999 – 2002. || 4. S. N. Srihari, H. Srinivasan, G. Fang, “Discriminability of fingerprints of twins,” J. of Forensic Identification, 2007. || 5. S. N. Srihari, H. Srinivasan,”On the discriminability of the handwriting of twins,” J. Forensic Science. 2007. || 6. W. Kong, D. Zhang, G. Lu. “A Study of identical twins' palmprints for personal authentication,” in Proceedings ofICB'2006. pp. 668-674 || 7. K .Hollingsworth, K. W. Bowyer, P. J. Flynn, “Similarity of iris texture between identical twins,” IEEE Computer Society Conf. On Computer Vision and Pattern Recognition Workshops, 2010, pp. 22-29. || 8. “Twins day’s festival official website,” http://www.twinsdays.org/. || 9. A. J. O’Toole, P. J. Phillips, F. Jiang, J. Ayyad, N. Pnard, and H. Abdi, “Face recognition algorithms surpass humans matching faces across changes in illumination,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1642–1646, September 2007. || 10. P. Viola and M. Jones. “Robust real-time face detection,” IJCV, 2004. || 11. A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki. The DET curve in assessment of detection task performance. In Eurospeech’97, pages 1895–1898, 1997. || 12. P. Jonathon Phillips, Hyeonjoon Moon, Syed A. Rizvi, and Patrick J. Rauss. The FERET evaluation methodology for face-recognition algorithms. IEEE Transactions on Pattern Analysis and Machine I\ntelligence, 22(10):1090–1104, 2000. || 13. R. Martinez and R. Benavente, the AR face database. Technical Report 24, Computer Vision. | 14. E. Bailly-Bailliere, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz,J. Matas, K. Messer, V. Popovici, F. Poree, B. Ruiz, and J. P. Thiran. “The BANCA database and evaluation protocol,” in Proceedings of the 4th Int. Conf. AVBPA. 2003, pp. 625–638. || 15. D. Socolinsky, L. Wolff, J. Neuheisel, and C. Eveland. “Illumination invariant face recognition using thermal infrared imagery,” in proceedings of the IEEE Conf. on Computer Vision and Pattern Recognition, 2001. || 16. R. Singh, M. Vatsa and A. Noore, “Face recognition with disguise and single gallery images,” Image and Vision Computing, 2009, vol. 27, pp. 245-257. || 17. R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, “Plastic Surgery: a new dimension to face recognition,” IEEE Computer Society Conf. On Computer Vision and Pattern Recognition Workshops, 2009, pp. 72-77. || 18. P. J. Phillips, P. J. Flynn, K. W. Bowyer, and R. W. V. Bruegge. Distinguishing Identical Twins by Face Recognition. Proc. of IEEE FG. pages 185-192, Mar. 2011. || 19. N. Srinivas, G. Aggarwal, P. J. Flynn, and R. W. V. Bruegge. Facial Marks as Biometric Signatures to Distinguish between Identical Twins. CVPRW. pages 106–113, June 2011. || 20. S. Milborrow and F. Nicolls. Locating facial features with an extended active shape model. ECCV, 2008. || 21. E.W. Kashikokodate, Rieko Inaba and T. Kamiva, “Facial recognition by a compact parallel optical correlator”, Measurement science and Technology, vol.13,Nov 2002. || 22. K. Nandakumar, A. Ross and A. K. Jain, Handbook of Multibiometrics. New York: Springer- Verlag, 2006. |