AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Biometrics Passport Authentication Using Facial Marks

[1]Ziaul Haque Choudhury and [2]M. Munir Ahamed Rabbani

[1]*B.S.AbdurRahman University, Department of Information Technology, Box.600048. Chennai India.*
[2]*B.S.AbdurRahman University, Department of Computer Applications, Box.600048. Chennai India.*

ARTICLE INFO

Article history:
Received 8 August 2014
Received in revised form
12 September 2014
Accepted 22September 2014
Available online 1 November 2014

Keywords:
Face recognition, Facial marks, Soft biometrics, Active Shape Model, Active Appearance Model, and Biometric Passport.

ABSTRACT

A secure biometric passport in the field of personal identification for national security is proposed in this paper. This paper discusses about how to secure biometric passport by applying face recognition. Proper biometric features are unique for each individual and it is invariably in time, it is an unambiguous identifier of a person. But it may fail to authorize a person, if there are some changes in an applicant's appearance, such as a mustache, hair cut, and glasses, etc., the case of similar individuals like twins, siblings, similar faces or even doubles could head to individuality mismatch. Our proposed face recognition method is based on facial marks present in the face image to authenticate a person. We applied facial boundary detection purpose ASM (Active Shape Model) into AAM (Active Appearance Model) using PCA (Principle Component Analysis). Facial marks are detected by applying Canny edge detector and HOG (Histogram Oriented Gradients). Experimental results reveal that our proposed method gives 94 percentage face recognition accuracy, using Indian face database from IIT, Kanpur.

To Cite This Article: Ziaul Haque Choudhury, Biometrics Passport Authentication Using Facial marks. ***Aust. J. Basic & Appl. Sci.,*** *8(16): 40-47, 2014*

INTRODUCTION

Biometric security systems are obtaining a lot of attention because of the potential to increase the reliability and accuracy of identification and authentication functions and in especially in national security, military applications and border crossing. A great deal of research has been executed to measure the operation of biometric systems with a significant on false acceptances and rejections. A lot of research has been executed on the usability and acceptability of biometric authentication systems when applied by Information Technology (IT) professionals and the cosmopolitan public.

Facial images are the most frequent biometric trait used by humans to make an individual authentication. Therefore, the estimate to apply this biometric technology for security purpose. It is a non intrusive method and publicly acceptable system for covert identification applications. Traditional identification documents are now being replaced by electronic documents with biometric features. This enables machine assisted check of a person's identity for both when the document is issued and successively for identity verification explained in T. Bourlai *et al.*(2009;2011). The (ICAO) International Civil Aviation Organization established a particular working group to find out the most desirable way of uniquely encoding a particular physical characteristic of a person into a biometric-identifier that can be machine asserted to confirm the ID holder's identity in ICAO (2003) and M. Ferrara*et al.*(2012). The International Civil Aviation Organization (ICAO) established a specific working group to ascertain the most suited way of uniquely encoding a particular physical feature of a person into a biometric-identifier that can build to confirm the presenter's identity in ICAO (2003). The decision was taken in 2002 in the so-called "Berlin resolution" which states that: A) the face is chosen as the primary globally interoperable biometric characteristic for machine-assisted identity confirmation in machine readable travel documents (MRTDs); B) the Member States have the possibility to use fingerprint and or iris recognition as additional biometric technologies in support of machine-assisted identity confirmation. The ISO/IEC 19794–5 standard (ISO International Standard ISO/IEC JTC 1/SC 37 N506), starting from the guidelines initially proposed by ICAO (2003), fixes rules for recording, encoding, and transmitting the facial image information and determines photographic properties, scene constraints and digital image attributes of facial images. The standard has been in proper order integrated with an amendment in (ISO/IEC 19794–5: 2005/ Amd 1:2007) describing the conditions for taking photographs and two corrigenda (ISO/IEC 19794–5: 2005/Cor 1&2:2008) which relax some of the constraints defined in the first version. An additional document in (ISO/IEC TR 29794-

Corresponding Author: Ziaul Haque Choudhury, B.S.Abdur Rahman University, Department of Information Technology, Vandalur,Chennai, Tamilnadu, Box. 600048, India.
Phone number :+91 9940180311; E-mail – ziaulms@gmail.com

5:2010) has been released and it's aimed at clarifying the terms and conditions that are applicable in the specification, utilize and testing of face image quality metrics and to define the intent, purpose, and interpretation of face image quality scores. Nevertheless, the authors of this document clearly state that performance assessment of quality algorithms and standardization of quality algorithms is outside the scope of the document. The ISO/IEC 19794–5 standard is referred to in the ANSI/NIST-ITL 1–2011 standard format explained in Facial & Other Biometric Information (2011) as one of the standard profiles for face acquisition. Overall, the ISO/IEC 19794–5 standard provides quite generic guidelines and several examples of acceptable/unacceptable face images; a clear and unambiguous description of all the requirements is still missing. A survey about the perception of the image quality as defined by the ISO standard was performed within the project Two Dimensional Facial Image Quality (2DFIQ) illustrated by O. Yuridia and G. Castillo (2006). In this work we proposed a face recognition method based on facial marks as a signature, which will identify the person and differentiate the similar faces.

Problem Definition:

A number of threat scenarios are listed which are relevant for the issuance of travel documents in (http://fpvte.nist.gov/.). The scenarios relevant for the issuing of electronic passports are listed below:

1. Using a fake declared lost/stolen e-passport of somebody who matches the bearer lookalike fraud.
2. Apply for an e-passport with the purpose of selling it to someone who resembles the owner lookalike fraud support.
3. Applying for an e-passport under a fake identity with genuine prove, improperly holder from another individual.
4. Applying for an e-passport under a fake identity, using manufactured prove.

Proposed Method:

Facial photograph of an applicant is utilized as a basic security component. But it may fail to authorize a person, if there are some changes in an applicant's appearance, such as a mustache, hair cut, and glasses, etc., the case of similar individuals like twins, siblings, similar faces or even doubles could head to individuality mismatch. Example, Fig. 1 shows the similar face and Fig. 2 shows the twins. If the facial photo is dealt from a biometric point of view, the face holds information that is constant in time and can be measured in decades. Biometric features are unique to the individual person and it should be constant in time "Generally from a particular age" and it is an unambiguous or an individual identifier of a person. To avoid the threat scenarios from the fake identities, we proposed a secure biometric passport authentication in the field of personal identification for national security. This paper discusses about biometric passport authentication based on face recognition, which focuses on facial marks as a signature. The facial marks can differentiate individual to identify a person. The paper is organized as follows: in Section 3, related work. Section 4, presents the proposed benchmark. Section 5, details the test carried out and discusses the results obtained, and finally Section 7, conclusions.

Fig. 1:

Fig. 2:

Example, Fig.1. Shows similar face and Fig. 2. Shows twins

Related Work:

A number of studies were examined to improve the face recognition by developing features representation schemes. These features include the salient skin regions, which appear on the human face such as scars, moles, freckles, wrinkles, etc. by N. A. Spaun (2007). Previous studies illustrate that facial marks are primarily focused upon in evaluating facial recognition performance using standard face image data set. Park and Jain (2010) expressed that facial marks are very essential in identifying twins using the semi automatic concept. They also labeled the demographic information such as ethnicity and gender. To detect the facial features the authors applied AAM manually and facial marks are detected using LoG and their methods are poor. Fig. 1, shows the example of different kinds of facial marks on the human face. An existing study found that for the face recognition purpose facial marks have been utilized very rarely by J. S. Pierrard and T. Vetter (2007). Also N. A. Spaun (2007; 2009) explained that facial examination has to provide identification of "class" and "individual" characteristics. The 'class' involves the overall facial shape, presence of hair, hair color, shape of nose, presence of marks, etc. Similarly 'individual' characteristics involve the number & location of scars, tattoos, location wrinkles etc. on a face. Lin and X.Tang (2006) first utilized the SIFT operator and D. G. Lowe (2004) to extract facial irregularities and fused them with global face matcher. However, the individual types of facial marks are not defined. Therefore, their method is not suitable for face database indexing. J.E. Lee *et al* (2008) introduced "scars, marks, and tattoos (SMT)" in their tattoo based image retrieval system. While tattoos can exist on any body part and are more descriptive, we are interested in marks appearing exclusively on the face, which typically show simple morphologies. J. S. Pierrard and T. Vetter (2007) proposed a method to extract moles using normalized cross correlation methods and a morphable model. They claimed that their method is pose and lighting invariant since it uses a 3D morphable model. They did not consider other types of facial marks besides moles. Our previous work based on facial marks detection from cosmetic applied faces and low quality image illustrated in Ziaul Haque Choudhury and K.M. Mehata (2012; 2013) has extended for biometrics passport security purpose and it improves the accuracy.

Facial Marks Present on the Face:

Facial marks are present in different regions on the face. To know the different categories of facial marks present in face, we need to analyze the categories of marks. Different kinds of facial marks are freckle, mole, scar, pockmark, acne, whitening, dark skin, etc. Freckle is a single or a set of dark spots present in the face. Wherever there was a dense set of spots we labeled them in a single bounding box. A mole typically appears large in size and darker in color compared to the other spots. Scar represents the discolored skin in the region due to a cut or injury. Acne is a red region caused due to a pimple and is stable for a few days to several months. Whitening represents a skin region that appears brighter in contrast with the surrounding region. We took into consideration the wrinkles that are larger and omitted the smaller wrinkles near the eyes and mouth. We also ignored the beard and facial hair in constructing the ground truth. All other kinds of marks which are not mentioned above are labeled under the "others" group. Fig.3 shows the different marks present on the face.

Fig. 3: Different facial marks on the face image

Facial Marks Detection Method:

The proposed mark detection method is based on the Histogram Oriented Gradients (HOG) by Navneet Dalal and Bill Triggs (2005) and O. Déniz *et al*(2011) that detect local silent points from the input image. Therefore, to detect the facial feature, it will increase the local extrema of facial features such as eyes, eyebrows, nose, and mouth. To avoid detecting unwanted local facial features we subtracted eyes, eyebrows, nose, and mouth from the face image using ASM in AAM using PCA also detects the facial landmark and we provide masking process using John Canny (1986). The complete facial mark detection process is illustrated in Fig.4

with the following steps, Facial feature detection, Designing the mean shape and mask construction, Histogram Oriented Gradients (HOG),Blob classification for facial marks and Experimental Results.

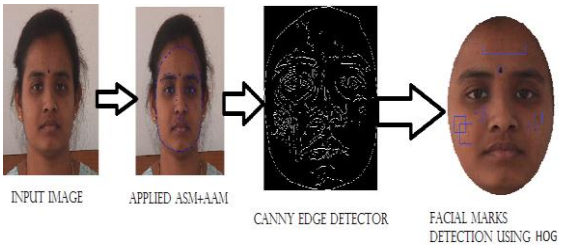

Fig. 4: Facial marks detection process

Facial Feature Detection:

By applying the Active Shape Model (ASM) into Active Appearance Model (AAM) using PCA proposed by Jaewon sung *et al* (2007) to detect automatically 120 landmarks that delineate the facial features such as the mouth, nose, eyes, eyebrows and face boundary. First detect the landmarks of two eyes, nose, mouth and face boundary. These facial features will be disregarded in the subsequent facial mark detection process. ASM into AAM identifies both the shape and texture of face images using the Principle Component Analysis (PCA). ASM finds the shape parameters so that the profile of each model is similar to the pre-learned profile. It is another way of keeping the shape parameter within the learned range in the parameter space. Similarly, AAM finds the shape and appearance model parameters such that the model instance is most similar to the input image. Models that are obtained from the current model parameter are as similar as the input image. ASM and AAM are hence combined to reduce the error rate and detect the face with perfect landmark points.

Designing Mean Shape and Mask Construction

Active Shape Model in Active Appearance Model has been applied to detect the landmarks, thereby to simplify the mark detection. We then map each face image to the mean shape. Consider that S_i where i=1,2…,N represents the shape of each of the N face images in the database (gallery) based on the 120 landmarks. The mean shape is calculated using the equation $S_\mu = \sum_{i=1}^{N} Si$.

Each face image S_i is mapped to the mean shape S_μ by using the Barycentric coordinate-based proposed by Samuel Morillas *et al* (2011) texture mapping process. We construct a generic mask and derive a user specific mask to suppress false positive value detection around the facial feature. The user specific mask covers small unusual landmarks around the facial feature. We suppress the false positives of small wrinkles or beard that are connected to the facial feature. We then build a user specific mask from the edge image obtained using the canny edge detector by John Canny (1986).

Histogram Oriented Gradients (HOG):

Histogram Oriented Gradients (HOG) algorithm proposed by Dalal and Trigs (2005), the author highlights that their method is well suited to robustly extract the features from the visual object recognition. The HOG descriptor can be computed as follows. The gradient of the image is computed and the phase is quantized according to a predefined number of orientation intervals, which will represent the bins in the histogram. Thereafter the image is divided into small regions called cells from which the orientation histogram is built by the votes of the quantized orientation of each pixel. These votes are weighted by the magnitude of the gradient for each pixel. Subsequently cells are grouped in blocks which are the normalization units of the algorithm. This normalization constitutes an important part of the algorithm, because it represents a smoothing factor and limits the effect of the variations of the gradient in local areas due to illumination and object/background contrast. Finally the descriptor is created by the concatenation of the block-normalized histograms of all the cells. The descriptor is tuned mainly by four parameters, namely the number of orientation bins, the size of the cells, the size of the blocks and the overlap factor. These parameters change the resolution of the grid, thus changing the quality of the descriptor, making the selection of their values important to a well adjusted description of the object. Other parameters include the range and sign of the orientations to consider and the normalization rule. These two were set to the values suggested by the authors to perform the best.

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 40-47

Blob Classification for Facial Marks:

Each detected local extrema such as Marks, Moles, freckles, etc. are assigned that bounding box. Pixels in the bounding box are binarized with a threshold value selected from the mean value of the surrounding pixels. Local extrema is brighter or darker than its surrounding region, so the average value of the surrounding area can serve effectively for fixing the bounding box. We then classify a mark in a hierarchical fashion: linear versus all, followed by circular point versus irregular. In the linearity classification of a blob, λ_1 and λ_2 are the two eigen value that we obtained from the eigen decomposition on the x and y coordinates of blob pixels. When λ_1 is larger than λ_2, the mark is considered as a linear blob. We calculate the second moment of the blob pixels M_2 for the circularity detection. A circle RM_2 with radius M_2 will enclose most of the blob pixels if they are circularly distributed. Therefore, a decision can be made based on the ratio of the number of pixels within and outside of RM_2. Fig. 7 elaborates facial marks detection results using our new method.

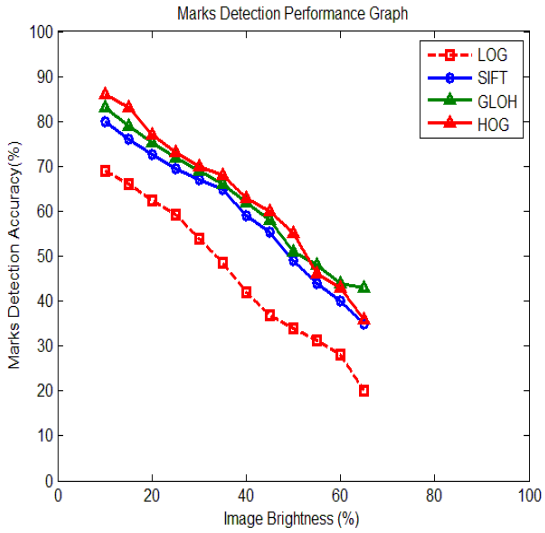

Fig. 5: Marks detection performance graph

LOG, SIFT, GLOH -- the existing mark detection performance.
HOG -- the proposed mark detection performance.

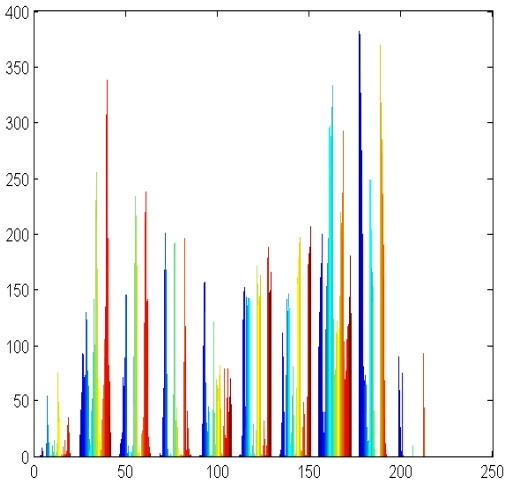

Fig. 6: Histogram of color face image

Mark detection performance is evaluated in terms of mark detection accuracy and image brightness, as shown in fig. 5. In Y axis carried out the mark detection accuracy in percentage and X axis carried out the image brightness level in percentage. In Y axis the number of marks which are detected from the face image with the adjustment of image brightness increments. The brightness, contrast increased up to 0 to 65 percentages. According to brightness percentage the marks detection has been changed. The marks have been detected 69% when the contrast level 10% and 26% for the contrast level 65% in LoG. For SIFT, marks are detecting 80% to

Australian Journal of Basic and Applied Sciences, 8(16) October 2014, Pages: 40-47

37% with image brightness level 10% to 65% in existing work and in our proposed work it detects 86% to 43% with image brightness level 10% to 65%. The mark detection performance graph in fig. 5, shows that the marks detection accuracy of our method is better than existing marks detection accuracy. This helps to improve the face recognition accuracy. Fig.6 shows the histogram present on the color face image and it is plotted.

Fig. 7: Examples of facial marks which are detected from face image.

Experimental Results:

Database:

We named the face images, data set which contains an Indian face database collected from IIT, Kanpur (http://www.face-rec.org/databases/) and named as DB1 and DB2. DB1 and DB2 are used to evaluate the proposed mark-based matcher. DB1 and DB2 are used to evaluate the proposed mark-based matcher. We gathered 1000 images to demonstrate the proposed facial mark detection method. The image size in our database is 640*480 (width * height) with 96 dpi resolution. We manually labeled different types of facial marks as ground truth. This process allows us to evaluate the proposed facial marks extraction method. DB1 is used to evaluate the effectiveness of the indexing scheme to improve the facial individuality. The soft biometric traits based matcher is used to retrieve the data from the database.

Image Matching and Retrieval for Security:

We applied our marks based matcher on facial images to identify the human face. The soft biometric matcher successfully retrieves the correct images to probe the face images. The facial feature points are manually labeled with 120 landmarks for the partial face and automatically labeled for the database images. Fig. 8 shows the face matching and retrieval results in which all the marks are detected automatically from the database. As some of the facial marks are not stabilized in our face for example pimples, acne or zits, problems occurred during the matching. To enhance the matching accuracy, we fixed up the permanent marks such as moles, scar, birth marks etc. on the face image. It improves the recognition or identification of the particular person. Our method detects majority of the facial marks from a low quality face image. We simply filtered out the unnecessary facial edges. It also improved the matching accuracy and enhances the results. Our proposed mark detection method is implemented using Matlab 7.10.0 (R2010a).

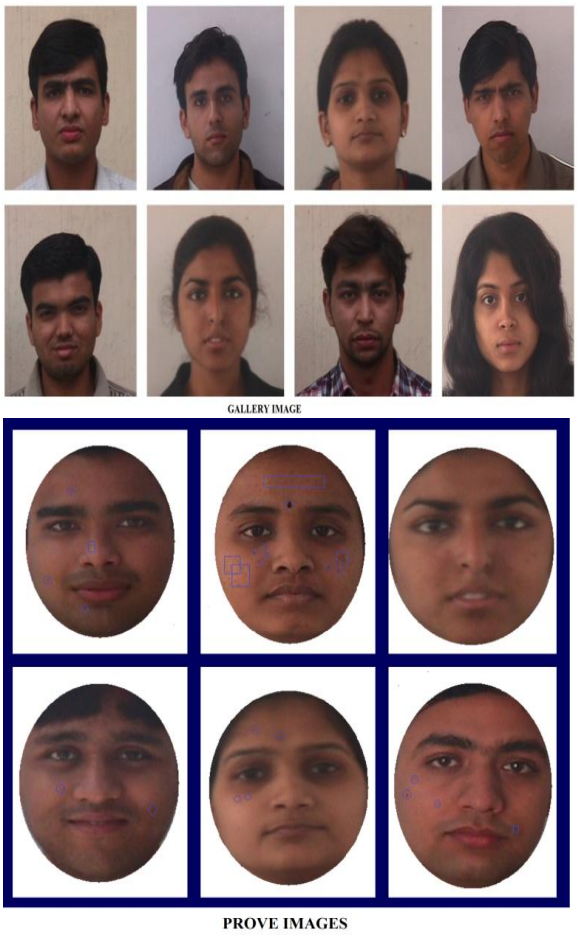

Fig. 8: Face matching and retrieval results

Conclusions:

To avoid the threat scenarios from the fake identities, we proposed a secure biometric passport in the field of personal identification for national security. This paper discussed about biometric passport authentication and focused on face recognition which is based on facial marks as a signature. It differentiates easily similar faces and twins by applying our algorithm. Here we consider that a means of identifying travelers with biometrics should be used in worldwide. We projected an authentication methodology based on facial marks as a signature to authenticate individuals. Our face recognition technique achieved 94%. We are focusing on security and privacy for future enhancement of RFID and we will improve the RFID security issues.

REFERENCES

Ajay Kumar and David Zhang, 2010. Improving Biometric Authentication Performance from the User Quality, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, 59: 3.

Albrecht, A., M. Behrens, T. Mansfield, M. Mc Meechan, M. Rejman-Greene (Ed.), M. Savastano, C. Schmidt, B. Schouten, P. Statham, M. Walsh, 2003. Roadmap to successful deployments of biometrics from the user and system integrator perspective, Technical report, Centre for Mathematics and Computer Science, CWI Report PNA-E0303, ISSN 1386-3711.

ANSI/NIST-ITL 1–2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information 2011.

Biometric Deployment of Machine Readable Travel Documents, ICAO 2003.

Bourlai, T., A. Ross and A.K. Jain, 2009. On matching digital face images against passport photos, in Proc. IEEE Int. Conf. Biometrics, Identity and Security, Tampa, FL.

Bourlai, T., A. Ross and A.K. Jain, 2011. Restoring degraded face images for matching faxed or scanned photos, IEEE Trans. Inf. Forensics Security, 6(2): 371-384.

Déniz, O., G. Bueno, J. Salido, F. De la Torre, 2011. Face recognition using Histograms of Oriented Gradients, Pattern Recognition Letters, 32: 1598-1603.

Ferrara, M., A. Franco and D. Maio, 2012. A multi-classifier approach to face image segmentation for travel documents, Expert Systems with Applications, 39(9): 8452-8466.

http://fpvte.nist.gov/.

http://www.face-rec.org/databases/

ICAO, 2003. Biometric Deployment of Machine Readable Travel Documents.

ISO International Standard ISO/IEC JTC 1/SC 37 N506, Text of FCD 19794–5, Biometric Data Interchange Formats—Part 5: Face Image Data 2004 [Online]. Available: http://isotc.iso.org.

ISO/IEC 19794–5: 2005/Amd 1:2007, Information Technology—Biometric data Interchange format—Part 5: Face Image Data/Amendment 1: Conditions for Taking Photographs for Face Image Data 2007.

ISO/IEC 19794–5: 2005/Cor 1&2:2008, Information Technology—Biometric Data Interchange Format—Part 5: Face Image Data, 2008, Technical Corrigendum 1&2.

ISO/IEC TR 29794-5:2010, Information Technology—Biometric Sample Quality—Part 5: Face Image Data 2010.

JAEWON SUNG, TAKEO KANADE, DAIJIN KIM, 2007."A Unified Gradient-Based Approach for Combining ASM into AAM" International Journal of Computer Vision., 75(2): 297-309.

John Canny, 1986. A computational approach to edge detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-8, No.6.

John Canny, 1986. A computational approach to edge detection, IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-8, No.6.

Lee, J.E., A.K. Jain and R. Jin, 2008. Scars, marks and tattoos (SMT): Soft biometric for suspect and victim identification, in Proc. Biometric Symposium, Biometric Consortium Conf., pp: 1-8.

Lin, D. and X. Tang, 2006. From macrocosm to microcosm. In Proc. CVPR, pp: 1355-1362.

Lowe, D.G., 2004. Distinctive image features from scale invariant keypoints, International Journal of Computer Vision, 60(2): 91-110.

Navneet Dalal and Bill Triggs, 2005. Histograms of oriented gradients for human detection. In Cordelia Schmid, Stefano Soatto, and Carlo Tomasi, editors, International Conference on Computer Vision and Pattern Recognition, vol.2, pp.886-893, INRIA Rhone-Alpes, ZIRST-655, av. de l'Europe, Montbonnot-38334.

Park, U. and A.K. Jain, 2010. Face matching and retrieval using soft biometrics, IEEE Transactions on Information Forensics and Sec-urity, 5(3): 406-415.

Pierrard, J.S. and T. Vetter, 2007. Skin detail analysis for face recognition. In Proc. CVPR, pp: 1-8.

Samuel Morillas, Valent´ın Gregori and Almanzor Sapena, 2011. Adaptive Marginal Median Filter for Colour Images, Sensors, 11: 3205-3213; oi:10.3390/s110303205

Spaun, N.A., 2007. Forensic biometrics from images and video at the Federal Bureau of Investigation, in Proc. BTAS, pp: 1-3.

Spaun, N.A., 2009. Facial comparisons by subject matter experts: Their role in biometrics and their training, in Proc. ICB, pp: 161-168.

Yuridia, O. and G. Castillo, Survey About Facial Image Quality, 2006.Fraunhofer Institute for Computer Graphics Research.

Ziaul Haque Choudhury, K.M. Mehata, 2012. Robust facial Marks detection method Using AAM and SURF, in IJERA, pp: 708-715.

Ziaul Haque Choudhury, K.M. Mehata, 2013. Biometrics Security: Facial Marks Detection from the Low Quality Images, in International Journal of Computer Applications (0975 – 8887), 66: 8.