IJITKM ISSN 0973-4414 Volume 6 • Number 2 • July-December 2013 pp. 176-181

Can Soft Biometric Traits assist Face Identification System?

Dr. Sheetal Chaudhary
Asst. Prof, Department of Comp. Sc. & App. K.U., Kurukshetra, Haryana, INDIA

Abstract: An automatic personal identification system based only on physiological (face, fingerprint, iris, palmprint, etc.) or behavioral (signature, keystroke dynamics, etc.) trait is often not able to meet the system performance requirements. Also soft biometric traits like age, gender, height, weight and eye color alone does not provide unique and reliable person recognition because they lack distinctiveness and permanence. However, soft traits can assist the identity information provided by the primary biometric traits. This paper describes a hybrid biometric system that uses face as primary biometric trait and age, gender as soft biometric traits. Face is one of the most important biometric features of human and contains lots of useful information such as gender, age, ethnicity and skin color. In this paper, a framework is presented for automatically extracting the ancillary information (age and gender) from face image and using them as filter for large face biometric database. It reduces the number of entries to be searched in the database. This greatly improves the speed of the primary face identification system.
Keywords: Face identification, soft biometric traits, facial feature extraction, age extraction, gender classification.

I. INTRODUCTION

Biometrics refers to identification of an individual based on his physiological or behavioral characteristics. Biometrics relies on “something which you are or you do” to make a personal identification and, therefore, inherently has the capability to differentiate between a genuine individual and a fraudulent impostor [1]. Traditional personal identification approaches which use “something that you know,” such as a Personal Identification Number (PIN), or “something that you have,” such as an ID card are not sufficiently reliable to satisfy the security requirements because they lack the capability to differentiate between a genuine individual and an impostor who fraudulently acquires the access privilege [2]. With increased need for reliable authentication schemes, the use of automatic identification systems based on biometrics has become widespread. Any human physiological or behavioral characteristic can be used as a biometric trait to make a personal identification as long as it satisfies the following requirements [3]:

- Universality: every person should possess the trait;
- Uniqueness: no two persons should be the same in terms of the trait;
- Permanence: the trait should be invariant with time;
- Collectability: to acquire and digitize the trait without causing any inconvenience to user;
- Performance: which refers to the achievable recognition accuracy and speed, robustness, the resources required to achieve the accuracy and speed;
- Acceptability: which indicates the extent to which people are willing to accept a particular biometric trait in their daily life; and
- Circumvention: which reflects how easily the system can be fooled by using fraudulent methods.

A. Face Recognition

Though people are good at face identification, recognizing human face automatically by computer is very difficult. Face recognition is influenced by many complications, such as the differences of facial expression, the light directions of imaging, and the variety of posture, size and angle. Even to the same people, the images taken in different surroundings may be unlike. Facial feature extraction has become an important issue in automatic recognition of human faces. Detecting the basic features as eyes, nose and mouth exactly is necessary for most face recognition methods [4]. Face recognition scenarios can be classified into two types: face verification and face identification [5]

1) Face verification (”Am I who I say I am?”) is a one-to-one match that compares a query face image against a template face image whose identity is being claimed.
2) Face identification (”Who am I?”) is a one-to-many matching process that compares query face image against all the template images in a face database to determine the identity of the query face. The identification of the test image is done by locating the image in the database which has the highest similarity with the test image.

B. Soft Biometric traits

Any trait that provides some information about the identity of a person, but does not provide sufficient evidence to precisely determine the identity can be referred to as soft biometric trait. Examples of soft traits are gender, age, skin color, height, weight, and eye color etc (figure 1). Soft traits like age, gender, and ethnicity can be automatically extracted with sufficient reliability from the face images. These secondary attributes can be used along with the primary biometric system to accurately identify the person. Soft biometric information assists the identity information provided by primary biometric traits such as fingerprint, iris, and voice etc. Utilizing soft biometric traits improves the recognition accuracy of primary biometric systems [6].

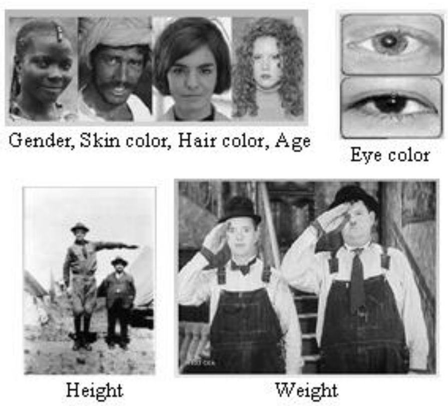

Fig.1. Examples of soft biometric traits

This paper introduces a hybrid biometric system, which makes personal recognition by extracting age and gender from facial image. The proposed biometric system operates in the identification mode. It automatically extracts ancillary information from input face image and incorporates age and gender classifiers to improve the identification performance. The rest of the paper is organized as follows. Section 2 addresses the literature study. In section 3 face feature set extraction technique is discussed. Sections 4 and 5 describe the soft traits and their automatic extraction from face feature set. Proposed system architecture with age and gender classifiers is discussed in Section 6. Finally, the summary and conclusions are given in Section 7.

II. RELATED WORK

In recent years face recognition has received substantial attention from both research communities and the market, but still remained very challenging in real applications. A lot of face recognition algorithms have been developed during the past decades. Face recognition consists in localizing the most characteristic face components (eyes, nose, mouth, etc.) within images that depict human faces [7]. Hong and Jain [8] designed a decision fusion scheme to combine faces and fingerprint for personal identification. Brunelli and Falavigna [9] presented a person identification system by combining outputs from classifiers based on audio and visual cues. Face recognition algorithms are categorized into appearance based and model-based schemes. For appearance-based methods, three linear subspace analysis schemes are presented (PCA, LDA, and ICA) [5].The model-based approaches include Elastic Bunch Graph matching [10], Active Appearance Model [11] and 3D Morphable Model [12] methods. Among face recognition algorithms, appearance-based approaches are the most popular. These approaches utilize the pixel intensity or intensity-derived features. There are a large number of commercial, security, and forensic applications requiring the use of face recognition technologies. These applications include automated crowd surveillance, access control, security system, credit-card verification, criminal identification, design of human computer interface (HCI), and content-based image database management [5].

Soft biometric information can be automatically extracted and utilized to establish the user’s identity. Automatic and reliable extraction of soft biometric traits is a difficult task. A number of techniques have been proposed in the literature for extracting soft biometric information. Wayman, 2000[13] proposed the use of soft biometric traits like gender and age, for filtering a large biometric database. Gutta et al., 2000 [14] proposed a mixture of experts consisting of ensembles of radial basis functions for the classification of gender, ethnic origin, and pose of human faces. Balci and Atalay, 2002 [15] reported gender classification that uses PCA for feature extraction. Moghaddam and Yang, 2002 [16] show that the error rate for gender classification can be reduced by using support vector machines. Kwon and Lobo, 1994 [17] present an algorithm for age classification from facial images based on cranio-facial changes in feature-position ratio and skin wrinkle analysis. Lanitis et al., 2004 [18] performed a quantitative evaluation of the performance of various classifiers developed for automatic age estimation from face images.

III. FACIAL FEATURE SET EXTRACTION

To recognize human faces, the prominent characteristics on the face like eyes, nose and mouth (figure 2) are extracted together with their geometry distribution and the shape of face. Human face is made up of eyes, nose, mouth and chin etc. There are differences in shape, size and structure of these organs, so the faces are different in thousands ways, and we can describe them with the shape and structure of these organs in order to recognize them.

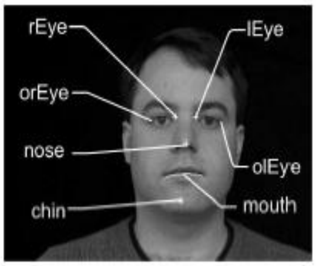

Fig.2. Feature point locations, rEye – Inside of the right eye; orEye - Outside of the right eye; lEye - Inside of the left eye; olEye - Outside of the left eye; nose - Nose tip; chin - chin tip; mouth - corners and middle of the mouth [19].

These feature points and relative distances between them make some patterns in every input signal. These characteristic features are called eigenfaces in the facial recognition domain (or principal components generally) [4] [20]. They can be extracted out of original image data by means of some mathematical tools like PCA, ICA, and LDA. In our proposed system PCA is used for face recognition. By means of PCA, each original image can be transformed into a corresponding eigenface. The eigenface approach is used because it has a compact representation so the facial image can be concisely represented by a feature vector with a few elements, and above all retrievals can be made efficiently in databases indexed with eigenface-based templates. The eigenface-based face recognition consists of the following two stages [7]:

1) training stage, in which a set of N face images are collected; eigenfaces that correspond to the M highest eigenvalues are computed from the data set; and each face is represented as a point in the M dimensional eigenspace, and
2) operational stage, in which each test image is first projected onto the M-dimensional eigenspace; the M dimensional face representation is then deemed as a feature vector and fed to a classifier to establish the identity of the individual.

In this approach, the 2-dimensional face image is considered as a vector, by concatenating each row (or column) of the image. By projecting the face vector to the basis vectors, the projection coefficients are used as the feature representation of each face image. Let $X = (x_1,x_2,\ldots,x_i,\ldots,x_n)$ represent the $n \times N$ data matrix, where each x_i is a face vector of dimension n, concatenated from a $p \times p$ face image, where $p \times p = n$. Here n represents the total number of pixels in the face image and N is the number of face images in the data set. The mean vector μ of the training images is subtracted from each image vector, where μ

$$\mu = \sum_{i=1}^{N} X_i \qquad \ldots. (1)$$

The Principal Component Analysis basis vectors are defined as the eigenvectors of the scatter matrix S,

N

i=1

$$S = \Sigma\, (X_i-\mu)\, (X_i-\mu)^T \qquad \ldots. (2)$$

The principal directions of S are the eigenvectors corresponding to the M largest eigenvalues of S, M << N. For each image X, we obtain a feature vector Y by projecting X onto the subspace generated by the principal directions. After applying the projection, the input vector (face) in an n-dimensional space is reduced to a feature vector in an m-dimensional subspace [8].

IV. AUTOMATIC AGE EXTRACTION

This section discusses visual age classification from facial images. Currently, this concept has only been implemented to classify input images into one of three age groups: babies, adults, and senior adults [17]. In the proposed system the age group of babies is further categorized into children and young. Cranio-facial development theory and skin wrinkle analysis are used for visual age classification. It proceeds by first determining primary features of the face followed by secondary feature analysis. The primary features are the eyes, nose, mouth, chin, virtual-top of the head and the sides of the face. From these features, ratios that distinguish all age groups are calculated. In secondary feature analysis, a wrinkle geography map is used to guide the detection and measurement of wrinkles. The wrinkle index computed in secondary feature analysis is sufficient to distinguish all age groups from each other. To categorize a face into one of the age groups a combination rule is used for combining ratios and wrinkle index.

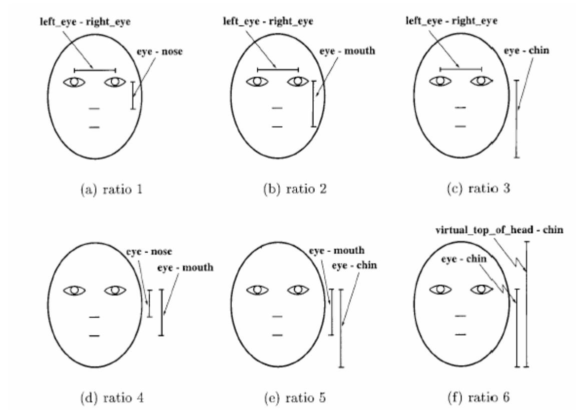

Fig.3. Six ratios used for visual age classification

To distinguish baby faces from the two older groups, a set of ratios has been calculated which are shown in figure 3.These ratios only require the automatic localization of primary features, namely the eyes, nose, mouth, chin, and virtual top of the head. Ratio 1 is the T -ratio formed by two segments: the segment T1 joining the two eyes and the segment T2 between the midpoint of T1 and the nose. Ratio 2 is the T -ratio formed by two segments: the segment T1 as above, and the segment T3 between the midpoint of T1 and the mouth. Ratio 3 is the T -ratio formed by two segments: the segment T1 as above, and the segment T4 between the midpoint of T1 and the chin. Ratio 4 is the ratio of the segment representing the difference in height between nose and eye-midpoint, and the segment representing the difference in height between mouth and eye-midpoint. Ratio 5 is the ratio of the segment representing the difference in height between mouth and eye-midpoint, and the segment representing the difference in height between chin and eye-midpoint. Ratio 6 is the height of the eyes within the top and bottom head-margins. Once the primary features have been found for the face, the wrinkle index is computed based upon the wrinkle geography map (figure 4) that is made in the secondary feature analysis. It is used to search for wrinkles. To capture wrinkle information from face images, it is necessary to zoom in to the areas depicted by the wrinkle geography to capture further detail. Finally the combination rule is applied for all the age groups to be categorized.

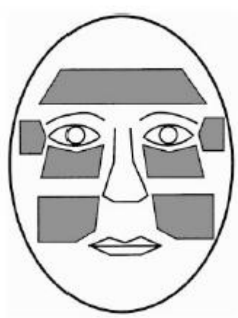

Fig.4. Wrinkle geography showing the regions that are searched for facial wrinkles, after the primary features of the face have been located.

V. AUTOMATIC GENDER EXTRACTION

Gender classification is to tell the gender of a person according to his/her face. Visual information from human faces provides one of the more important sources of information for gender classification. The system consists of mainly three modules, face detection, normalization and gender classification. Face detection is the fundamental module of almost all face information processing systems. The input is gray-scale digital image. First, a detector is used to scan the image to locate face. Then three important facial landmark points (two eye centers and the mouth center) are extracted from each face and thereby it is aligned geometrically and further adjusted in illumination to generate a normalized face sample (figure 5). Finally, the normalized sample is fed into the gender classifier [21].

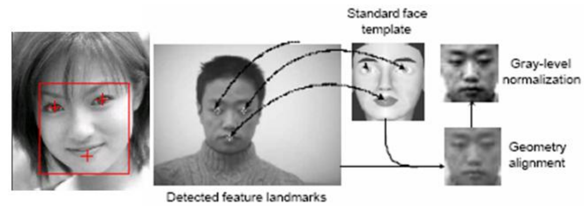

Fig.5. Facial landmark detection and Face sample normalization

In the proposed system we are using Support Vector Machine [16] [22] as the two-class gender classifier. SVM is an optimal discriminant method based on the Bayesian learning theory. We have focused our study on images in which only the main frontal facial regions (inside the oval of face) are visible and almost completely excluded hair information (outside the oval). Hairstyles can change in appearance easily and frequently; therefore, in robust face identification system face images are usually cropped to keep only the main facial regions. Given a set of samples, which belong to either of two classes, SVM finds the hyper-plane leaving the largest possible fraction of points of the same class on the same side, while maximizing the distance of either class from the hyper-plane. Assuming m examples from two classes $(x_1,y_1)(x_2,y_2)\ldots(x_m,y_m)$, $x_i \in R^N, y_i \in \{-1,+1\}$ computing the optimal hyper-plane implies solving a constrained optimization problem using quadratic programming. The discriminate hyper-plane is defined as:

$$f(x) = \sum_{i=1}^{m} y_i a_i k(x,x_i) + b \qquad \ldots (3)$$

Where $k(x,x_i)$ is a kernel function and the sign of $f(x)$ indicates the membership of x. Constructing the optimal hyper-plane is equivalent to finding all the nonzero a_i. Any data point x_i corresponding to a nonzero a_i is a support vector of the optimal hyper-plane. An input facial image x generates a scalar output $f(x)$ whose polarity (sign of $f(x)$) determines class membership.

VI. PROPOSED SYSTEM

This section describes the working of the proposed system. The proposed system improves the performance of primary face identification system by incorporating age and gender as soft biometric traits. They are automatically extracted from the facial feature set during the enrollment phase and work as filter for large face database. Filtering means limiting the number of entries in the database to be searched based on some characteristics of the user (age and gender) to be identified. If the user is identified as a middle-aged female, the search will be restricted only to the subjects with this profile enrolled in the database. It is assumed that the entries in the database are appropriately tagged with these attributes (age and gender). Filtering greatly improves the speed or the search efficiency of the primary face identification system. Logically, it can be divided into two modules:

1) Enrollment module
2) Identification module

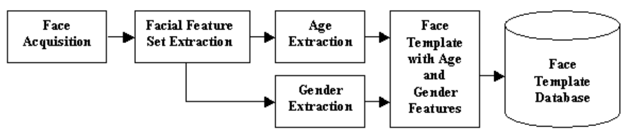

Fig.6. Proposed Enrollment process

During the enrollment phase (figure 6), the face of an individual is captured by a camera to produce a digital representation of the biometric characteristic. Any camera (with a sufficient resolution) can be used to capture the image of the face. The proposed facial identification system uses only the gray-scale information. The lighting conditions required are mainly dependent on the quality of the camera used. It requires the user to stand a specific distance away from the camera and look straight at the camera. This ensures that the captured image of the face is within a specific size tolerance and keeps the features (e.g., the eyes) in as similar position each time as possible. To facilitate the matching and the identification process, the digital representation is further processed by a feature extractor to generate a template. The extraction of facial components means to locate certain characteristic points, e.g. the center and the corners of the eyes, the nose tip, the center and the corners of the mouth, the chin tip, the top of the head etc as shown in figure 2. After facial feature set extraction, age and gender (soft traits) are automatically extracted from it without causing any inconvenience to the user. The templates to be stored in the database contain facial feature components along with age and gender of the individual. Automatically extracted soft traits will be utilized during matching and decision making processes to improve the overall performance of the primary face identification system.

The identification module (figure 7) is responsible for identifying individuals at the point-of-access. In the operational phase, the biometric reader captures the primary characteristic (face) of the individual to be identified and converts it to a raw digital format, which is further processed by the feature extractor, age extractor and gender extractor to produce a compact representation that is of the same format as the template. The resulting representation is then fed to the gender and age classifiers shown in figure 8. These extracted soft traits will work as filter for large face database. Gender classifier will tell the gender of the individual. Only those templates whose gender class is matched with the gender of the individual to be identified will be retrieved from the database. Now comes the role of age classifier. Age classifier will tell the category (children, young, adult, senior adult) of the individual depending upon the age group which matches with the age of the individual.

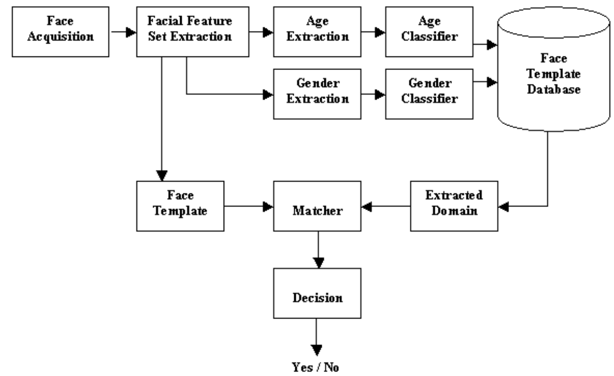

Fig.7. Proposed Face Identification system

Extracted domain will contain only those templates which are filtered by the gender and age classifiers. The role of soft biometric traits has now been completed with the extraction of selected templates filtered by gender and age classifiers.

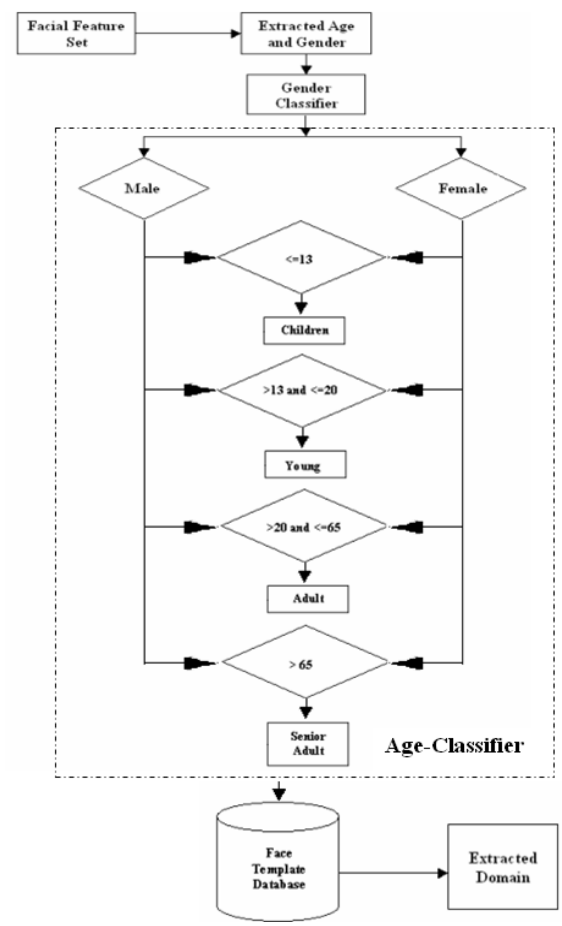

Fig.8. Gender and Age classifiers

Now the input face template is compared with only the templates filtered by classifiers in the extracted domain to establish the identity. By incorporating soft biometric traits (age and gender) into the primary face identification system, lots of comparisons got reduced and also enhanced the system performance.

Let us take a simple example to calculate the performance of the proposed system as compared to the existing system. Assume there are 10^6 (1000000) templates in the database and for scanning a single template of face in database, it takes t μ sec.

Efficiency of existing system:

Calculation for the worst case:

Time taken = 10^6 X t μ sec.

Now we will calculate the efficiency of proposed system with following assumption:

For Gender classifier:

Assume 50% templates are male and 50% are female.

For Age classifier:

Assume 5% templates are children, 20% are young, 50% are adult, and 25% are senior adult.

At gender level ½ of input templates get filtered and $10^6/2$ templates will be again filtered by age classifier as follows:

Average of ($10^6/2$ X 5% + $10^6/2$ X 20% + $10^6/2$ X 50% + $10^6/2$ X 25%) = 125 X 10^3 templates.

Calculation for the worst case:

Time taken = 125 X 10^3 t μ sec.

$$\text{Efficiency} = \frac{\text{Time taken by proposed system}}{\text{Time taken by existing system}}$$

$$\text{Efficiency} = \frac{125 \text{ X } 10^3 \text{ t } \mu \text{ sec}}{10^6 \text{ X t } \mu \text{ sec}} = \frac{1}{8}$$

This proves that the proposed system is 8 times faster than the existing system. We can also further improve the efficiency of proposed system by categorizing the age classifier into more classes, but it will increase the system complexity.

VII. CONCLUSION

It is well known that soft biometric traits like gender, age, height, weight, ethnicity, and eye color cannot provide reliable user recognition because they are not distinctive and permanent as the primary biometric traits like fingerprint, face, hand geometry, iris etc. However, such ancillary information can assist the identity information provided by the primary biometric traits to establish user identity with higher accuracy. In this paper, we have proposed a hybrid biometric system that uses face as the primary characteristic and age, gender as the soft characteristics. Soft biometric information is automatically extracted from the face image and it works as a filter for the large face biometric database. It has reduced the number of entries to be searched in the database for establishing a user's identity and has increased the search efficiency of the primary face identification system. To compare the efficiency of proposed system with the existing system, calculations are done by assuming data and it has been found that the proposed system gives a significant improved recognition performance over the existing system. Hence the recognition performance of the primary biometric system can be improved significantly by making use of soft biometric information. Face recognition systems are among the top choices for reliable authentication because face recognition is friendly and non-invasive with high universality, collectability and acceptability. Our future work will be focused on integrating liveness detection with biometric recognition systems.

REFERENCES

[1] A.K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Norwell, Mass.: Kluwer Academic Publishers, in press.

[2] E. Newham, The Biometric Report. New York: SJB Services, 1995.

[3] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," Information Technology & People, vol. 7, no. 4, pp. 6–37, 1994.

[4] Hua Gu ,Guangda Su, Cheng Du, Feature Points Extraction from Faces, Image and Vision Computing NZ, Palmerston North, November 2003.

[5] Xiaoguang Lu, Image Analysis for Face Recognition – A brief survey, Dept. of Computer Science & Engineering, Michigan State University, personal notes, May 2003.

[6] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating faces, fingerprints, and soft biometric traits for user recognition," in LNCS 3087, 2004, pp. 259–269.

[7] Lu, X. ; Wang, Y. & Jain, A.K. (2003). Combining Classifiers for Face Recognition, In IEEE Conference on Multimedia & Expo, Vol. 3, pp. 13-16

[8] L. Hong and A.K Jain, "Integrating faces and fingerprint for personal identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295–1307, 1998

[9] R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955–966, Oct. 1995.

[10] L. Wiskott, J.M. Fellous, N. Kruger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 775–779, 1997

[11] G.J. Edwards, T.F. Cootes, and C.J. Taylor, "Face recognition using active appearance models," in Proc. European Conference on Computer Vision, 1998, vol. 2, pp. 581–695.

[12] V. Blanz and T. Vetter, "A morphable model for the synthesis of 3D faces," in Proc. ACM SIGGRAPH, Mar. 1999, pp. 187–194.

[13] J.L. Wayman, Large-scale Civilian biometric Systems-Issues and Feasibility, in National Biometric Test Center Collected Works:1997-2000,pages 137-156, 2000.

[14] S. Gutta, J. Huang, P. Phillips, and H. Wechsler, "Mixture of experts for classification of gender, ethnic origin, and pose of human faces," IEEE Trans. Neural Networks, vol. 11, no.4, pp. 948–960, Jul. 2000.

[15] Balci, K., Atalay, V.,PCA for Gender Estimation: Which Eigenvectors Contribute?, in16th International Conference on Pattern Recognition (ICPR'02) Vol. 3., QC, Canada, (2002) 363-366
[16] B. Moghaddam and M. Yang, "Learning gender with support faces," IEEE Trans. PAMI, vol. 24, no. 5, pp. 707–711, May. 2002.
[17] Y. Kwon and N. Da Vitoria Lobo, Age classification from facial images, in Proc. CVPR, Seattle, WA, June 1994, pp. 762–767.
[18] A. Lanitis, C. Draganova, and C. Christodoulou, "Comparing different classifiers for automatic age estimation," IEEE Trans. Syst., Man, Cybern.. B, Cybern., vol. 34, no. 1, pp. 621–628, Feb. 2004.
[19] Dirk Colbry, George Stockman, and Anil Jain, Detection of Anchor Points for 3D Face Verification, in IEEE Workshop on Advanced 3D Imaging for Safety and Security, June 2005.
[20] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, Mar. 1991.
[21] Bo WU, Haizhou AI, Chang HUANG, Real-time Gender Classification, SPIE Conference Proceeding: Multi-spectral Image Processing and Pattern Recognition, Oct 2008.
[22] Zehang Sun, George Bebis, Xiaojing Yuan, and Sushil J. Louis, Genetic feature subset selection for gender classification: A comparison study, in Proceedings of the sixth IEEE Workshop on Applications of Computer Vision, December 2002.