International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 35530-35536

Biometric IRIS Recognition based Age Estimation in Security Systems

U. Satheeshwaran
Research Scholar,
Department of Electronics and Communication Engineering,
St.Peter's University, Chennai,
Tamilnadu, India.

T.Saravanan
Professor,
Department of Electronics and Telecommunication Engineering ,
Bharath University, Chennai,
Tamilnadu, India.

Abstract - Most of the researcher mainly focused on human face image used to identify the face recognition and also used to calculate age estimation. Here we are mainly focusing and using the human Iris images. Iris recognition presents a challenging problem in the field of image analysis and computer vision, and as such has received a great deal of attention over the last few years because of its many applications in various domains. Iris recognition is an important role for playing security purpose. This kind of application is mainly used for banking services, database access and login, ATM services and so on. In this paper first we consider the human Iris image these images it may be static, dynamic, still, and video image. Images may be stored in CASIA iris database it will also work for UBIRIS. First we exactly identify and check the Authentication using GLCM algorithm. Above the images already stored in database or real time. Suppose I give some iris images in real time our software exactly identify and recognize that person is valid or not. Our system consistently achieved a nearly perfect recognition rate (over 99.7% on all databases).

Keywords: Canny edge detection, Age classification, Age estimation, Gender classification.

Introduction

In today's information technology world, security for systems is becoming more and more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defense against intruders. The three main types of authentication are something you know (such as a password), something you have (such as a card or token), and something you are (biometric). Passwords are notorious for being weak and easily crack able due to human nature and our tendency to make passwords easy to remember or writing them down somewhere easily accessible. Cards and to kens can be presented by anyone and although the token or card is recognizable, there is no way of knowing if the person presenting the card is the actual owner. Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal. If biometrics is used in conjunction with something you know, then this achieves what is known as two-factor authentication. Two-factor authentication is much stronger as it requires both components before a user is able to access anything. Biometric identification utilizes physiological and behavioral characteristics to authenticate a person's identity.

Some common physical characteristics that may be used for identification include fingerprints, palm prints, hand geometry, retinal patterns and iris patterns. Behavioral characteristics include signature, voice pattern and keystroke dynamics. A biometric system works by capturing and storing the biometric information and then comparing the scanned biometric with what is stored in the repository. The diagram below demonstrates the process followed when using a biometric system for security. Today, biometric recognition is a common and reliable way to authenticate the identity of a living person based on physiological or behavioral characteristics. In statistical texture analysis, texture features are computed from the statistical distribution of observed combinations of intensities at specified positions relative to each other in the image. According to the number of intensity points (pixels) in each combination, statistics are classified into first-order, second-order and higher-order statistics. The Gray Level Co-occurrence Matrix (GLCM) method is a way of extracting second order statistical texture features. GLCM introduced by Haralick contains information about the positions of pixels having similar gray level values. A GLCM is a matrix where the number of rows and columns is equal to the number of gray levels, G, in the image. The matrix element $P(i, j \mid d, \theta)$ is the relative frequency with which two pixels, separated by distance d, and in direction specified by the particular angle (θ) , one with intensity i and the other with intensity j. The basic GLCM algorithm is as follow:

i. Count all pairs of pixels in which the first pixel has a value i, and its matching pair displaced from the first pixel by d has a value of j.
ii. This count is entered in the i-th row and j-th column of the matrix Pd[i,j]
iii. Note that Pd[i,j] is not symmetric, since the number of pairs of pixels having gray levels[i,j] does not necessarily equal the number of pixel pairs having gray levels [j,i].
iv. The elements of Pd[i,j]can be normalized by dividing each entry by the total number of pixel pairs.
v. Normalized GLCM N[i,j], defined by:

$$N(i,j) = \frac{p[i,j]}{\sum_i \sum_j p[i,j]} \quad \text{.........(1)}$$

The main focus of the UBIRIS database is to minimize the requirement of user cooperation, i.e., the analysis and proposal of methods for the automatic recognition of individuals, using images of their iris captured at-a-distance and minimizing the required degree of cooperation from the users, probably even in the covert mode.

The physiological properties of irises are major advantages to using them as a method of authentication. As discussed earlier, the morphogenesis of the iris that occurs during the seventh month of gestation results in the uniqueness of the iris even between multi-birth children. These patterns remain stable throughout life and are protected by the body's own mechanisms. This randomness in irises makes them very difficult to forge and hence imitate the actual person. In addition to the physiological benefits, iris-scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology. It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless he user actually engages it. It poses no difficulty in enrolling people that wear glasses or contact lenses. The accurateness of the scanning technology is a major benefit with error rates being very low, hence resulting in a highly reliable system for authentication. Scalability and speed of the technology are a major advantage. The technology is designed to be used with large-scale applications such as with ATMs. The speed of the database iris records are stored in is very important. Users do not like spending a lot of time being authenticated and the ability of the system to scan and compare the iris within a matter of minutes is a major benefit.

The most obvious use of iris recognition technology is within the computing environment. There is a lot of valuable data stored on a company's network and being able to access the network with a username and password is the most common method of authentication today. If a username and as sword is stolen then this gives the thief all of that person's access privileges and this can be detrimental to a company in today's competitive environment. Implementing an iris recognition system to authenticate users on the network means that there are no passwords to steal and no tokens to lose. Users are only able to access the systems they have privileges to access and it's very difficult for someone to replicate an iris for authentication. The technology can not only be used for securing log on but also in areas such as file and directory access, web site access and key access for file encryption and decryption. In a network environment, a system may be configured to compare the live template to the stored template and if a match is found then the user's access privileges are passed back to the client. In other implementations, after a match is found, the server returns a username and password to the client, which then transmits this information to the network server to allow access to the systems the user has privileges to.

Enterprise applications are also being worked on in the areas of ecommerce, healthcare applications for medical records protection, insurance and brokerage transactions. Another area iris recognition is useful with is physical security to data centre's or computer rooms. Mounting a canner by the access door a and authenticating people via their iris is a good method of ensuring only those whose templates are in the database for computer room access are actually allowed in. This helps to alleviate problems associated with swipe card access where some systems have to be manually programmed with specific card numbers and robust processes need to be in place to ensure access lists are regularly reviewed. Swipe cards are also easily lost, stolen or borrowed. Iris recognition system has proven its capability in implementing reliable biometric security protocols in various high risk sectors like aviation, border patrol and defense. However, lately, due to falling prices of iris scanners it has found further application in the retail industry.

The banking and financial sector has adopted this system wholeheartedly because of its robustness and the advantages it provides in cutting costs and making processes more streamlined. The technology started out as a novelty however due exigencies in the banking sector characterized by decreasing profits it became a necessity. The use of Biometric ATM's based on iris recognition technology has gone a long way in improving customer service by providing a safe and paperless banking environment. Iris recognition technology captures the intricate iris patterns with the help of an iris scanning device. This data is then digitalized and stored in a database for future reference along with some other parameters like name and address. Iris data is more reliable and durable because the iris is covered by a protective sheath which protects it from damaged. Due to this durability iris recognition system requires only a single enrolment. Other technologies are subjected to wear and tear due to the nature of the work environment which requires repeated enrolment.

Iris based biometric ATM's are more secure than conventional pin based ATM's because it requires biometric verification which cannot be stolen, copied or faked. Pin based security systems can be compromised leading to losses for the consumer as well as the bank. Also, the customers find it very tedious to remember passwords and pin numbers; moreover, the task of requesting for new set of passwords is itself fraught with endless communication to and from the customer and the bank leading to poor customer experience.

Age Estimation Methods

The main contributions of this work are three-fold:

i. We present a web image mining scheme to harness the Internet images for collecting a large and diverse face database with nearly-correct age labels, and then use it for learning universal human age estimator;
ii. We propose a novel learning algorithm to robustly derive a human age estimator based on images with multiple face instances and possibly noisy labels; and
iii. We develop a fully automatic system for automatic training image collection, age regresses learning, and final age estimation, which does not rely on any kind of human interactions and is thus of great potentials in real scenarios.

A system overview is illustrated in Fig. 2 and the three major components of the proposed research are summarized as follows:

A. Internet Aging Image Collecting
The Internet aging image collection is performed by automatically crawling images from the image search engines or photo sharing websites based on a set of age related text enquiries, *e.g.*, "15-years-old", "age-15" and "15th-birthday" for the age of 15 years. In this step, generally more than 10*k* of images can be downloaded for each age, but a large portion of these images do not contain any face instance or contain only face instances with other different ages.

B. Noisy Image and Label Filtering
In this work, we propose to adopt a pipeline approach to retain good face instances for model training as well as to filter out those noisy images or face instances as many as possible. First, we propose to conduct parallel face detection based on multiple face detectors for improving the probability to obtain well-aligned face instances for each image, and then the face instances overlapping with those at least one face instance from distinct detectors are retained as good samples for model training. Then, Principal component analysis is applied for each age and those face instances with large reconstruction errors are filtered out. This pre-screened dataset is then input into the proposed robust multi-instance regression algorithm to learn a universal human age estimator.

C. Robust Multi-instance Regression
In this step, we are given a set of training face images with multiple face instances within each image, and the task is to learn a human age regression. This problem can be considered as a specific multi-instance learning problem, but those previous multi-instance learning algorithms cannot be directly applied for this problem since there may exist noisy image labels for the training data. In this work, we present a robust multi-instance learning algorithm to tackle this problem with the awareness of label outliers. Figure 1 shows the system overview for learning universal age estimator. Note that multi-instance learning is a widely studied research topic in the past few years. Keeler et al. first proposed the multi-instance learning concept when dealing with the hand-printed numerals detection problem, motivated by the observation that there might exist more than one numerals in a single image.

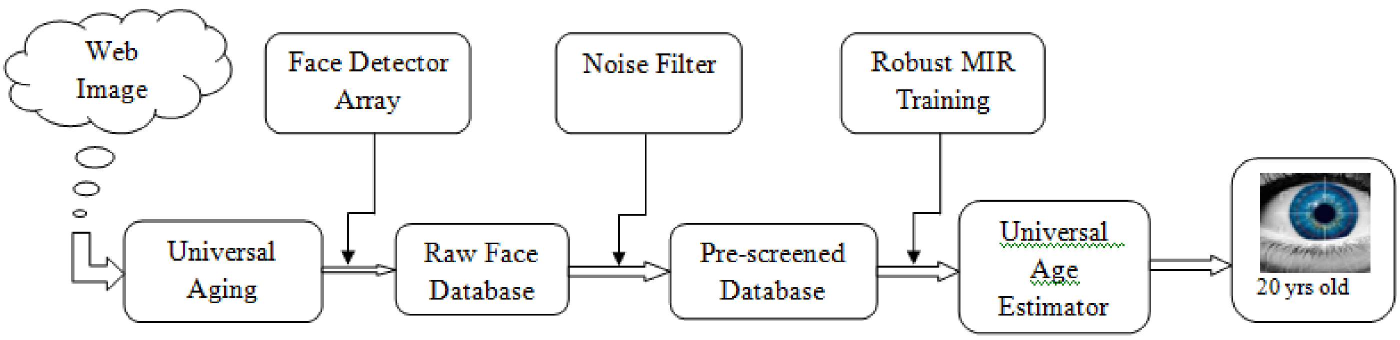

Fig.1. The system overview for learning universal age estimator

After that, many researchers proposed various related schemes such as DD, EM-DD and citation-kNN to tackle this problem. Also the multi-instance learning concept was incorporated into both boosting and support vector machine algorithms, yielding the so called MIL-boosting and MIL-SVM algorithms. There also exist several algorithms proposed for the multiple instances multiple label learning problems. Besides these classification problems, recently Ray et al. proposed a multi-instance regression framework to deal with the regression problem, which is the most related work with our research in this work. This algorithm does not consider the noisy label issue, and therefore the algorithmic robustness cannot be guaranteed.

Proposed Method
Figure 2 gives the block diagram of FEBFRGAC for verification of iris, gender and age.

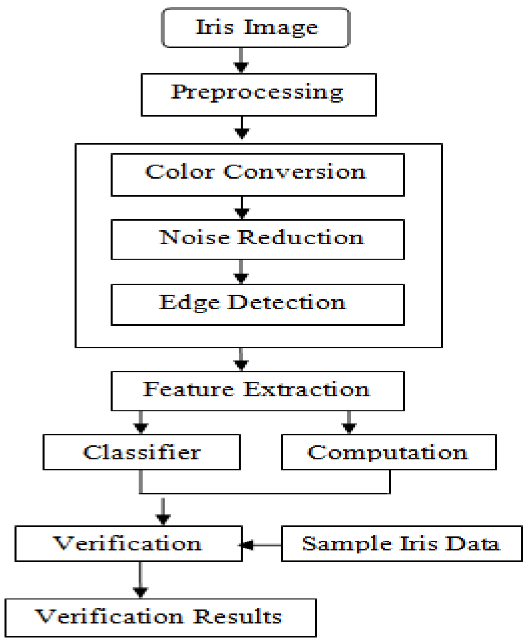

Fig.2. Block Diagram of FEBFRGAC

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 35530-35536

A. IRIS image

The Iris image samples are collected from website as well as captured from the mobile phone and digital cameras.

B. Preprocessing

i. *Color Conversion*

An RGB color image is an MxNx3 array of color pixels is a triplet corresponding to the red, green and blue components of an RGB image at a specific spatial location. The data class of the component images determines their range of values. If an RGB image is of class double, the range of values is [0, 1]. Similarly, the range of values is [0,255] or [0, 65535] for RGB images of class unit8 or unit16 respectively. The number of bits used to represent the pixel values of component images determines the bit depth of an RGB image. The number of possible colors in an RGB image is $(2^b)^3$, where b is the number of bits in each component image. For 8-bit case, the number is 16,777,216 colors. Three dimensional RGB is converted into two dimensional gray scale images for easy processing of iris image.

ii. *Noise reduction*

A noise reduction filter is applied to the binary image for eliminating single black pixel on white background. 8-neighbors of chosen pixels are examined if the number of black pixels are greater than white pixels then it is considered as black otherwise white. Dirt on cameras or scanner lens, imperfection in the scanner lighting etc., introduces the noise in the scanned iris image. A filtering function is used to remove the noise in the image and works like a majority function that replaces each pixel by its majority function.

iii. *Edge detection method*

Point and line detections are important in image segmentation. Edge detection is far most common approach for detecting many discontinuities in intensity values. Canny edge detection finds edge by looking for local maxima of the gradient of f(x, y). The gradient is calculated using the derivatives of Gaussian filter.

$$G(x, y) = [Gx + Gy]^{1/2} \qquad (2)$$

Where, G_X and G_Y are the first derivatives of the function f(x, y), digitally

$$\alpha(x, y) = \tan^{-1}(Gx / Gy) \qquad (3)$$

Where, α(x, y) is edge direction shown in the Figure 3.

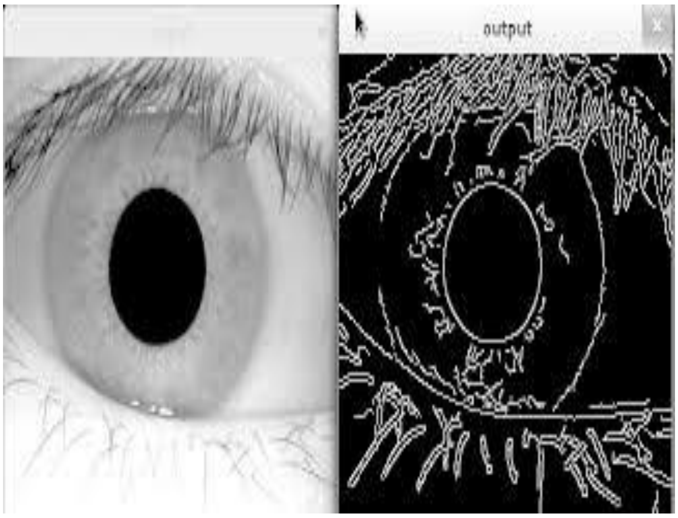

Fig.3. Canny Edge Detected Image

C. Feature Extraction

A combination of Global and Grid features are used to extract features. The Global features includes inter ocular distance, to the line joining two eyes.

i. Computation

Iris feature ratios: The primary facial features are located to compute the ratios for age classification. Four ratios are calculated for facial iris database comprising young aged, middle aged and old aged adults. Figure 3 gives the ratios of left eye to right eye distance for feature extraction.

ii. Classifier

The posteriori class probabilities are used to classify the testing iris to one of the genders.

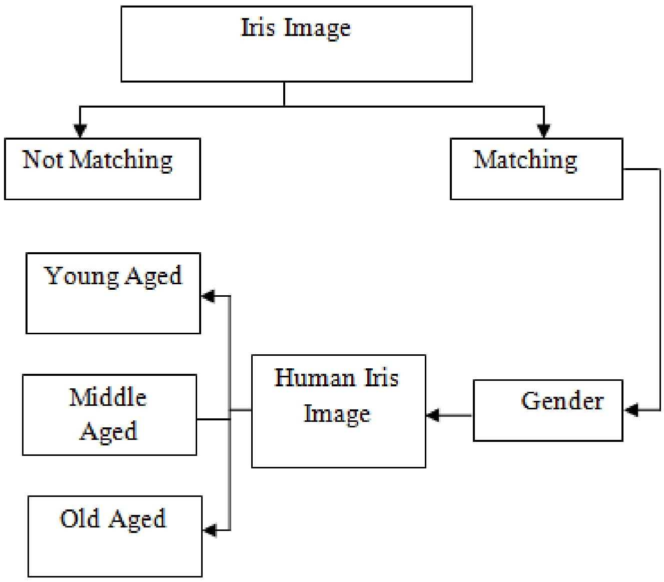

Fig.4. Complete Classifier flow for FEBFRGAC

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 35530-35536

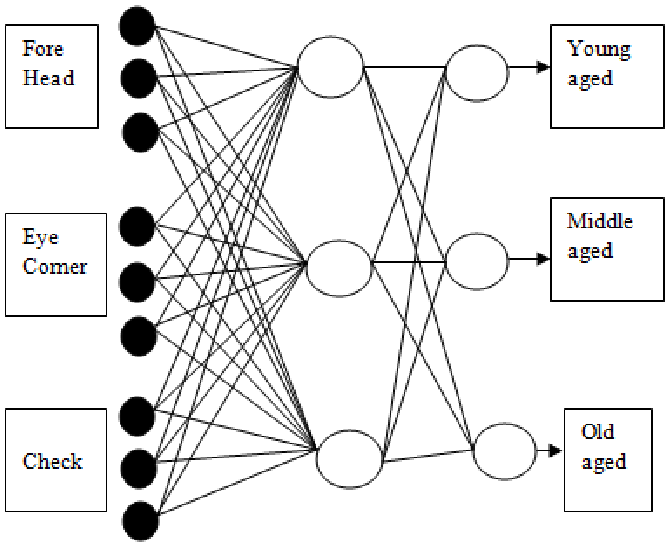

Fig.5. Age Group Classification Network

Figure 4 gives complete classifier for FEBFRGAC. For age estimation, two classifiers are prepared corresponding to gender. Each age classifier has been trained with male and female data. Based on the output of the gender classifier, suitable age classifier is used. The extracted feature of test iris image is compared with the iris database. Figure 5 shows the proposed age group classification network. If the extracted features of the test iris image match with the sample iris database then accepted as matching, otherwise, it is accepted as not matching.

Problem Identification

Input: Test iris image and iris image database. Output: Iris recognition, gender classification and age determination.

i. Pre-processing.
ii. Feature extraction from the iris image by using shape and texture transformation for iris recognition.
iii. Feature viz., total number of white pixels, mustache and left and right eye tail regions are extracted for gender classification.
iv. Feature such as wrinkle are extracted for age identification.
v. Posteriori class probability and ANN classifiers are used for gender and age classification respectively.
vi. Verification of test iris image with the iris database.

Result and Analysis

Age group classification is done using ANN training method as shown in Table 1. If the total number of pixels for forehead region and the eyelid region is greater than 140 pixels and lesser than 150 pixels or the sum of forehead region and the eyelid region is lesser than 100 pixels then the iris image is classified as young aged (less than 30 years). If the product of right canthus region and the left canthus region pixels is more than 44000 and less than 45000 or lesser than 22000 then the facial image is classified as middle aged (30- 40 years). If the number of pixels other than the above features is classified as old aged (more than 40 years).

TABLE.1. Age Group Network

Algorithm	AG	Sample size	CL	CR	Total CR
FEBFRGAC	Y	28	25	89.3%	89.65%
	M	20	18	90%	
	O	10	09	90%	
CAGBFF	Y	44	37	84.4%	78.49%
	M	32	25	78.1%	
	O	17	11	64.7%	

TABLE.2. Results of the Complete Age Classification

Subjects	Ratio2 Threshold=0.21	No. of pixels	Computed label
I01	0.9096	140	Young
I02	0.9422	142	Young
I03	0.9516	147	Young
I04	0.9068	144	Young
I05	0.8826	146	Young
I06	0.8957	149	Young
I07	0.9985	141	Young
I08	0.9938	408	Middle
I09	0.9032	418	Middle
I10	0.9916	808	Old
I11	0.9320	826	Old
I12	0.9494	875	Old
I13	0.9025	818	Old
I14	0.8349	861	Old

The age group classification depends on the number of pixels on the iris image. The subjects 1 to 7 has pixels approximately equal to 150 referred as young aged, the subjects 8 and 9 has pixels approximately equal to 410 referred as middle aged and the subjects 10 to 14 has pixels approximately equal to 810 referred as old aged is as shown in the Figure 6. It is observed that as age increases number of pixels also increases correspondingly. Figure 7 shows the performance comparison among FEBFRGAC and CAGBFF. Figure 8 shows the dependence of false rejection rate and false acceptance rate on threshold.

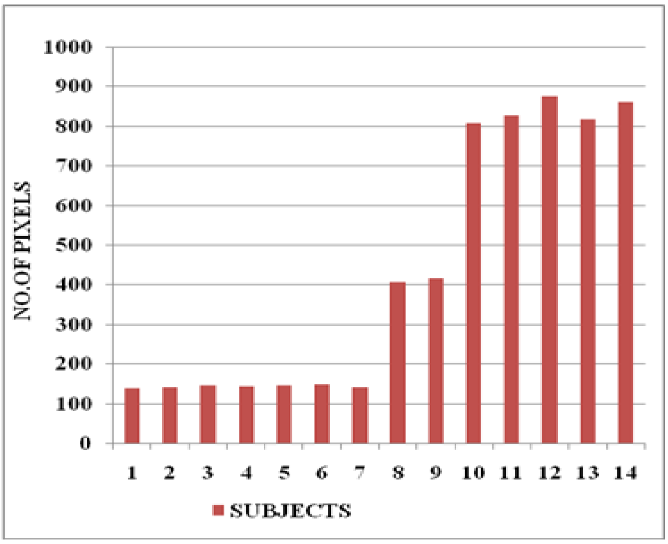

Fig.6. No. of Pixels Versus Age Group Classification

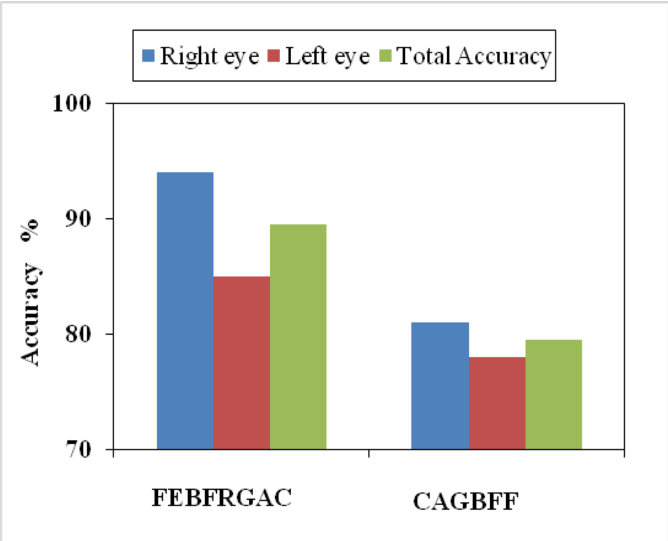

Fig.7. Performance Comparison among FEBFRGAC and CAGBFF

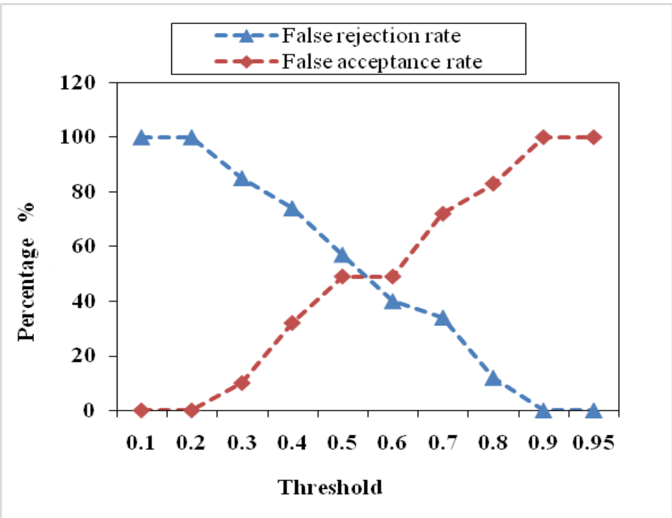

Fig.8. Dependence of False Rejection Rate and False Acceptance Rate on Threshold

Conclusions

In this paper FEBFRGAC algorithm is proposed. The iris images are preprocessed and Canny edge detector is used to derive the edges of iris images. The features of iris are used for matching. The gender is classified using Posteriori class probability classifier and ANN is used to classify age, based on features of iris images. It is observed that iris matching ratio is 100%, gender classification is 95%, and age classification is 90%. In future the algorithm may be modified for different iris angle and illumination variations.

References

[1] X. Geng, Z. H. Zhang, G. Li, and H. Dai, “Learning from facial aging patterns for automatic age estimation,” in Proc. 14th ACM International Conference on Multimedia, 2006, pp. 307–316.

[2] N. Ramanathan and R. Chellappa, “Face verification across age progression,” IEEE Transactions on Image Processing, vol. 15(100), pp. 3349–3362, 2006.

[3] “Face verification across age progression,” in IEEE Conference on Computer Vision and Pattern Recognition, vol. 2, San Diego, U.S.A, June 2005, pp. 462–469.

[4] Y. Fu and T. S. Huang, “Human age estimation with regression on discriminative aging manifold,” IEEE Transactions on Multimedia, vol. 10(4), pp. 578–584, 2008.

[5] G. Guo, Y. Fu, C. R. Dyer, and T. S. Huang, “Image-based human age estimation by manifold learning and locally adjusted robust regression,” IEEE Transactions on Image Processing, vol. 17(7), pp. 1178–1188, July 2008.

[6] N. Ramanathan and R. Chellappa, “Modeling age progression in young faces,” in IEEE Conference on Computer Vision and Pattern Recognition, vol. 1, New York, U.S.A, June 2006, pp. 387–394.

[7] “Modeling shape and textural variations in aging adult faces,” in IEEE International Conference on Automatic Face and Gesture, Amsterdam, Netherlands, 2008 (to appear).

[8] J. Suo, F. Min, S. Zhu, S. Shan, and X. Chen, “A multi-resolution dynamic model for face aging simulation,” in IEEE Conference on Computer Vision and Pattern Recognition, Minnesota, U.S.A., June 2007.

[9] U. Park, Y. Tong, and A. K. Jain, “Face recognition with temporal invariance : A 3d aging model,” in IEEE Conference on Automatic Face and Gesture Recognition, 2008 (to appear).

[10] M. Gandhi, “A method for automatic synthesis of aged human facial images,” Master’s thesis, McGill University, September 2004.

[11] H. Ling, S. Soatto, N. Ramanathan, and D. Jacobs, “A study of face recognition as people age,” in IEEE International

Conference on Computer Vision, Rio De Janeiro, Brazil, October 2007.

[12] Z. Yang and H. Ai, “Demographic classification with local binary patterns,” in International Conference on Biometrics, 2007, pp. 464–473.

[13] T. Sim, S. Baker, and M. Bsat, “The CMU pose illumination and expression database,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25(12), pp. 1615–1618, December 2003.

[14] L. G. Farkas and I. R. Munro, Anthropometric Facial Proportions in Medicine. Springfield, Illinois, USA: Charles C Thomas, 1987.

[15] Z. Xu, H. Chen, and S.-C. Zhu, “A high resolution grammatical model for face representation and sketching,” in IEEE Conference on Computer Vision and Pattern Recognition, vol. 2, 2005, pp. 470–477.

[16] A. M. Albert and K. Ricanek, “The MORPH database: Investigating the effects of adult craniofacial aging on automated face-recognition technology,” in Forensic Science Communications, vol. 10(2), April 2008.

[17] K. Ricanek and T. Tesafaye, “MORPH : A longitudinal image database of normal adult age-progression,” in IEEE International Conference on Automatic Face and Gesture, 2006, pp. 341–345.

[18] E. Patterson, A. Sethuram, M. Albert, K. Ricanek, and M. King, “Aspects of age variation in facial morphology affecting biometrics,” in IEEE International Conference on Biometrics : Theory, Applications and Systems, Crystal City, VA, 2007.