Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

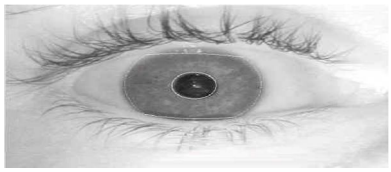
Person Identification Technique Using Human Iris Recognition

Mr.Sachin S.Bhosale[1], Mr.Rakesh P.Kumawat[2], Mr.Pramod P.Gadekar[3], Mr.Prashant P.Ratnaparkhi[4], Mr. Jaydeep T.Arote[5]
[1,2,3,4,5]*P.Dr.V.V.Patil Instt.of technology &Engg.(Polytechnic),Loni*

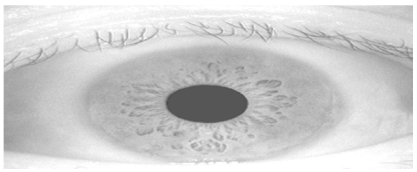
Abstract- The security is an important aspect in our daily life whichever the system we consider security plays vital role. The biometric person identification technique iris is well suited to be applied to access control and provides strong e-security. A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristics possessed by the individual. A good biometric is characterized by use of a feature that is highly unique so that the chance of any two people having same characteristic will be minimal, stable so that the feature does not change over time and be easily captured in order to provide convenience to the user and to prevent misrepresentation of the feature. Iris is an internally protected organ whose texture is stable from birth to death. So, it is very reliable as iris texture is unique in each individual with probability of two same is 1/1051 as proved by Dr. J. Doughman. Iris recognition is a biometric system for access control that uses the most unique characteristic of the human body, the iris employed in automated border crossings, national ID systems, etc. this paper illustrates techniques to improve performance of iris recognition system based on stationary image. In this paper we focused on an efficient methodology for identification and verification for iris detection. The iris recognition approach is implemented via many steps, these steps are concentrated on image capturing, enhancement and identification.
Keywords: iris,pupil, thresholding, iris pattern.

I. INTRODUCTION

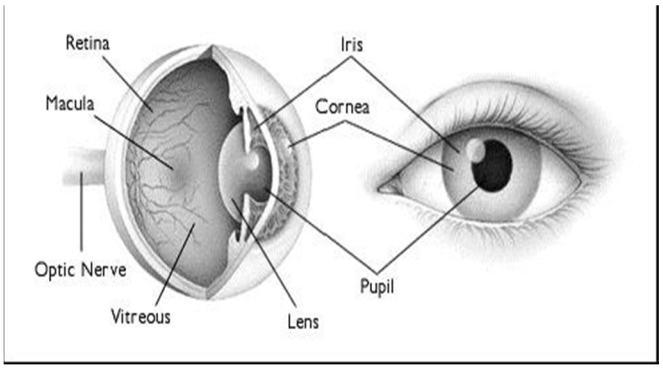
Iris recognition is a rapidly expanding method of biometric authentication that uses pattern recognition techniques on images of irises to uniquely identify an individual. Iris based recognition is the most promising for high-security environments among various biometric techniques (face ,finger- print, palm vein, signature, palm print, iris, etc.) because of its unique, stable, and non-invasive characteristics. Iris recognition system can be used to either prevent unauthorised access or identity of individual using a facility. When installed, this requires users can present their iris to the system and get identified. Enrolment takes less than 2 minutes, authentication takes less than 2 seconds.



Normal Eye



Example of iris



Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

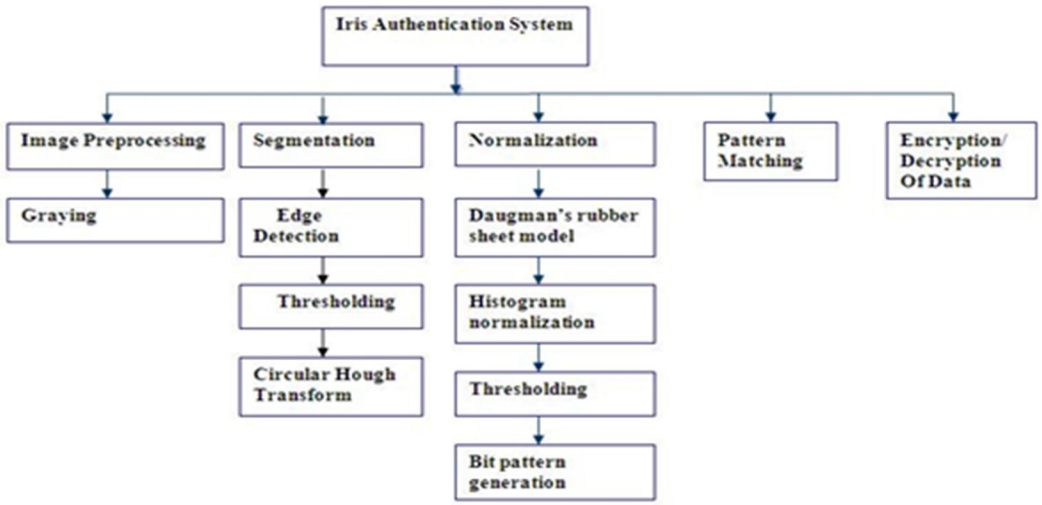


Fig. Typical Structure of an Iris Image

processing techniques can be employed to extract the unique iris pattern from the digitized image of an eye and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates. Thus the iris based recognition techniques include **image acquisition**, **iris pre-processing** which includes **iris localization and segmentation**, **iris normalization**, **feature extraction i.e. encoding** and **comparison**.

II. RELATED WORK

Today's e-security are in critical need of finding accurate, secure and cost-effective alternatives to passwords and personal identification numbers (PIN) as financial losses increase dramatically year over year from computer-based fraud such as computer hacking and identity theft. Biometric solutions address these fundamental problems, because an individual's biometric data is unique and cannot be transferred. Some traditional methods used for authentication are – textual passwords, biometrics, graphical passwords, digital signature, voice/face recognition, etc. these various comprehensive investigation on the various existing authentication schemes have been accomplished. And it has been discerned that none of the recent schemes can resist all sorts of attacks. With this outcome, this project proposes an authentication scheme which overcomes almost all the existing authentication schemes. The textual passwords, graphical passwords have some vulnerabilities due to which they can be easily cracked by some methods such as eves dropping, dictionary attack, social engineering and shoulder surfing, etc. The digital authentication schemes are very hard and complicated to use. In this way almost all of the above drawbacks are overcame in this project. To choose the right biometric to be highly fit for the particular situation, one has to navigate through some complex vendor products and keep an eye on future developments in technology and standards. Here comes a list of Biometrics with comparatives:

A. Facial Recognition

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas. This biometric system can easily spoof by the criminals or malicious intruders to fool recognition system or program. Iris cannot be spoofed easily.

B. Palm Print

Palm print verification is a slightly modified form of fingerprint technology. Palm print scanning uses an optical reader very similar to that used for fingerprint scanning; however, its size is much bigger, which is a limiting factor for use in workstations or mobile devices.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Signature Verification

It is an automated method of examining an individual's signature. This technology is dynamic such as speed, direction and pressure of writing, the time that the stylus is in and out of contact with the ―paper‖. Signature verification templates are typically 50 to 300 bytes. Disadvantages include problems with long-term reliability, lack of accuracy and cost.

D. Fingerprint

A fingerprint as in Figure1 recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. As it is more common biometric recognition used in banking, military etc., but it has a maximum limitation that it can be spoofed easily. Other limitations are caused by particular usage factors such as wearing gloves, using cleaning fluids and general user difficulty in scanning.

III. PROPOESD WORK

The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds. The picture of eye first is processed by software that localizes the inner and outer boundaries of the iris. And it is encoded by image-processing technologies. In less than few seconds, even on a database of millions of records, the iris code template generated from a live image is compared to previously enrolled ones to see if it matches to any of them. An iris recognition camera takes a black and white picture from 5 to 24 inches away. The camera uses non-invasive, near-infrared illumination that is barely visible and very safe. And this iris recognition cannot take place without the person permission.

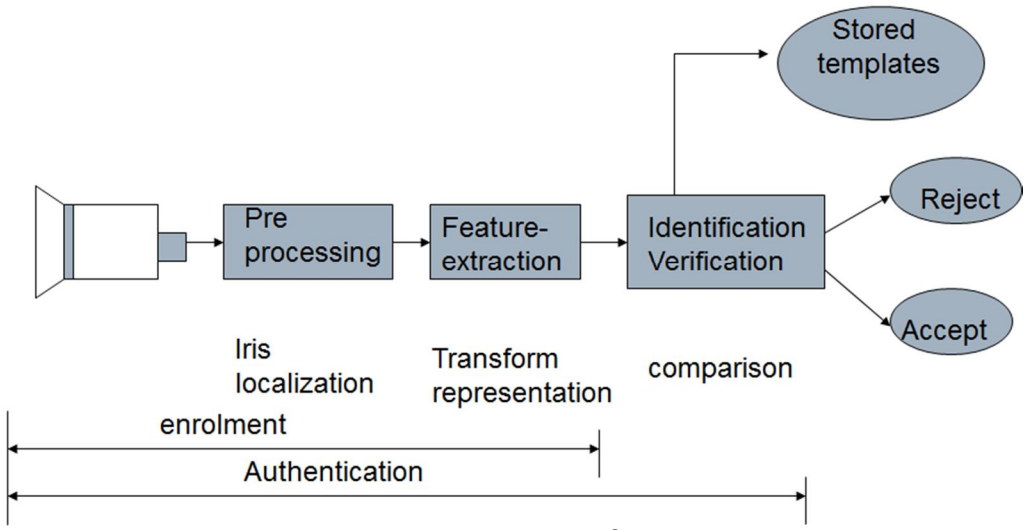
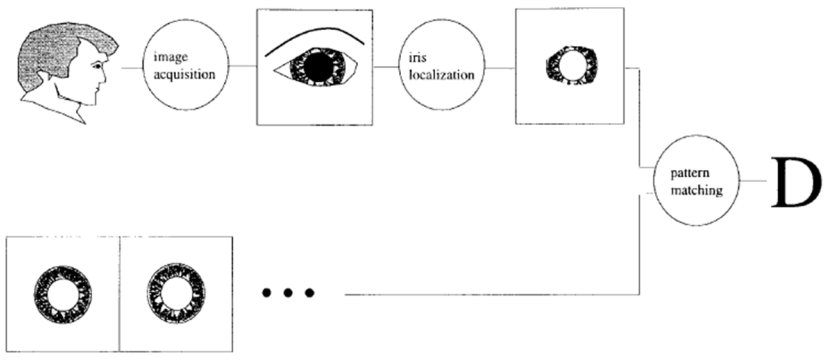


Fig. : Iris Recognition Mechanism

As we discussed, the typical iris recognition system is consists of image acquisition, iris pre-processing which includes iris localization and segmentation, iris normalization, feature extraction i.e. encoding and comparison.



Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. IMAGE ACQUISITION

One of the major challenges of automated iris recognition is to capture a high-quality image of the iris while remaining noninvasive to the human operator. The concerns of the image acquisition are,

Obtained images with sufficient resolution and sharpness

Good contrast in the interior iris pattern with proper illumination

Well centered without unduly constraining the operator

Artifacts eliminated as much as possible

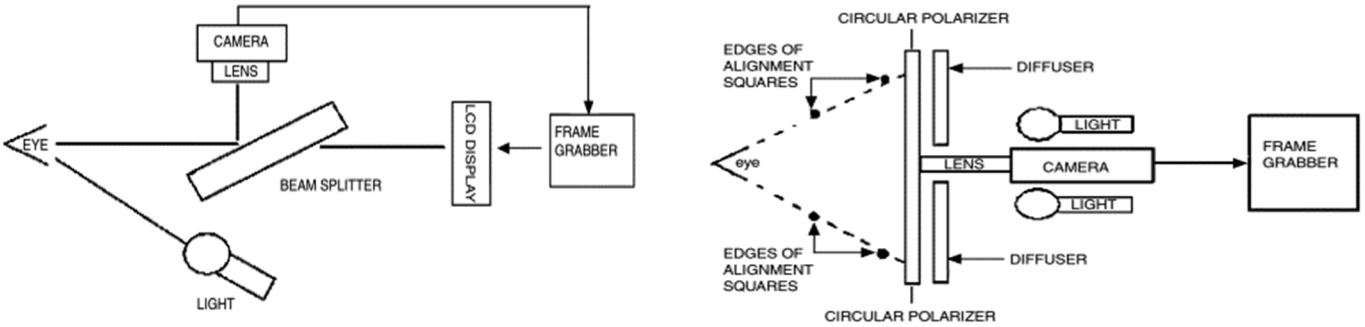
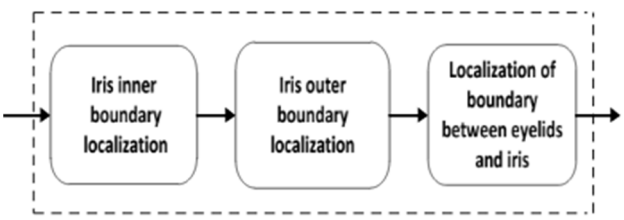


Image Acquisition

V. IRIS PRE-PROCESSING

A. Iris Localization

After getting the input image, the next step is to localize the circular edge in the region of interest. Canny edge detection operator uses a multi-stage algorithm to detect a wide range of edges images. It is an optimal edge detector with good detection, good localization and minimal response. In localization we used this detection, in which the inner and outer circles of the iris is approximated, in which inner circle corresponds to iris/pupil boundary and outer circle corresponds to iris/sclera boundary. But the two circles are usually not concentric. Also, comparing with other parts of the eye, the pupil is much darker. The inner boundary is detected between the pupil and the iris. At the same time, the outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. So, we detect the outer boundary by maximizing changes of the perimeter-normalized along the circle.



B. Iris Segmentation

Iris segmentation is an essential process which localizes the correct iris region in an eye image. Circular edge detection function is used for detecting iris as the boundary is circular and darker than the surrounding.

C. Iris Normalization

In normalization the obtained iris regions is transformed in order to have fixed dimensions for the purpose of comparison. The size of pupil may change due to the variation of the illumination and associated elastic deformation in iris texture may interface with

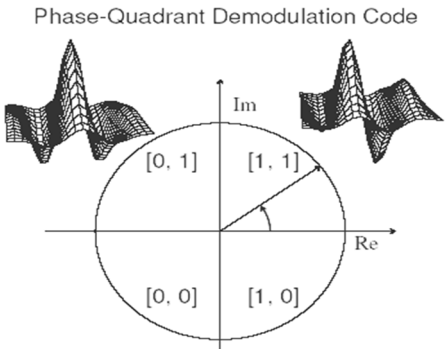
results of pattern matching. And so, for the purpose of accurate texture analysis, it is necessary to compensate this deformation. Since we have detected both inner and outer boundaries of the iris, it is easy to map the iris ring to a rectangular block of texture of a fixed size. The original image has low contrast and may have non- uniform illumination caused by the position of the light source. These may impair the result of the texture analysis. We enhance the iris image in order to reduce the effect of non-uniform illumination.

D. Feature Extraction (Encoding)

The most important step in automatic iris recognition is the ability of extracting some unique attributes from iris, which help to generate a specific code for each individual. Gabor and wavelet transforms are typically used for analysing the human iris patterns and extracting features from them,

E. Pattern Matching (Comparison)

The purpose of pattern matching is to establish a precise correspondence between characteristic structures across the two images.
Four steps:
Bringing the newly acquired iris pattern into spatial alignment with a candidate data base entry.
Choosing a representation of the aligned iris patterns that makes their distinctive patterns apparent.
Evaluating the goodness of match between the newly acquired and data base representations.
Deciding if the newly acquired data and the data base entry were derived from the same iris based on the goodness of match.



Identical Pattern Matching

Matching of two iris code is performed using the Hamming distance. The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one. The Hamming distance is the matching metric employed by Dr. Daugman and calculation of the Hamming distance is taken only with bits that are generated from the actual iris region.

VI. APPLICATIONS

The need for secure methods of authentication is becoming increasingly important. Currently, highly accurate personal recognition is feasible using the human iris mainly because of its stability throughout a lifetime and its uniqueness. Iris recognition systems are relatively compact and efficient and have shown promising performance .The combination of iris recognition and smart cards can be used to authenticate the users and entities in the system, and it is possible to build very secure systems using smart cards. On-card matching is an outstanding way of user-authentication within security applications that meet the three paramount requirements of security, ease of use, and data privacy.Iris authentication is the most feasible because of stability throughout the life and its uniqueness. Iris authentication systems are compact and efficient and have shown promising performance. The need for secure methods of authentication is becoming increasingly important.Encryption/Decryption of data using RSA algorithm is among the best algorithms. Hence we can go for high level of secure data transfer.

VII. CONCLUSION

As per the goal of this project an Iris authentication is the most feasible because of stability throughout the life and its uniqueness. Iris authentication systems are compact and efficient and have shown promising performance. The need for secure methods of

authentication is becoming increasingly important. Encryption/Decryption of data using RSA algorithm is among the best algorithms. Hence we can go for high level of secure data transfer. Iris authentication is the most feasible because of stability throughout the life and its uniqueness. Iris authentication systems are compact and efficient and have shown promising performance. The need for secure methods of authentication is becoming increasingly important. Encryption/Decryption of data using RSA algorithm is among the best algorithms. Hence we can go for high level of secure data transfer.

REFERENCES

[1] A.K. Jain, R.M. Bolle, and S. Pankanti, Eds., "Biometrics: Personal Identification in a networked Society", Norwell, MA: Kluwer, 1999.
[2] D. Zhang, "Biometrics Technologies and Applications", Proc. of International Conference on Image and Graphics, pp.42-49, Tianjing, China, August 2000.
[3] G. Lawton, "Biometrics: A New Era in Security", IEEE Computer, pp.16-18, Aug. 1998.
[4] E. Wolff, "Anatomy of the Eye and Orbit." 7 edition, H. K. Lewis & Co. LTD, 1976.
[5] A. Poursaberi, B.N. Araabi, "A Fast Morphological Algorithm for Iris Detection in Eye Images", 6th International Conference on Intelligent Systems, Kerman, Iran, 2004.
[6] A. Bertillon, "la couleur de l'iris, Revue scientifique", France, 1885.
[7] J. Daugman, "How Iris Recognition Works", Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.
[8] R.P. Wildes,, Asmuth, J.C. et al., "A System for Automated Iris Recognition", Proc of the Second IEEE Workshop on Applications of Computer Vision, 1994, pp.121 -128.
[9] W.W. Boles and B. Boashash, "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Trans. on Signal Processing, 46(4), 1998, pp.1185-1188.
[10] L. Ma, Y. Wang, and T. Tan, "Personal Identification Based on Iris Texture Analysis," IEEE Transaction on pattern analysis and machine intelligence, vol. 25, no. 12, December 2003.
[11] L. Ma, Y. Wang, and T. Tan, "Personal Iris Recognition Based on Multi channel Gabor Filtering" ACCV2002: The 5th Asian Conference on Computer Vision, 23-25 January 2002, Melbourne, Australia.
[12] L. Ma, Y. Wang, and T. Tan, "Iris Recognition Using Circular Symmetric Filters," Proc. 16th Int'l Conf. Pattern Recognition, vol. II, pp. 414-417, 2002.
[13] C. Tisse, L. Martin, L. Torres and M. Robert, "Person identification technique using human iris recognition", St Journal of System Research , 2003, Vol. 4, pp. 67-75
[14] K.W. Nam, K. L. Yoon, J. S. Bark, W. S. Yang, "A feature extraction method for binary iris code construction", Proceedings of the 2nd International Conference on Information Technology for Application (ICITA 2004).
[15] S. Lim, K. Lee, O. Byeon and T. Kim, "Efficient Iris Recognition through Improvement of Feature Vector and Classifier" ETRI Journal, Volume 23, Number 2, June 2001
[16] P. Jaboski, R. Szewczyk, Z. Kulesza, et. al., "Automatic People Identification on the Basis of Iris Pattern Image Processing and Preliminary Analysis", Proc. Int. Conf. on Microelectronics (MIEL 2002), VOL 2, Yugoslavia pp. 687-690, May, 2002.
[17] R. Szewczyk, P. Jaboski, et. al., "Automatic People Identification on the Basis of Iris Pattern - Extraction Features and Classification", Proc. Int. Conf. on Microelectronics (MIEL 2002), VOL 2, Yugoslavia pp. 691-694, May, 2002.
[18] SC. H. Daouk, L. A. El-Esber, F. D. Kammoun and M. A. Al Alaoui, "Iris Recognition", IEEE ISSPIT 2002, Marrakesh.
[19] M.H. Jafar Ali, A. Ella Hassanien, "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory", AMO - Advanced Modeling and Optimization, Volume 5, Number 2, 2003
[20] L.W. Liam, A. Cheima, L. C. Fan and J. A. Dargham, "Iris Recognition Using Self-Organizing Neural Network", IEEE Conference on Research and Development Proceedings, Shah Alam, Malaysia, 2002.