E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

A PHASE-BASED IRIS RECOGNITION ALGORITHM

Mr. S.S.JOSHI, Dr. S.B.Patil
Department of E&TC
MBT Campus,Islampur
Maharashtra India
sj_224238@rediffmail.com
patilsbp@gmail.com

***Abstract*-The increase demand in security system concern to issues such as person identity and theft detection the need of a new reliable security system. A biometric system provides automatic identification of an individual, based on a unique feature or characteristic possessed by the individual. Iris recognition is regarded as the most reliable and accurate biometric identification system. Iris recognition is perhaps the most accurate means of personal identification due to uniqueness of the patterns contained in each iris. The iris recognition system consists of an automatic segmentation system that is based on edge detection and Hough transform, and is able to detect the circular iris and pupil region and occluding eyelids and eyelashes. The extracted iris region is then normalized into a rectangular block with constant dimensions to account for imaging in consistencies. Finally, the image matching algorithm which specifically focuses on the characteristics of the phase components obtained from two-dimensional Fourier Transformation of an image. The Phase Only Correlation (POC) and Band Limited Phase Only Correlation (BLPOC) are the most fundamental transformations, the features of which include superior discrimination capability over the ordinary recognition system.**

***Keywords*-** Biometric, Iris recognition, edge detection, Hough Transform, Phase based Image Matching Algorithm

I. INTRODUCTION

With the advent of modern technology and services in life, human activities and transactions have increased, in which quick and reliable personal identification is necessary. Examples contain passport control, computer login control, bank automatic teller machines and other transactions authorization, premises access control, and security systems generally.All such identification efforts stake thecommon goals of speed, reliability and automation. The use of biometric indicia for identification purposes requires that a particular biometric factor should be unique for every individual, readily measurable, and invariant over time. Biometrics such as signatures, photographs, fingerprints, voiceprints and retinal blood vessel patterns all have significant drawbacks. Thoughsignatures and photographs are economical and easy to obtain and store, they are difficult to identify automatically with guarantee, and can be easily forged. Electronically recorded voiceprints are susceptible to changes in a person's voice, and they can be simulated. Fingerprints or handprints require physical contact, and they also can be counterfeited and marred by artifacts. Human iris on the other hand as an internal organ of the eye and as well protected from the external environment, yet it is easily observable from within one meter of distance makes it a perfect biometric for an identification system with the simplicity of speed, reliability and automation.

Biometric personal identification has been largely motivated by the increasing requirement for security in a networked society. The traditional way of identifying people is via possession and knowledge. Possession is the method that uses a physical item to gain access to the security area, e.g. identity cards, smartcards, tokens etc. Knowledge is the method to gain authorization by the use of something that only the authorized people know, e.g. passwords, PIN numbers, security codes etc. However, physical items can be lost or stolen and password can be forgotten or guessed. Biometric recognition is one solution to the problem. Biometric recognition is theapplication of science to measure Individual's properties. These properties can be a behavioral or a physical feature. Unlike

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

traditional possession-based or knowledge-based methods for personal identification, biometrics employs variousphysiological or behavioral characteristics, suchasfingerprints, face, iris, retina, gait, palm-prints and hand geometry etc., to accurately identify each individual. The physical feature used in a biometric recognition system must be unique and stable over lifetime. Iris recognition is one of the best biometric recognition systems. It was pioneered by Daugman in 1993. The iris recognition system uses grayscale Near Infrared (NIR) image of eyes as the input. It can extract the iris pattern from the image and use the iris pattern to recognize each individual. The iris can be used as a biometric system because the iris is rich in texture pattern. The iris pattern is developed independent from the generic factor. Individual difference that exists in the development of anatomical structure of body results in such unique patterns. Therefore even identical twins will not have the same iris pattern. There is no physical contact with eye while using the iris recognition system which makes it convenient to use. This is because the iris recognition only needs to take an image of a person's eye at a certain distance. Then iris pattern can be extracted through image preprocessing. Unless a risky surgery is taken, iris pattern remains stable and does not change throughout the life. As a physiological biometric, iris recognition aims to identify persons using iris characteristics of human eyes. Recently, iris recognition has received increasing attention due to its high reliability. These are some of the reasons that iris recognition is better than other biometric recognition.

II. VARIOUS BIOMETRIC SYSTEMS

a) Face -A facial recognition system has numerous advantages over other biometric systems. First of all, the system can be unobtrusive, operating at a large distance from the subject. Also, it does not require the person to have a set interaction with the system. The camera only needs to capture a useable image of the face. Next, the system is usually passive and can operate on fairly low power. Finally, a face recognition system would probably be widely accepted by the general public. There have been significant achievements in the face recognition field over the past few years. Thanks to these advancements, this problem appears to eventually become technologically feasible as well as economically realistic. Several companies now offer face recognition software that can produce high-accuracy results with a database of over 1000 people. In addition, current research involves developing more robust approaches that accounts for changes in lighting, expression, and aging, where potential variations for a given person. Also, other problem areas being investigated includedealing with glasses, facial hair, and makeup. These systems face strong difficulties when the faces arecaptured underdifferent angles and uncontrolled ambient illumination. Moreover, it is still questioned if a face itself is sufficient basis for reliably recognition of a subject, as, for instance, twins have very similar faces. Another problem could be with counterfeit, as users can dramatically change the appearance of their face, through decorative objects or even through plastic surgeries.

b) Fingerprint-Fingerprint recognition has been present for a few hundred years. Nowadays, the technology in this area has reached a point where the cost of purchasing a fingerprint scanner is very affordable. For this reason, these systems are becoming more widespread in a variety of applications. Cell phones, PDAs, and personal computers are a few examples of items incorporating fingerprint recognition to increase user security. Fingerprint systems are generally best utilized in verification systems or small-scale identification systems because a large-scale identification system requires extensive computational resources under current products. In addition, a large system would undoubtedly encounter some fingerprints that are unsuitable for use, due to cuts or other defects. Therefore, cell phones and computers, which both potentially have a small number of users, are ideal products for this Technology .A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy is acceptable. In the past, patterns were extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. The recognition process starts by capturing the finger image by direct contact with a reader device that can also perform some validation procedures to avoid counterfeit measures (check of temperature and pulse). The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as by the minutiae points. These are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The feature values typically correspond to the position and orientation of certain critical points, known as minutiae points. The matching process involves comparing the two-dimensional minutiae sample and template patterns.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

c) Hand Geometry-Hand geometry for biometric purposes is used since the early 1980s. Since hand geometry is not thought to be as unique as other biometric traits, its use is often related with low security applications and, sometimes, associated with other security procedures. Avariety ofmeasurements of the human hand, containing its shape and lengths and widths of the fingers, can be used as biometric characteristics. Feature extraction computes the widths and lengths of the fingers at various locations of the captured image. These metrics define the feature vector of the user's hand. Current research work seeks for new features that could increment the discrimination capacity between different hands, as well the design of a deformable model for the hand, in order toincrease robustness. As main advantages, it can be referred that the hand geometry based biometric systems are easy to use and inexpensive. Additionally, operational environmental factors such as dry weather, or individual differences such as dry skin, generally have no negative effects on identification accuracy. However, it should be stressed that its main disadvantage is its relative low discriminating capacity. Also, the hand geometry may not be invariant over the lifespan of an individual, particularly during childhood.

d) Voice-Oppositely to the majority of the biometric traits that are image-based, voice possesses the singularity of dealing with acoustic information. The most relevant features of a subject's vocal pattern are determined by physical characteristics as the vocal tracts, mouth, nasal cavities and lips shape. These are low varying features over adult lifetime, although the individual behavior and social environments can highly influence the subject's voice. Feature extraction techniques typically measure formants or sound characteristics unique to each person's vocal tract and the pattern matching algorithms are similar to those used in the face recognition. Speech-based authentication is currently restricted to low-security applications because of the high variability in an individual's voice and poor accuracy performance of typical speech based authentication systems. As advantages, the fact that most existing voice based systems are designed for use with standard telephone networks makes it possible to support a broad range of deployments for voice based biometric applications. This turned the technology as the focus of considerable efforts by the telecommunication industry and by the United States government intelligence community, which continues to work on improving its reliability.

e) Signature-Signature can be regarded as unique and results from both behavioral and hand geometry variations associated to each subject. The way a person signs his or her name is known to be characteristic of that individual since centuries, although the analysis of the signature dynamics is recent. There are twomajor strategies to performsignature recognition image based and dynamics analysis. The image based approach is the most classical and is based on the visual appearance of the signature. The dynamic approach analyzes speed, direction and pressure of writing. It has advantages over other biometric techniques that it is asocially accepted identification method already in use in bank and credit card transactions, most of the new generation of portable computers and personal digital
Assistants use handwriting as main input channel. It has disadvantage that oppositely to finger, iris or retina patterns, a signature may be changed by the user, similarly to a password. However, the use of signature-based biometrics has several weaknesses. Individuals with muscular illnesses and people who sometimes sign with only their initials might result in high false rejection rates. Often, signatures dramatically change over a period of time and are influenced by physical and emotional conditions of the subjects. Additionally, since many users are unaccustomed to signing on a tablet, some subjects' signatures may differ from their signatures on ink and paper, increasing the potential for false rejection.

3. INTRODUCTION TO IRIS RECOGNITION

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

The iris is the only internal organ of the body that is readily visible from the outside. The iris begins to form in the third month of gestation and the structures creating its pattern are generally completed by the eighth month. It is the annular region of the eye bounded by the pupil and the sclera (white part of the eye) on either side. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona freckles and a zigzag collarette. Each iris is unique and even irises of identical twins are different. Furthermore, the iris is more easily imaged than retina; it is extremely difficult to surgically tamper iris texture information and it is possible to detect artificial irises. Although the early iris based identification systems required considerable user Participation and were expensive, efforts are underway to build more user-friendly and cost-effective versions. To obtain a good image of the iris, identification systems typically illuminate the iris with near-infrared light, which can be observed by most cameras yet is not detectable by humans. The available results of both accuracy and speed of iris-based identification are highly encouraging and point to the feasibility of large-scale recognition using iris Information .Due to this and to the above described characteristics, it iscommon to consider iris as one of the best biometric traits. Biometrics can be physiological or behavioral Physiologicalcharacteristics include fingerprints, face, retina, iris, etc. Behavioral characteristics include voice, signature, gait, etc. While fingerprint is the oldest and most widely used biometric, recent advances in iris recognition have made iris a very promising biometric trait. Of all the different unique characteristics of human beings, the usage of iris patterns has been found to be the most robust and accurate for the purposes of verification and identification of individuals.

4. DESIGN ISSUES

4.1 Image Acquisition-The first step of Iris Recognition is image acquisition. In image acquisition the image of an eye is captured. While capturing image the environmental conditions such as light intensity, camera to eye distance and orientation of eye affect the quality of captured eye image. A camera must have enough resolution to capture the details of iris pattern.

4.2 Image Segmentation (Boundary Detection)-

The main objective of segmentation is to remove non useful information, namely the pupil segment and the part outside the iris (i.e. sclera, eyelids). As, the useful information lies only in the ring like structure i.e. iris, so the non-useful information i.e. pupil region and sclera region has to be cropped out.

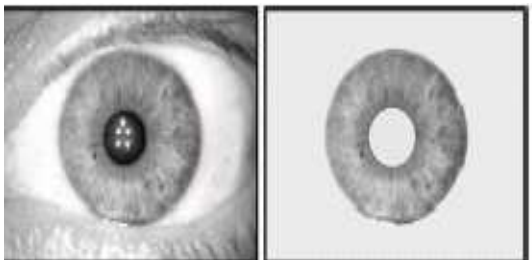

Fig1.Sample eye image and isolated iris pattern.

4.3Iris Feature Extraction-After the segmentation the sample is then transformed using some sort of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectivelycompared with other templates in order to determine identity.

4.4 Iris Pattern Matching-After the feature extraction of the iris, the template is then matched with unknown templates stored in the database. If the match occurs, then the corresponding iris pattern belongs to the

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

storeddatabase and if the matchdoes not occur, then the corresponding iris pattern does not belong to the stored database.

5. DESIGN OF IRIS RECOGNITION SYSTEM

We design low cost, time invariant, secure iris recognition system.

5.1 Proposed System Block Diagram-

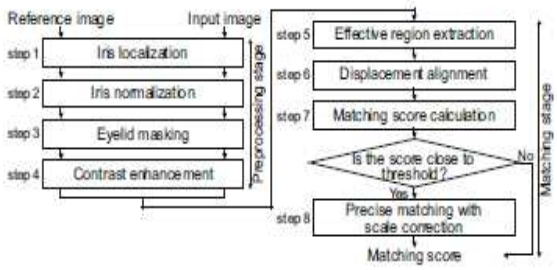

Fig 2: proposed System block Diagram

I) Iris Image Acquisition-This step consists of collection of eye pattern which is to be compared with the images stored in the database.

II) Iris Segmentation (Boundary Detection)-This step consists of extraction of the region between pupil and sclera for analysis i.e. deleting the non-useful part of the eye image and conversion of the iris image into the template form, which contains the discriminating feature and this template can be used for matching.

III) Feature Extraction-This step consists of extraction of the rubber sheet from the segmented iris image.

IV) Iris Template Pattern Matching-This step consists of matching of the template of the input iris image with the template stored in the database. In this iris templates are compared using the phase based image matching algorithm. The phase based image matching technique involves the following steps:

♦ Apply the DFT to the input iris template.
♦ Apply the DFT to the reference iris template.
♦ Determine the phase difference between these two.
♦ Depending upon the phase difference between these two, it can be decided that whether the input iris pattern belongs to the stored database or not.

6. CONCLUSION

As mentioned above we have introduced a various biometric based identification techniques. As we compare various techniques Iris recognition is considered to achieve high security and several advantages compared to otherTechnique. We can successfully design system of low cost with fast response. This proposed system as designed currently can considered a good alternative for security applications though further work is being carried out to achieve better result and ease in implementation

Acknowledgement

This is a part of the M.E thesis work of Mr. S.S.Joshi , submitted to Shivaji University, Kolhapur, India.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

REFERENCES

[1] Daugman, J.G., *How Iris Recognition Works*, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, Number 1, January 2004.
[2] R. Wildes. "*Iris recognition: an emerging biometric technology*". Proceedings of the IEEE, Vol. 85, No. 9, 1997.
[3] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "*An efficient iris recognition algorithm using phase-based image matching*," *Proc. Int. IEEE Conf. on Image Processing*, vol. II, pp. 49–52, Sept. 2005.
[4] K. Miyazawa, K.I to, T. Aoki, K. Kobayashi, and H. Nakajima, "*A phase based iris recognition algorithm*," *Lecture Notes in Computer Science (ICB2006)*, vol. 3832, pp.356–365, Jan. 2006.
[5] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, K. Kobayashi and A. Katsumata, "*An iris recognition system using phase based image matching*," *Lecture Notes in Computer Science (ICB2006)*, vol. 3879, pp. 325–328, Jan. 2006.
[6] L. Ma, T. Tan, Y. Wang, and D. Zhang, "*Efficient iris recognition by characterizing key local variations*," *IEEE Trans. Image Processing*, vol. 13, no. 6, pp. 739–750, June2004.
[7] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, K. Kobayashi and A. Katsumata, "*An implementation oriented iris recognition algorithm using phase based image matching*," *Lecture Notes in Computer Science (ICB2006)*, vol. 7803, pp. 231–234,Jan. 2006.
[8] K. Ito, H. Nakajima, K. Kobayashi, T. Aoki, and T. Higuchi, "*A fingerprint matching algorithm using phase-only correlation*," *IEICE Trans. Fundamentals*, vol. E87-A,no. 3, pp. 682–691, Mar. 2004.
[9] *CASIA iris image database*, Institute of Automation, Chinese Academy of Sciences, [http://www.sinobiometrics.com]