Realtime IRIS Recognition & Authentication System

Ms. Megha Goel
Dept. of IT
S.R.M.C.E.W, RTMNU
Nagpur.
megha.bgoel@gmail.com

Ms. Dhanshri Nikaju
Dept. of CSE
S.R.M.C.E.W, RTMNU
Nagpur
dhanshrinikaju@gmail.com

Ms. Lata Parate
Dept. of CSE
S.R.M.C.E.W, RTMNU
Nagpur
Lparate11@gmail.com

Ms. Vaishnavi Balpande
Dept. of CSE
S.R.M.C.E.W, RTMNU
Nagpur.
vaishubalpande1995@gmail.com

Ms. Minal Ambagade
Dept. of CSE
S.R.M.C.E.W, RTMNU
Nagpur.
minalambagade@rediffmail.com

Ms. Ganga Khandekar
Dept. of CSE
S.R.M.C.E.W, RTMNU
Nagpur.
gangakhandekar95@gmail.com

Abstract— Many organizations are using different kinds of automated person's identification systems which improve the user's need, satisfaction and efficiency to secure resource. The information depends on the recent developments in person's identification using Biometric technology method. By using this technology we are to ensure to identify a person weather he/she is real person or fake person. The aim is to increase the security of biometric reorganization frameworks, by adding liveness assessment in a fast, user friendly and non-intrusive manner.

In this first, a user must be enroll in the system so that his biometric template can be captured. This template is securely stored in a database. This template is retrieved when an individual needs to be identified. Biometric refers to automatic identification of a person based on his/her physiological or behavioral characteristics. This offers several advantages over traditional methods involving ID cards or PIN. To implement this we are using MATLAB.

Keywords: *liveness assessment, iris recognition, authentication, Biometric technology, Image Processing.*

*****

I. INTRODUCTION

A biometric application is essentially a pattern recognition application that operates by acquiring biometric information from particular, extracting a feature vector from the acquired information, comparing this feature vector from the database feature vector. Person authentication has always been an attractive goal in computer vision. Authentication systems based on human characteristics such as face, finger, iris and voice are known Biometrics applications. The basis of many biometric applications is to get the input image and generate important feature vectors like color, texture, etc. The iris of a human being has been historically recognized to possess characteristics unique to each person and so the feature vector extracted from it is also unique. Iris scan biometrics makes use of the unique characteristics and feature vector of the human iris in order to identify a particular with new technologies the eyes are more than “windows to our soul”. Person is carrying with them a living key or password that will never be forget and will always be there. The technology is available now through work in computer vision, pattern recognition, and man-machine interface to create an authentic lock that a person’s iris pattern will open. Iris scan biometrics makes use of the unique characteristics and features of the human iris in order to identify a particular. This iris is the portion of the eye where the pigmented or colored circle, usually brown or blue, rings the dark pupil of the eye. The iris is the colored tissue in the eyeball that surrounds the pupil, and consists of the muscles that adjust the size complex details that can be measured, such as striations, pits, and furrows. The resulting framework in the iris is created at random during the early growth period and is fixed about two years after the birth, and remains unchanged for the rest of one’s life.

The amount of information that can be measured in only one iris is much greater than any other biometrics such as fingerprints, face, voice etc, and the purity is greater than DNA. Iris scanning is considered a particular accurate identification application because the characteristic of the iris does not change during a person’s lifetime, and there are several more variables in an iris, which can be measured. This iris scanning is too fast: it does not take bigger than one or two seconds.

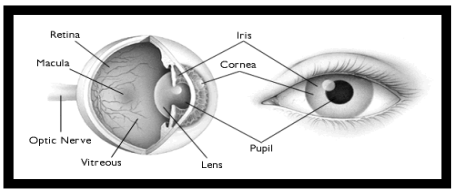

Fig 1.1: Structure of Eye

Fig 1.show the structure of Eye, in this figure**,** the iris scans method start with a photograph. A specialized camera, very close to the subject, not more than three feet, uses an infrared imager to light the eye and capture a very high-resolution image. This process takes only 1 to 2 seconds and provides the details of the iris that are mapped, recorded and stored or future matching and also for verification or authentication. The quality of iris image does not get affected due to the presence of the contact lens and eyeglass and the iris-scan application check for a live eye by checking for the normal continuous rise and fall in pupil size. Iris frameworks are extremely complex, carry an astonishing amount of information and have over 200 unique spots. The fact a particular right eye and left eye are different and that frameworks are easy to capture, setup iris-scan technology as one of the biometrics that is very resistive to false matching and fraud. The false acceptance rate for iris recognition systems is 1 in 1.2 million, statically better than the average fingerprint recognition application. The real benefit is in the false-rejection rate, a measure of authenticated persons who are not accepted.

II. Overview and Problem Definition

A. Overview

Biometrics (ancient Greek: bios ="life", metron ="measure") means two very different fields of study and application. The first, which is the older and is used in biological studies, including forestry, is the collection, synthesis, analysis and management of data on biological communities such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply shown as "biological statistics".

Authentication is the act of confirming something (or someone) as authentic, that is, that claims made by or about the thing are true. The pressure on today's system administrators to have secure systems is ever increasing. One area where security can be improved is in authentication. Iris recognition is a biometric, provides one of the most secure methods of authentication and identification thanks to the unique characteristic of iris. Once the image of the iris has been captured using a standard camera, the authentication method, involving comparing the current subject iris with store data, is one of the most accurate with very low false acceptance and rejection rates. This makes the application very useful in areas such as information security, physical access security, ATMs and airport security.

B. Problem definition

More traditional means of access control include token-based identification systems, such as a driving license or passport, knowledge based system, such as a password or personal identification number. Sometimes these documents or data may not be real. Sometimes this can be steal or hack easily.

III. Literature Survey

[1] Mr. Mule Sandip "Review on Biometric Authentication Methods" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015.

By this paper, we know that eyes are the unique feature for authentication that a person is real user or not and this also tells that we can use multi biometric system for better security. Proper design and implementation of the biometric system can indeed increase the overall security. It is necessary to trust the input device and make the communication link secure.

[2] PROF. MANISHA MORE "A Survey on Iris Recognition Techniques" International Journal of Novel Research in Computer Science and Software Engineering Vol. 2, Issue 1, pp: (89-94), Month: January - April 2015

Iris recognition is regarded as the most reliable and accurate biometric identification application available. By this paper, we describe the novel techniques that are developed to create an Iris Recognition System.

[3] Penny Khaw,"Iris Recognition Technology for Improved Authentication "by SANS Institute Infosec Reading Room, 2002.

The uniqueness of the iris and low probability of a false acceptance or false rejection all contribute to the advantage of using iris recognition technology. It provides an accurate and secure method of real users onto company systems, is a non-intrusive method and has the speed required to minimize user despair when accessing company systems.

[4] Sajida Kalsoom, Sheikh Ziauddin,"Iris recognition: Existing methods and open issues "the fourth international conferences on pervasive and Applications,2012

By this paper, We can use more than one characteristics of biometric to make the multi-biometric system to overcome the problem of single characteristic.

IV. Proposed System

As protecting template in the database securely is one of the challenges in any biometric application. Here real time video preview applied to iris authentication system. In this system there are 5 modules as follows:

1) Live video preview an image dataset implementation
2) Preprocessing
3) Scale invariant feature transform
4) Database image enrollment.
5) Authentication.

For accessing any resource by authentication users, this system can be used.

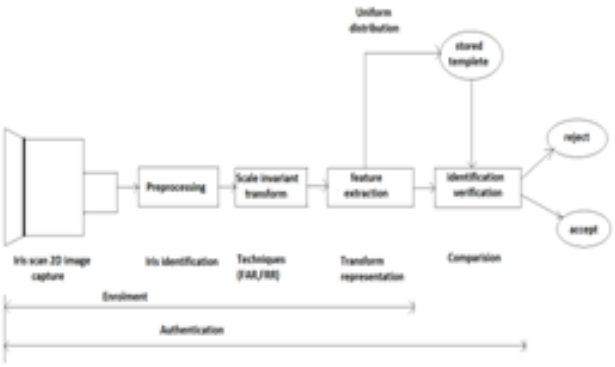

Fig: Typical iris system configuration**.**

V. Methodology

The methodology of our biometric recognition system is to improve the template protection by using the SIFT algorithm. The proposed technique consists of following steps

1. Preprocessing of iris,
2. Iris template extraction,
3. Storing images,
4. SIFT algorithm,
5. Authentication.

In the first step of the system we capture the images of eyes of person from live video preview i.e. just click the image.
The acquired image always contains not only the ‘useful’ parts but also some ‘unuseful’ parts. Under some conditions, the lightness is not uniformly distributed. In addition, various eye-to eye cameras may result in various image sizes of the same eye. For the purpose of analysis, the original image needs to be pre-processed. The pre-processing is made up of three steps as follows:

A. Iris localization:- Both the inner range and the outer range of a typical iris can be taken as circles. But the two circles are usually not co-centric. Compared with the other portion of the eye, the pupil is much darker. We find out the inner range between the pupil and the iris by means of threshold. The outer range of the iris is more difficult to detect because of the low contrast between the two sides of the range. We find out the outer range by maximizing changes of the circumferences-normalized sum of gray level values along the circle. The technique is found to be very efficient and also effective.
B. Iris normalization:- The size of the pupil may change due to the variation of the light, and the associated elastic ups and downs in the iris texture may interface with the results of pattern matching. For the purpose of accurate texture analysis, it is necessary to compensate these ups and downs. Since both the inner and outer ranges of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size.
C. Adaptive thresholding:-The original iris image has low contrast and may have non-uniform light caused by the position of the light source. These may damage the result of the texture analysis. We improve the iris image and reduce the effect of non-uniform light by means of local histogram equalization.
D. Scale invariant feature transform:-The original image of iris has lot of measures due to which we cannot process as it is image for matching purpose. To accomplish the goal of matching we find the important points i.e. features to process on a image. In this step of system we find the features.
Techniques**:**-In this system, techniques FRR and FAR are used as follows:

1. FRR (False Rejection Rate)
   False rejection rate is the rate of authorized person incorrectly rejected by the system.
2. FAR(False Acceptance Rate)
   False acceptance rate is the rate for which the system identifies the non-authorized person. It occurs due to the wrong matching of template with the input.

Scale invariant feature transform:
Image matching is a fundamental aspect of many difficulties in computer world, including object or scene recognition, solving for 3D structure from many images, stereo correspondence, and motion tracking. This paper describes image information that has many properties that make them suitable for matching different images of an object or scene. The features are invariant to image scaling and rotation, and partially invariant to change in light and 3D camera viewpoint. They are well localized in both the spatial and frequency domains, reducing the probability of disruption by occlusion, clutter, or noise. Large numbers of information can be extracted from typical images with efficient algorithms. In addition, the data are highly distinctive, which allows single information to be correctly matched with high probability against a large database of information, providing a basis for object and scene recognition.

The cost of extracting this information is minimized by taking a cascade filtering approach, in which the more expensive operations are applied only at locations that pass an initial test. Following are the major stages of computation used to generate the set of image information:

A. Scale-space extrema detection: The first step of computation searches over all scales and image locations. It is implemented effectively by using a difference-of-Gaussian function to determine potential interest points that are invariant to scale and orientation.

B. Key point localization: At each candidate location, a detailed model is fit to identify location and scale. Key points are selected based on measures of their stability.

C. Orientation assignment: One or more orientations are assigned to each key point location based on local image gradient side. All future operations are performed on image data that has been transformed relative to the assigned orientation, scale, and location for each information's, thereby providing invariance to these transformations.

D. Key point descriptor: The local image gradients are measured at the selected scale in the region around each key point. These are transformed into a representation that permit for significant levels of local shape ups and downs and change in light.

This approach has been named the Scale Invariant Feature Transform (SIFT), as it transform image information into scale-invariant coordinates relative to local information.

An important phase of this approach is that it generates large numbers of information that densely cover the image over the full range of scales and locations. A typical image of size 500x500 pixels will give rise to about 2000 stable information (although this number depends on both image content and choices for multiple parameters). The quantity of features is particularly important for object recognition, where the ability to detect small objects in disorganized backgrounds requires that at least 3 features be correctly matched from each object for reliable identification.

For image matching and recognition, SIFT information are first extracted from a set of reference images and stored in a database. A new image is matched by individually comparing each data from the new image to this previous database and finding candidate matching data based on Euclidean distance of their information vectors. This paper will discuss fast nearest-neighbor algorithms that can perform this computation rapidly against large databases.

The key point descriptors are highly distinctive, which allows single information to find its correct match with good probability in a large database of features. However, in a disorganized image, many features from the background will not have any correct match in the database, giving rise to many false matches in addition to the correct ones. The correct matches can be filtered from the full set of matches by identifying subsets of key points that agree on the object and its location, scale, and orientation in the new image.

VI. Future Scope

Iris Scanning offers numerous advantages over other biometrics, although there are a few definite issues surrounding this application. First and foremost, iris scanning is fairly expensive. Iris scanning produces an accurate image, but it still depends on user co-operation. a user must know he is being scanned and agree to it for the scan to work. This is because a person must sit quite still even just momentarily to get an accurate scan.

VII. Conclusion

While biometric authentication can offer a high degree of security, they are away from perfect solution. Sound principles of system engineering are still necessary to ensure a high level of security rather than the assurance of security coming simply from meeting of biometrics in some form. The risks of compromise of distributed database of biometrics used in security application are high- particularly where the privacy of persons and hence non-repudiation and irrevocability are not easy. It is possible to remove the need for such distributed databases through the concern application of biometric infrastructure without compromising security.

Careful consideration of the importance of biometrics information and how it should be unlawfully protected is now required on a wider scale. In our project we are providing the person is authenticated or not.

References

[1] Mr. Mule Sandip "Review on Biometric Authentication Methods" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 11, November 2015.

[2] PROF. MANISHA MORE "A Survey on Iris Recognition Techniques" International Journal of Novel Research in Computer Science and Software Engineering Vol. 2, Issue 1, pp: (89-94), Month: January - April 2015

[3] Penny Khaw,"Iris Recognition Technology for Improved Authentication " by SANS Institute Infosec Reading Room, 2002.

[4] Sajida Kalsoom, Sheikh Ziauddin,"Iris recognition: Existing methods and open issues "the fourth international conferences on pervasive and Applications2012

[5] H. B. Kekre, Tanuja K. Sarode, Vinayak Ashok Bharadi, Abhishek A. Agrawal, Rohan J. Arora, And Mahesh C. Nair, "Iris Recognition Using Discrete Cosine Transform And Kekre's Fast Codebook Generation Algorithm", Journal Of Electronic Science And Technology, Vol. 8, No. 3, Pp. 223-229, September 2010.

[6] Shirke Swati D., ShirkeSuvarna D. And Gupta Deepak, "Iris Recognition", Emerging Trends In Computer

Science And Information Technology 2012 (ETCSIT2012), Pp. No. 20-23.

[7] G. Savithiri, A.Murugan, "Performance Analysis On Half Iris Feature Extraction Using GW, LBP And HOG", International Journal Of Computer Applications, Volume 22, No.2, Pp. 27-32, May 2011.

[8] Rishabh Parashar, Sandeep Joshi, "Comparative Study of Iris Databases And UBIRIS Database For Iris Recognition Methods For Nonco-operative Environment", International Journal Of Engineering Research & Technology (IJERT), Vol. 1, Issue 5, July – 2012.

.