IJCSE International Journal of Computer Science and Engineering Open Access
Technical Paper Volume-2, Issue-3 E-ISSN: 2347-2693

IRIS Recognition and Authentication System for Enhancing Data Security

Yogesh Badhe[1*], Hafij Balbatti[2], Neelkanth Kaladagi[3] and Kranti Kumar[4]

[1*,2,3,4]*Computer Department, PCCOE, Pune University, India, yogerocks@gmail.com*

www.ijcseonline.org

Received: 7 March 2014 Revised: 18 March 2014 Accepted: 26 March 2014 Published: 30 March 2014

***Abstract*—** IRIS recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the IRIS es of an individual's eyes. Not to be confused with another less prevalent ocular-based technology, retina scanning, IRIS recognition uses camera technology, and subtle IR illumination to reduce specular-reflection from the convex cornea to create images of the detail-rich, intricate structures of the IRIS . These unique structures converted into digital templates, provide mathematical representations of the IRIS that yield unambiguous positive identification of an individual. IRIS recognition efficacy is rarely impeded by glasses or contact lenses. IRIS technology has the smallest outlier (those who cannot use/enroll) group of all biometric technologies. The only biometric authentication technology designed for use in a one-to many search environment, a key advantage of IRIS recognition is its stability, or template longevity as, barring trauma, a single enrolment can last a lifetime.

***Index Term*—** Image Processing, IRIS recognition, Biometrics for Data Security, Secure Biometrics

I. INTRODUCTION

Basically a system is to be implemented to provide security to data using IRIS recognition of the individual by comparing it the stored IRIS image of the same person.

One of the most dangerous security threats in today's world is impersonation, in which somebody claims to be someone else. Through impersonation, a high-risk security area can be vulnerable. An unauthorized person may get access to confidential data or important documents can be stolen. Normally, impersonation is tackled by identification and secure authentication, however, the traditional knowledge-based (password) or possession-based (ID, Smart card) methods are not sufficient since they can be easily hacked or compromised. Hence, there is an essential need for personal characteristics-based (biometric) identification due to the fact that it can provide the highest protection against impersonation. Among other biometric approaches, the new IRIS recognition technology promises higher prospects of security. Therefore, this research is conducted to further explore the potential of the IRIS recognition technology and to demonstrate its potential through the development and evaluation of a working prototype.

The IRIS recognition system consists of an automatic segmentation system and is able to localize the circular IRIS and pupil region, occluding eyelids and eyelashes, and reflections. You have to store an IRIS image of an individual in database. Using that stored template in database we will be matching the present image. Based on the result we will be identifying a particular person.

Along with IRIS identification system we will be designing a encryption/ decryption toolkit using IRIS code as key. The encryption and decryption process works in combination with a key a word, number, or phrase to encrypt the data. The same data encrypts to different cipher data with different keys. The security of encrypted data is entirely dependent on two things:

- The strength of the cryptographic algorithm
- The secrecy of the key.

But when we talk about the secrecy of the key then, in the case of passkey used as, a word, phrase or a number, any of these passkeys can be leaked out. Hence a better authentication technique is needed to be implemented so that it would help in the following

- No leakage of passkey
- High security to a confidential data
- Unique authentication for data

So IRIS scanning is really a reliable means of identification. Unlike other forms of identification, such as passwords or keys, a person's IRIS cannot be stolen, forgotten or lost.

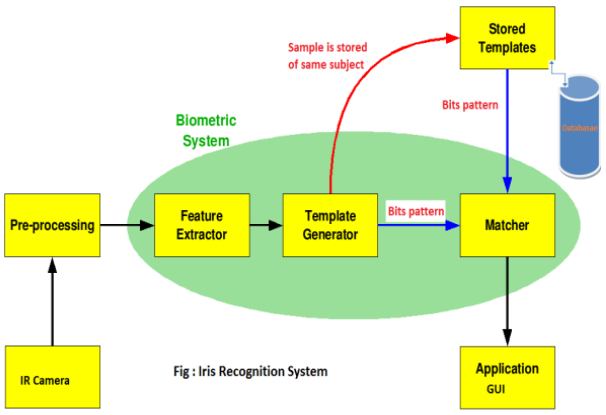


Fig.1 IRIS Recognition System

Corresponding Author: *Yogesh Badhe*

II. RELATED WORKS

IRIS recognition is the process of identifying a person on the basis of IRIS template. An IRIS is identified by comparing an IRIS image stored in the database. User identification is basically a pattern classification problem preceded by a feature extraction stage.

Software engineering approaches its midlife with many accomplishments. Today, it is recognized as a legitimate discipline, one worthy of serious research, conscientious study, and tumultuous debate. Throughout the industry, software engineer has replaced programmer as the job title of the preference. Software process models, software engineering methods, and software tools have been adopted successfully across a broad spectrum of industry applications. For achieving reliability and effectiveness in the project, an appropriate software model should be chosen to do the work in a systematic and disciplined way.

In [1] paper presents the complete IRIS recognition system consists of an automatic segmentation system based on the Hough Transform, and is able to localize the circular IRIS and pupil region, occluding eyelids and eyelashes, and reflections. And in [2] show that the Levenstein distance has better discrimination in comparing IRIS codes than the Hamming Distance. But in our work we are using bit pattern matching technique for matching the IRIS codes.So our work is improving the previous work done in the IRIS recognition system and also our work shows how we can enhance the security of data by protecting with the unique IRIS code.

III. PROBLEM STATEMENT AND OBJECTIVES

Capturing Of Image:

Within the biometrics context, the IRIS is commonly accepted as one of the most accurate biometric traits and has been successfully applied in such distinct domains as airport check-in or refugee control. However, for the sake of accuracy, present IRIS recognition systems require that subjects stand close (less than two meters) to the imaging camera and look for a period of about three seconds until the data is captured. This cooperative behavior is required to capture images with enough quality for the recognition task. However, it simultaneously restricts the range of domains where IRIS recognition can be applied, especially those where the subject's cooperation is not expectable (e.g., criminal/terrorist seeks, missing children). [3]

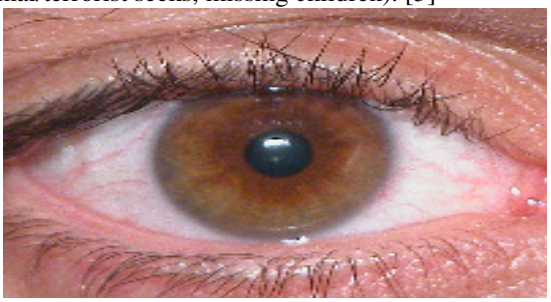


Fig.2 Infra Red Image Of Eye

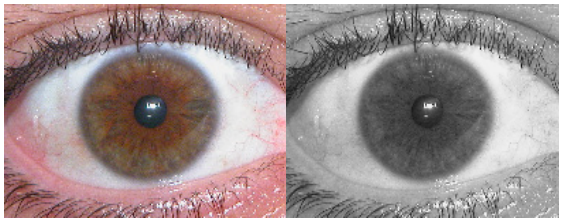
Therefore we are using IR images of eye. And this is readily available from UBIRIS [4] database. The main focus of the UBIRIS database is to minimize the requirement of user cooperation, i.e., the analysis and proposal of methods for the automatic recognition of individuals, using images of their IRIS captured at-a-distance and minimizing the required degree of cooperation from the users, probably even in the covert mode.

Gray Scaling Of IRIS Image:

In image processing, a grayscale or greyscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest. [5]

Grayscale images are often the result of measuring the intensity of light at each pixel in a single band of the electromagnetic spectrum (e.g. infrared, visible light, ultraviolet, etc.), and in such cases they are monochromatic proper when only a given frequency is captured. But also they can be synthesized from a full color image; see the section about converting to grayscale.-

Mathematical formula: Gs=(R+G+B)/3



Input Image Gray Scale Image

Fig.3 Conversion Of IR Image Of Eye To Gray Scale Image

Sobel Edge Detection:

Edges characterize boundaries and are therefore a problem of fundamental importance in image processing. Edges in images are areas with strong intensity contrasts – a jump in intensity from one pixel to the next. Edge detecting an image significantly reduces the amount of data and filters out useless information, while preserving the important structural properties in an image. There are many ways to perform edge detection.

We are using Sobel edge detection algorithm for detecting the edge of IRIS

Sobel edge detection algorithm:

The input image is first converted to gray scaled image.
– Traverse through entire image.
– For each pixel in the image we will take a window of 3*3 pixels and multiply it the given template for matrix.
– Then we will calculate the G using formula.

$$|G| = \sqrt{Gx^2 + Gy^2}$$

- Template

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Apply the templates to a 3x3 filter window

a1	a2	a3
a4	a5	a6
a7	a8	a9

3x3 filter window

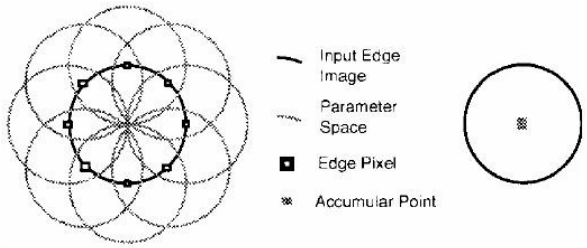
Where a1 .. a9 are grey levels of each pixel in the filter window.

X = -1*a1 + 1*a3 - 2*a4 + 2*a6 - 1*a7 + 1*a9
Y = 1*a1 + 2*a2 + 1*a3 - 1*a7 - 2*a8 - 1*a9

Sobel Gradient = sqrt(X*X + Y*Y) then set every pixel to reconstruct the image again.

Circular Hough Transform:
A commonly faced problem in computer vision is to determine the location, number or orientation of a particular object in an image. Often the objects of interest have different shapes than lines, it could be parables, circles or ellipses or any other arbitrary shape. The general Hough transform can be used on any kind of shape, particularly for circular shapes we will look at the Circular Hough Transform (CHT).

Circular Hough Transform Algorithm:
The algorithm for Circular Hough Transformation can be summarized to [6]:
1. Find edges
//HOUGH BEGIN
2. For each edge point
Draw a circle with center in the edge point with radius r and increment all coordinates that the perimeter of the circle passes through in the accumulator.
3. Find one or several maxima in the accumulator
//HOUGH END
4. Map the found circle corresponding to the maxima back to the original image



Working of Circular Hough Tranform :

Output imaged detecting circle

Fig. 4.Working Of Circular Hough Transform [7]

Daugman's Rubber Sheet Model:
It is a process of normalization of IRIS region by unwrapping the IRIS and converting it into its polar coordinates. The rubber sheet model remaps each point within the IRIS region to a pair of polar coordinates. The homogenous rubber sheet model accounts for pupil dilation, imaging distance and non-concentric pupil displacement, it does not compensate for rotational inconsistencies.

The radial resolution was set to 100 and the angular resolution to 2400 pixels. For Every pixel in the IRIS , an equivalent position is found out on polar axes. The normalized image was then interpolated into the size of the original image, by using the interp2 function. The parts in the normalized image which yield a NaN, are divided by the sum to get a normalized value.

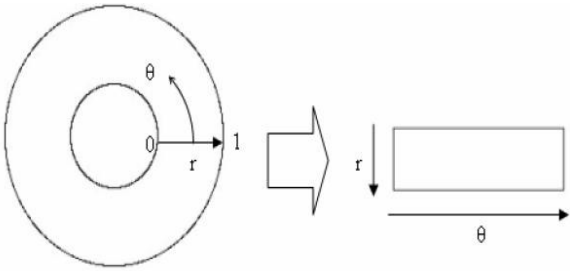


Fig.5 Unwrapping of IRIS into polar coordinates [8]

Bit Pattern Generation Using Local Binary Pattern:
Local binary patterns (LBP) are a type of feature used for classification in computer vision. Using Local Binary Pattern, bit pattern is generated from the IRIS . Since an individual IRIS region contains features with high degrees of freedom, each IRIS region will produce a bit-pattern which is independent to that produced by another IRIS , on the other hand, two IRIS codes produced from the same IRIS will be highly correlated.

Concept
The LBP feature vector, in its simplest form, is created in the following manner:

- Divide the examined window into cells.
- For each pixel in a cell, compare the pixel to each of its 8 neighbours (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle, i.e. clockwise or counter-clockwise.
- Where the center pixel's value is greater than the neighbour's value, write "1". Otherwise, write "0". This gives an 8-digit binary number (which is usually converted to decimal for convenience).
- Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center).
- Optionally normalize the histogram.
- Concatenate (normalized) histograms of all cells. This gives the feature vector for the window.[9]

Template matching:
Now in template matching what we do is we now match the generated Bit pattern with the stored bit pattern of IRIS in database. We will match the two bits if match is found some score value is added and that goes on increasing accordingly and if not found we start with the negative value of the starting score value. On the basis of threshold score decision of valid IRIS is made and authentication is done [10].

Encryption/Decryption Of Data:
The RSA algorithm can be used for public key encryption. The 3 basic steps of this algorithm are: [11]

(1) Key Generation Algorithm
(2) Encryption
(3) Decryption

RSA offers a very secure encryption method that addresses these concerns

(1) Authentication
(2) Confidentiality
(3) Key exchange

RSA Key Generation Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1)(q-1).
3. Choose an integer e, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent d, 1< d < phi, such that e d = 1(mod phi).
5. The public key is (n, e) and the private key is (n, d). The values of p, q, and phi should also be kept secret.
   Where
- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

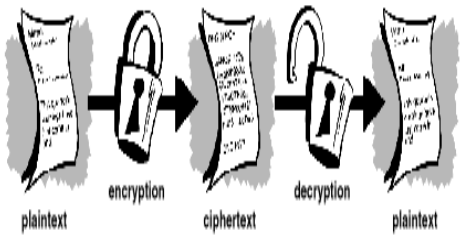


Fig. 6 RSA Encryption and Decryption Algorithm

a) Encryption
Sender A does the following:-

(1) Obtains the recipient B's public key (n, e).
(2) Represents the plaintext message as a positive integer m.
(3) Computes the cipher text $c = m^{\wedge e} \bmod n$.
(4) Sends the cipher text c to B.

b) Decryption

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^{\wedge d} \bmod n$.

Extracts the plaintext from the integer representative m.

IV. METHODOLOGY

IRIS recognition is the process of identifying a person on the basis of IRIS image. It is a known fact that recognition is a image dependent feature that enables us to recognize individual. During the years ahead, it is hoped that IRIS recognition will make it possible to verify the identity of persons accessing systems, allow automated control of services, such as banking transactions; and also control the flow of private and confidential data. While fingerprints and retinal scans are more reliable means of identification, image can be seen as a non-evasive biometric that can be collected with or without the persons knowledge. Unlike other forms of identification, such as passwords or keys, a person's IRIS cannot be stolen, forgotten or lost. IRIS recognition allows for a secure method of Transfer of data.

V. APPLICATIONS

- Using IRIS Recognition data is more secure than other methods.
- It can be used in banks and big organizations for security purpose.

- IRIS Recognition can be used in going through investigation of criminal records.
- IRIS Recognition can be used to make personal lock chambers in banks and other secret organizations so that it can allow only selected entry.
- Secure data exchange between two parties as it is protected by IRIS pattern template.

VI. CONCLUSION

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.

REFERENCES

[1] IRIS Recognition System using Biometric Template Matching Technology Sudha Gupta, Asst. Professor, LMIETE, LMISTE,Viral Doshi, Abhinav Jain and Sreeram Iyer, K.J.S.C.E.Mumbai India 2010 International Journal of Computer Applications (0975 8887)Volume 1,No. 2.

[2] IRIS Recognition**,** Shirke Swati D.,Shirke Suvarna D.,Gupta, Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012)Proceedings published in International Journal of Computer Applications (IJCA).

[3] http://IRIS .di.ubi.pt/about.htm

[4] http://IRIS .di.ubi.pt/

[5] Stephen Johnson (2006). Stephen Johnson on Digital Photography (http://books.google. com/ books?id=0UVRXzF91gcC& pg=PA17&dq=grayscale+ black-and-white-continuous-tone& ei=XlwqSdGVOILmkwTalPiIDw). O'Reilly. ISBN 0-596-52370-X.

[6] Bryan S. Morse. Lecture 15: Segmentation (edge based, hough transform). Brigham Young University:Lecture Notes, 2000.

[7] Object Detection using Circular Hough Transform, American Journal of Applied Sciences 2 (12): 1606-1609, 2005,ISSN 1546-9239.

[8] Mahboubeh Shamsi, Abdolreza Rasouli "A Novel Approach for IRIS Segmentation and Normalization" Faculty of Computer Science & Information System Islamic Azad University.

[9] http://en.wikipedia.org/wiki/Local_binary_patterns

[10] Christel-loïc TISSE1, Lionel MARTIN1, Lionel TORRES 2, Michel ROBERT "Person identification technique using human IRIS recognition" 21Advanced System Technology STMicroelectronics – ZI Rousset – 13106 Rousset Cedex, France.

[11]]Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126. doi:10.1145/359340.359342.