

AC 2007-1553: PRACTICAL CONSIDERATION FOR IMPLEMENTING A GUI-BASED IRIS RECOGNITION SYSTEM IN A LEARNING ENVIRONMENT

Amjad Zaim, University of Texas-Brownsville

Mahmoud Quweider, University of Texas-Brownsville

Practical Considerations for Implementing a GUI-Based Iris Recognition System in a Learning Environment

Abstract

The iris, the concentric ring-shaped colored portion of the eye that encloses the dark disc of the pupil, possesses rich and distinct features unique for each individual. Although most current identification and authentication systems use more traditional biometric features, e.g. fingerprints and hand-written signatures, the iris-based recognition has proven to be far more accurate and therefore provides a good alternative resource. The main algorithmic components that are usually involved in any personal identification system that utilizes the human iris are: image data acquisition, iris localization and segmentation, feature extraction and decision making. These scientific methods that enable this advanced biometric technology is a good example of how cross-disciplinary scientific methods –such as artificial intelligence or AI, image processing, as well as practical software design tools such as graphical-user-interface-design, can come together to provide an integrated solution to a challenging security problem. In our computer science department, we have a need to demonstrate this computer-based technology to our new graduate and undergraduate students as a means to enhance their learning experience and motivate them to utilize their computer knowledge and skills in solving real-life problems. Aside from the scientific algorithm involved, the project addresses several practical considerations involved in the design and development of iris-based recognition systems such as system functionalities as well as the flexibility and the acceptability for the user interface. Two computer science students were assigned the task of designing, building and implementing a prototype using software development tools and scientific computing methods. In this paper, we provide general guidelines while highlighting some of the important issues involved in the design of biometric systems exploring the specific case of iris-based recognition.

Introduction

A biometric is a distinct, unique, and measurable physical and/or physiological characteristic of a person which can be used to identify or verify his or her identity. Iris pattern, voice, facial characteristics or fingerprints are some examples of biometric measures. Additionally, the term biometrics implies automatic recognition of an individual. The iris, or the colored portion of the eye around the pupil, has been found to possess rich and distinct features unique for each individual [1-4]. Using an individual's iris features for the purpose of identification enables a high degree of certainty of a person's identity because of its unique features (Fig. 1), especially when combined in a hybrid arrangement. Iris biometrics has proven to be a viable solution to a number of security-related applications. Its application ranges from allowing physical access into secure sites, networked computers, sensitive facilities, and financial transactions where prevention of identity theft is vital, as well as surveillance applications such as identifying a potential terrorist in a public place. In academic and research environments, biometrics is especially useful for access control to private areas, laboratories containing

hazardous materials, network access to academic and administrative online electronic records and others. In industrial and business applications, it can also be used as a time-register or an attendance system. The technology continues to evolve at a rapid pace in response to numerous security issues; hence, the study of this newly emerging field is being increasingly incorporated into the curriculum of several computer science and engineering undergraduate and graduate programs in US colleges and universities.

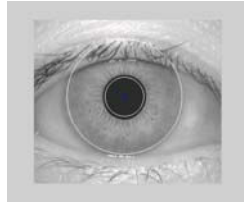


Figure 1. An image of the eye with the iris encircled with a circle.

This field of biometric identification is a highly interdisciplinary field that draws upon human anatomy and physiology, physics, mathematics, engineering and computer science to achieve rapid, positive authentication of individuals. However, this multidisciplinary technology has firm foundations in several branches of computer science such as Digital Image Processing (DIP), Computer Security Systems, Software Design and Artificial Intelligence (AI) (particularly in Machine Learning). For example, image processing deals with the challenging task of capturing, extracting and transforming individual's raw biometric data/images into unique and recognizable digital feature. Machine Learning, a subfield in AI, deals with the construction of classifiers from previously observed examples that can accurately classify or distinguish an individual by matching his/her extracted biometric features to one that has previously been stored in a populated database with a catalogue of users' features. Computer Security deals with the issue of generating digital signatures from biometric features of authenticated individuals in order to limit network access and prevent the menacing activity of hackers. Software Engineering plays a crucial role in creating a modular and parallel implementation of complex recognition algorithms so that real-time or semi real-time realization of human identification enhances its practicality in real-life situations.

With such a critical and developing field of technology, and because advancements in biometrics is highly contingent upon several areas of computer science, it becomes important to expose our students, who are potentially future contributors and leaders in this domain, to the latest systems and methods of biometric identification. Currently, our students are modestly exposed to the principles of biometrics theory in two undergraduate and graduate level courses: Digital Image Processing and Artificial Intelligence. In this paper we describe a GUI-based iris-recognition system that has been developed by students in the undergraduate program of our computer science department. The main purpose of such as system is to demonstrate how CS students can harness their computer science skills in this rapidly advancing technology of biometric. This also comes as part of our future plan to build a comprehensive and integrated state-of-the-art Biometrics Laboratory to support all efforts to introduce this emerging technology into research, education and training of our computer science undergraduates and graduates. In this

paper, we provide an overview of iris recognition technology and discuss critical design issues of iris-based recognition systems that have significant impacts on functionality and performance.

How Does Iris Recognition Works?

The concept of iris recognition technology borrows from computer vision, pattern recognition, and optics. In a typical setting, a black-and-white infrared video camera zooms in on the iris and records a sharp image of it while being lit by a low-level light to aid the camera in focusing. A frame from this video is then digitized usually into a 512 byte file and stored on a computer database. Most iris recognition cameras are capable of recording this image from as much as 16 inches (40.64 centimeters) away, so no physical contact is necessary. An individual's identity can then be confirmed by taking another picture of their iris and comparing it to those in the database. Most iris recognition technology can confirm someone's identity within a matter of few seconds. The main subsystems that are usually involved in any personal identification system that utilizes the human iris are: image data acquisition, iris localization and segmentation, feature extraction and decision making [1], [4]. The literature is rich with extensive studies on all these subsystems. Feature extraction and decision making, however, is the most critical part is aimed at deriving iris features of high discrimination power using several mathematical algorithms (i.e. phase-based methods [4], zero-crossing representation methods, texture analysis-based methods [2], and intensity variation analysis-based methods [1]). Due to the subtleness and the great irregularity of iris features, the best method of iris recognition is still the subject of some debate although Daugman's method described in [4] seems to be the most widely used in industry. Although, the focus of this paper is on the software design aspect of iris-based recognition systems regardless of the mathematical algorithms used, it is rather important to briefly outline the general idea and the purpose of each algorithm involved.

Algorithm Description

a) Signature Generation

One of the greatest challenges in most biometric applications is to transform the raw biometric signal/image obtained for different individuals into a unique code or signature with one standard format that can be compared or matched against other similar signatures. This is accomplished with a set of procedures described below.

1) Image capturing and selection

The first task is to acquire one or more images of the eye. Often, acquired iris images contain several defects which make iris recognition very difficult. For example, the iris may be occluded by eyelids or eyelashes, or the subject may have moved their eye causing a blurred image. For this reason, it is common to take several images of the iris in

succession and choose the best one as a candidate image. It is also common to apply a set of image processing techniques to improve the quality of the captured image and enhance the iris features especially in dark environments or under excessive lighting conditions. Artifacts due to motion blurring can also be reduced if the proper image processing tools are used.

2) Image Segmentation

In order to process the iris data and exclude the rest of the features, such as eyelids, it's necessary to extract or segment the iris from the rest of the candidate eye image. This task can be difficult especially under poor illumination conditions. Often, segmenting the whole iris is not possible since the subject's eye may not be fully open. Fortunately, this is not necessary since most of the information needed can be found in a small annular region of the iris. Again, the power of image processing can be exploited to accentuate iris features by reducing, for example, the effects of varying background illumination and increasing contrast through some image enhancement algorithms.

3) Feature Encoding

The iris image is primarily a gray-scale values that carry subtle and unique features. Depending on many factors including subject-to-camera distance, the distinct patterns are embedded within the iris in variable scale and orientation. Therefore, it becomes necessary to extract a feature, or a set of features stored in a feature vector, that will serve as the iris code or signature to be used for comparisons with other iris features. This module is responsible for generating the iris code or signature using predefined mathematical texture features.

b) Matching

Having been extracted and encoded, the iris signature must be efficiently matched and compared to other stored signatures using some type of a similarity or a difference measure. One commonly used similarity measure called hamming distance (HD) entails converting each feature vector to a binary sequence using an exclusive OR operation. The hamming distance is written as:

$$HD = \frac{1}{N} \sum_{j=1}^N X_j (XOR) Y_j$$

Where X and Y are two signatures of two individuals and HD(X,Y) describes the hamming distance from X to Y. Another similarity measure describes the normalized correlation Q between the acquired and database representation for goodness of match

$$\frac{\sum_{i=1}^n \sum_{j=1}^m (p_1[i, j] - \mu_1)(p_2[i, j] - \mu_2)}{nm\sigma_1\sigma_2}$$

where p_1 and p_2 are two-dimensional signatures of size $n \times m$, μ_1 and σ_1 are the mean and standard deviation of p_1 , and μ_2 and σ_2 are the mean and standard deviation of p_2 . The choice of the similarity measure to use is not a trivial one and depends largely on the nature of the encoded signatures. Often, a matching score is derived from two or more similarity measures, by using their weighted sum for example. The critical decision to accept or reject a user depends significantly on how the similarity measure can capture inter-class (of different subjects) variability and intra-class (of the same subject) similarity.

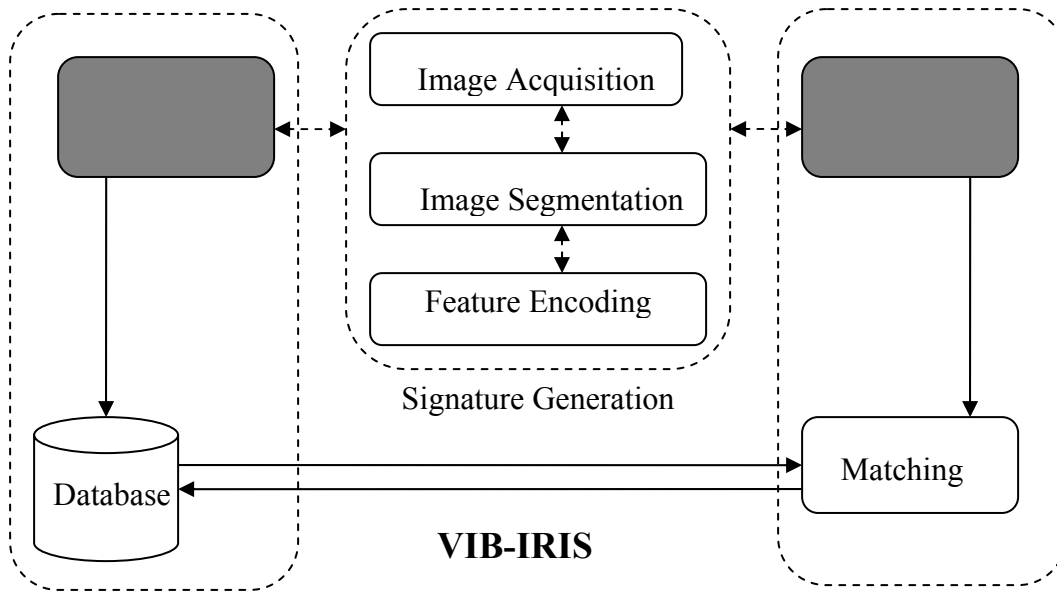


Figure 2. Design illustration of the Iris recognition System.

System Description

The design phase of the Iris-based security system took into consideration three important elements: efficient memory allocation to handle the large size of raw camera images of the eye, a highly optimized code to reduce execution time and improve real-time performance, and an interactive and intuitive GUI to enhance the user experience. A description of the system is shown in figure 2. The main modules involved are the enrollment module and recognition module which are described in details below.

a) Enrollment Module

The first step in the operation of any biometric system is to create a pool of users from which an unknown individual can be identified. In our system, the enrollment module starts by archiving the user information to an attached ACCESS database. During enrollment of a new user, a unique ID number is automatically generated and the administrator is prompted to enter the user's first name, last name, age and street address. The administrator can also choose to designate the user's status as either active or inactive. This facilitates the process of removing or restoring an existing user easily with one mouse click.

Once the user information has been gathered, the enrollment module proceeds to obtain his/her iris signature. At this point, The Signature Generation module calls upon the *Image Acquisition* module to acquire a fine image (picture) of the Iris using the attached Infrared Iris camera. The user is then instructed to look directly into the camera lens and pause while as series of images of his eye are captured. The best-quality image is then passed to *Segmentation* to isolate the iris portion of the eye and then to the *Feature Extraction* subroutine where a binary signature files is generated and stored. The signature file is given a unique name using the user ID as a prefix to a filename associated with the user record referenced from the database. Therefore, the fields in the database have the following form:

ID	LastName	FirstName	Address	Age	Enabled	SignatureFilename
----	----------	-----------	---------	-----	---------	-------------------

There are other functionalities that the enrollment module provide including the ability to modify the user information currently in the database and to load a new database where a set of different users have been previously stored. The enrollment module also allows simultaneous visualization of the users. In addition, the enrollment also facilitates activation and deactivation of users from two lists of active and inactive users (Fig. 3).

b) Iris Recognition Module

Authentication:

Once the users have been manually entered and their iris signature have been generated and associated with their record, the system is ready to identify new unknown users through the Authentication button (Fig. 3). This option again prompts an incoming user, who has not yet been identified, to look directly into the camera so that his/her iris signature can be obtained. At this point, the Signature Generation module is invoked again resulting in an iris signature to be obtained. The recognition module passes this signature to the matching module which proceeds to match this signature against all other signature file in the current database. The matching process relies on a similarity measure or a score that describes how similar or different the unknown iris signature is to each of the other signatures, as described in the matching algorithm.

The key objective of an iris recognition system is to be able to achieve a distinct separation of intra-class and inter-class distributions using the similarity measure. With

clear separation, a similarity measure or correlation factor value can be chosen which allows a decision to be made when comparing two signatures. If the similarity between two signatures is less than a separation point, or a Threshold, we can conclude that the both signature were generated from the same iris and hence from the same subject and therefore a match is found. Otherwise if the similarity is greater than the separation point the two signatures are considered to have been generated from different irises and therefore belong to two different subjects. The following pseudo code illustrates this point.

```
FOR J = 1 : N
    IF ([Similarity (Sig(J), Sig(R)] < Threshold ) then
        Subject(R) Is Subject(J)
    ELSE
        Subject(R) IsNot Subject(J)
    END IF
END FOR
```

Therefore, for an unknown subject R, the matching process is an iterative process of comparing its signature Sig(R) to all other signatures {Sig(1), Sig(2),...Sig(N)}. The Threshold is a predefined variable that can take a range of values depending on the similarity measure used (0-0.5 for HD and 0-1 for NQ). Varying the threshold value allows the user to vary the security level (or the level of acceptance or rejection) during recognition. The optimal value is usually obtained experimentally as explained next.

Security Level:

The distance between the minimum Threshold value for inter-class comparisons and maximum Threshold value for intra-class comparisons could be used as a metric to measure the “goodness of the match” and to decide on a match vs. non-match. However, this metric is very dependent on the number of iris signatures compared. A better metric is ‘decidability’, which takes into account the mean and standard deviation of the intra-class and inter-class distributions [4]. With a pre-determined separation distance, a decision can be made as to whether two signatures were created from the same iris (a match), or whether they were created from different irises. However, the intra-class and inter-class distributions may have some overlap, which would result in a number of incorrect matches or false accepts, and a number of mismatches or false rejects. The false reject rate (FRR), measures the probability of an enrolled genuine individual being rejected by the system. The false accept rate (FAR), measures the probability of an individual, or an imposter, being wrongly accepted and authenticated. The false accept and false reject rates can be calculated by the amount of overlap between two

distributions. A typical probability plot demonstrates both concepts (Fig. 4). Clearly the separation point will influence the false accept and false reject rates, since a lower separation distance will decrease FAR while increasing FRR, and vice versa. Therefore, when choosing a separation point it is important to consider a reasonable ratio between the false accept rate and false reject rate.

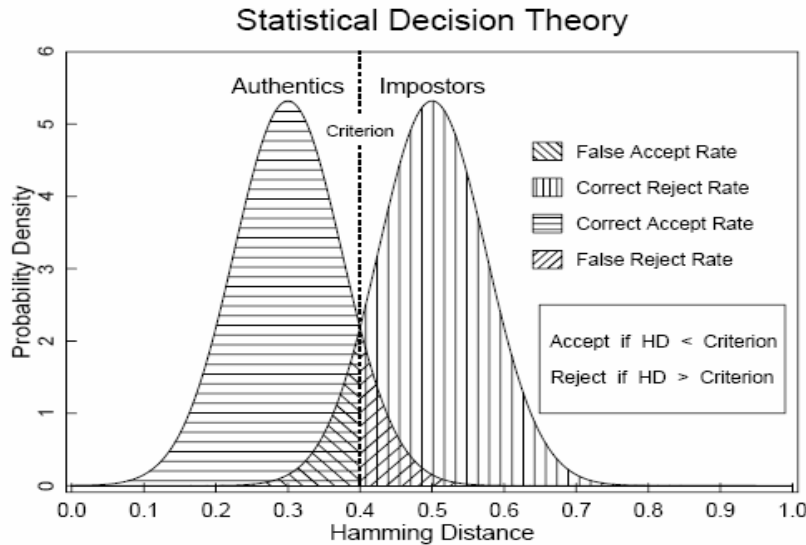


Figure 4. A typical plot showing the authentication performance of an iris-recognition system.

In light of the discussion above, it's often that a compromise has to be reached between the two extreme ends of FRR vs. FAR. It is recommended that the administrator is given the option to choose from three levels of security "Low", "Med" and "High". The lowest level of security can be used in situations where security breaches do not result in a great threat or when the recognition process is secondary to more traditional authentication methods such as usernames and passwords. On the other hand, a highest level should be instituted if false authentication of an imposter can result in access to sensitive information or to highly classified materials.

Event Trigger:

Usually upon making the decision to accept or reject an unknown individual, an event or a list of events are considered depending on the security application at hand. For example, to control access to a private facility, an electronic door latch can be wired to the PC serial port and triggered by a control signal issued by the recognition module. A network access can also be facilitated by using the iris codes itself as a user password after storing it for each person in a central database. The iris features can also be incorporated into cryptography by mapping the iris code into a bit string, for example.

Conclusion:

In this paper, we discussed practical issues in the design and implementation of iris-based recognition security system. Although, the main concepts provided in this report can be used as general standard guidelines for development of iris-based recognition, our primary motivation behind this project is to familiarize our computer science students with this rapidly emerging technology and to increase their level of enthusiasm about the its promising future. The developed system is expected to support courses and faculty research, courses and visitor familiarity with this interesting application of computer science. The system will also be installed in different laboratory modules for use in capstone projects and to demonstrate concepts in digital image processing and artificial intelligence (particularly those in machine learning) that are crucial for understanding subjects in biometrics, respectively. These laboratory modules will in turn motivate students to engage in coursework projects of biometric nature for lower level courses such as, Database, Software Design, and others. Other similar courses aimed toward advancing students proficiency in biometrics technology for engineering students can also benefit from this system to emphasize the engineering components of biometrics such as sensor characteristics, signal processing, as well as experimental design and analysis.

Bibliography

- [1] R. Wildes, "Iris Recognition: An Emerging Biometric Technology", *Proc. IEEE*, vol. 85, pp. 1348-1363, 1997.
- [2] R. G. Johnson, "Can iris patterns be used to identify people," Los Alamos National Laboratory, CA, Chemical and Laser Sciences Division, Rep. LA-12331-PR, 1991
- [3] D. Miller, *Ophthalmology*. Boston, MA: Houghton Mifflin, 1979.
- [4] J.Daugman, "Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns", *International Journal of Computer Vision*, Vol.45(1),pp.25-38, 2001.
- [5] J.Daugman, "High Confidence Visual Recognition by a Test of Statistical Independence", *IEEE Trans.Pattern Analysis and Machine Intelligence*, Vol. 15, No.11, pp.1148-1161,1993.
- [6] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, "A Machine Vision System for Iris Recognition," *Mach. Vision App.*, vol. 9, pp.1-8, 1996
- [7] J. G. Daugman, "Complete Discrete 2-D Gabor Transforms by Neural Network for Image Analysis and Compression" *IEEE Trans. Acoust., Speech, Signal Processing*, vol. 36, pp.1169-1179, 1988.

[8] Ma., L, Y.Wang, and T.Tan, "Iris Recognition Using Circular Symmetric Filters", *Proceedings of the Sixteenth International Conference on Pattern Recognition*, vol.2, pp.414-417, 2002.

[9] Kwanghyuk B., Seungin N., and Jaihei Kim, "Iris Feature Extraction Using Independent Component Analysis", *AVBPA 2003, LNCS*, vol. 2688, pp. 838-844,2003.