Introduction

to

Biometric Technology
Chapter 1

Introduction to Biometric Technology

1.1 Introduction

Biometric technology deals with recognizing the uniqueness of individuals based on their unique physical or behavioral characteristics. Physical characteristics such as finger-print, handwriting, voice, palm print, face, retina, hand geometry and iris patterns or behavioral characteristics such as typing pattern and hand-written signature present unique information about a person and can be used in authentication applications. The developments in science and technology have made it possible to use biometric in applications where it is required to confirm the identity of individuals. Applications such as passenger control in airports, access control in restricted areas, border control, database access and financial services are some of the examples where the biometric technology has been applied for more reliable identification and verification [1].

In recent years, biometric identity cards and passports have been issued in some countries based on Iris, fingerprint, face recognition and palm print technologies to improve border control process and simplify passengers travel at the airports. In UK and Australia, biometric passports based on face recognition are being issued. The technology is designed which automatically takes a picture of the passengers and match it to the digitized image stored in the biometric passports. Recently, US government is also conducting a Registered Traveller Program which uses a combination of fingerprint and Iris recognition technology to speed up the security check process at some airports. In the field of financial services, biometric technology has shown a great potential in ordering more comfort to customers while increasing their security. For an example, banking services and payments based on biometrics are going to be much safer, faster and easier than the existing methods based on credit and debit cards. Proposed forms of payments such as pay and touch scheme based on fingerprint or smart cards with stored Iris information are on these biometric applications. Although there are still some concerns about using biometrics in the mass consumer applications due to information protection issues,
it is believed that the technology will find its way to be widely used in many different applications.

Moreover, access control applications such as database access and computer login also benefit from these biometric technologies. Compared to passwords, biometric technologies order more secure and comfortable accessibility and have dealt with problems such as forgetting or hacking passwords. For instance, the new login method based on combination of a password with its typing pattern has been an innovative proposal where knowing the password itself would not be sufficient. The method is based on typing pattern of a person by measuring the delays between the typing instances, which a behavioral characteristic is similar to hand written signature. This method has added up the security of login-based access systems where a limited number of individuals are expected to have access to the systems. Overall, the future of biometric technology is understood to be open for more investments based on the new services it has to offer to the society.

1.2 Iris Recognition System

A biometric system provides 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 available. Most commercial Iris recognition systems use patented algorithms developed by John G. Daugman, and these algorithms are able to produce perfect recognition rates. The Iris of each eye is unique, No two irises are alike in their features even between identical twins and triplets or between one's own left and right eyes.

Iris patterns are formed by combined layers of pigmented epithelial cells, muscles for controlling the pupil, stromal layer consisting of connective tissue, blood vessels and an anterior border layer. The physiological complexity of the organ results in the random patterns in Iris, which are statistically unique and suitable for biometric measurements. In addition, Iris patterns are stable over time and only minor changes happen to them throughout an individual's life [3].

It is also an internal organ, located behind the cornea and aqueous humor, and well protected from the external environment. The characteristics such as being
protected from the environment and having more reliable stability over time, compared to other popular biometrics, have well justified the ongoing research and investments on iris recognition by various researchers and industries around the world. For instance, the developed algorithm by Daugman, which is known as the state-of-the-art in the field of iris recognition, has initiated huge investments on the technology for more than a decade. IriScan Inc. patents the core technology of the Daugman's system and several companies such as IBM, Iridian Technologies, IrisGuard Inc., Securimetrics Inc. and Panasonic are active in providing iris recognition products and services.

If we focus on the history of iris recognition it goes back to the mid 19th century when the French physician, Alphonse Bertillon, studied the use of eye colour as an identifier [2]. However, it is believed that the main idea of using iris patterns for identification, the way we know it today, was first introduced by an eye surgeon, Frank Burch, in 1936. In 1987, two ophthalmologists, Flom and Sar, patented this idea and proposed it to Daugman a professor at Harvard University, to study the possibility of developing an iris recognition algorithm [17, 18]. After a few years of scientific experiments, Daugman proposed and developed a high confidence iris recognition system and published the results in 1993. A few years after the publication of the first algorithm by Daugman, other researchers developed new iris recognition algorithms. Systems presented by Wildes et al., Boles and Boashash, Tisse et al., Zhu et al., Lim et al., Noh et al., and Ma et al., are some of the well-known algorithms proposed by them so far. Among these algorithms, the works done by Lim et al. and Noh et al. are also commercialized.

The algorithms developed by Wildes and Boles are suitable for verification applications because the normalization of irises is performed in the matching process and would be very time consuming in identification applications. Although these algorithms have been successful, they still require to be improved in the accuracy and speed aspects compared to the proposed algorithm by Daugman [4].
Chapter 1 - Introduction to Biometric Technology

Segmentation Process

ROI Extracted Normalization process

Enhanced Image

Feature Extraction

Feature Process

Classifier

Matching Process

Figure 1.1: Iris Recognition System
1.2.1 Iris Recognition at a Distance

The Samoff Corporation in Princeton, New Jersey presented results from a DARPA funded program called Human ID at a Distance. The inspiration is to capture Iris data up to 30'. It is said that Iris is important due to "no false matches in 2m comparisons" and only 2% non-matches. One of the major problems with Iris is that current systems are highly constrained.

They must be at controlled distances and under special lighting. The result is that a system has limited throughput.

The test system used two lenses for two cameras which operated at 5m and 10m. IR was used for illumination at 880nm. There were 128 pixels across the diameter of the Iris. Each image was captured at 12f/s for 10 seconds. Variables in the collection included: 5 or 10m distance, angle 0 or 30 degrees, eye movement or tracking and lighting that was background or spotlight. The technique used was 97% successful, including with glasses, in locating the Iris.

1.3 Motivation Behind Study

Biometric refers to the automatic identification of an individual based on his/her physiological or behavioral attributes [1]. This identification method is preferred over traditional methods involving passwords PIN's (Personal Identification numbers) for several reasons, including person to be identified is required to be physically present at the point of identification and/or identification based on biometric techniques avoids the need to remember a password. Biometric techniques can possibly prevent unauthorized access to ATMs, Workstations, Computer Network, Bank accounts, Smart Cards etc.

PIN's and passwords may be forgotten and token based identification methods may be stolen or lost. Thus, Biometric identifications are being used for real time identification. The most popular are based on face recognition, and fingerprint matching; however, other biometric system uses iris and retinal scans and speech recognition. Biometric system is essentially for pattern recognition system that makes a personal identification by determining the authenticity of a specific attributes possessed by the user. However, this technology is very real and is
Currently being used in the private sector. One method of particular interest is the use of iris patterns to authenticate users [1].

There are a number of other factors that weigh heavily in iris recognition's favor for applications requiring large databases and real time authentication.

**Accurate:** Like a snowflake, every iris is absolutely unique. A subject's left and right iris is as different from each other as they are from any other individual's. It has been calculated that the chance of finding two randomly formed identical irises is on an almost astronomical order of 1 in $10^{78}$.

At the root of iris recognition's accuracy is the data-richness of the iris itself. The Iris Access system captures over 240 degrees of freedom or unique characteristics in formulating its algorithmic template. Fingerprints, facial recognition and hand geometry have far less detailed input in template construction. In fact, it's probably fair to say that one iris template contains more data than is collected in creating templates for a finger, a face and a hand combined. This is one reason why iris recognition can authenticate with confidence even when significantly less than the whole eye is visible.

**Stability:** Virtually every other biometric template changes significantly over time, detracting from overall system performance and requiring frequent re-enrollment. Voices change. Hands and fingers grow. The type of labor one does, even weather temperature or one's medical condition can result in template changes in other technologies. Barring trauma and certain ophthalmologic surgery, the patterns in the iris are constant from age 1 to death. (At death, iris tissue is among the most rapidly deteriorating of all body tissues, something that leads to its use by forensic pathologists in estimating time of death.)

**Fast:** No other biometric technology is designed to deliver 1-n searching of large databases in real time. A 2001 study conducted by the UK's National Physical Laboratory, found that iris technology was capable of nearly 20 times more matches per minute than its closest competitor. Looking at speed in conjunction with accuracy, there is simply no other technology that can deliver high accuracy authentication in anything close to the real-time performance of iris recognition.
Conversely, fingerprint searches are challenged by database size, adding time to searches or necessitating filtering as a search acceleration technique. Even so, fingerprint technology often returns multiple "possible matches," forcing introduction of human decision factors and increasing the potential for error in an authentication decision.

**Scalable:** Iris Recognition and the LG Iris Access 3000 are ideal for large-scale ID applications or enterprise physical security and applications characterized by large databases. As iris data templates require only 512-bytes of storage per iris, very large databases can be managed and speedily searched without degradation of performance accuracy.

**Non-Invasive:** No bright lights or lasers are used in the imaging and iris authentication process. The user can stand as far as 10" away from the unit, and even wear glasses or contact lenses without compromising system accuracy. Unlike some other popular biometrics, iris authentication involves no physical contact. Not only does this mean "no touch" authentication, it also means the technology is ideally suited for use in environments where rubber gloves or other protective gear is used. Iris recognition applications are generally opt-in—there is none of the surveillance stigma sometimes affiliated with facial recognition, which scans crowds looking for individuals. Nor is there any tie in to the large fingerprint databases maintained by law enforcement agencies, which often gives a negative stigma to finger print based systems.

### 1.4 Literature Review for Iris Recognition

J. G. Daugman (1993), "High confidence Visual Recognitions of Persons by a statistical Independence," had first proposed an algorithm for iris recognition. His algorithm is based on Iris Codes. Integro-differential operators are used to detect the inner and outer part of the iris. The image is normalization by converting it from Cartesian to polar transform and rectangular representation of the region of interest is generated which is known as rubber sheet model. For Feature extraction, Gabor wavelets algorithm was used to generate the Iris codes. Finally Hamming Distance was used for matching purpose [4].
R. P. Wildes (1994), "A system for automated iris recognition," described personnel verification based on automated iris recognition. The motivation for this endeavor stems from the observation that the human iris provides a particularly interesting structure on which to base a technology for noninvasive biometric measurement. Since the iris is an overt body its appearance is amenable to remote examination with the aid of a computer vision system. The proposed system exhibits flawless performance in the evaluation of 520 iris images [5].

J. G. Daugman and C. Downing (1994), "Recognizing iris texture by phase demodulation," Authors had described a method for rapid visual recognition of personal identity based on the failure of a statistical test of independence in which the most unique phenotypic feature visible in a person's face is the detailed texture of each eye's iris: an estimate of its statistical complexity in a sample of the human population reveals variation corresponding to several hundred independent degrees-of-freedom. Morphogenetic randomness in the texture expressed phenotypically in the iris trabecular meshwork ensures that a test of statistical independence on two coded patterns originating from different eyes is passed almost certainly, whereas the same test has failed almost certainly when the compared codes originate from the same eye [6].

J. G. Daugman (1995), "High confidence recognition of persons by rapid video analysis of iris texture," author had presented a method based on the failure of a statistical test of independence. The most unique phenotypic feature visible in a person's face is the detailed texture of each eye's iris. The visible texture of a person's iris in a real time video image is encoded into a compact sequence of multi scale quadrature 2D Gabor wavelet coefficients, whose most significant bits comprise a 256 byte "iris code." Statistical decision theory generates identification decisions by using Exclusive OR comparisons of complete iris codes at the rate of 10,000 per second, including calculation of decision confidence levels. The distributions observed empirically in such comparisons imply a theoretical "cross over" error rate of one in 131,000 this is verified by equalizing the FAR and FRR [7].

R. Herpers, et. al., (1996), "Context based detection of keypoints and features in eye regions," authors had represented facial keypoints such as eye corners as
important features for a number of different tasks in automatic face processing. Facial keypoints rather have an anatomical high-level definition than a low-level one. Therefore, they cannot be detected reliably by purely data-driven methods like corner detectors that are only based on the image data of the local neighborhood. This method integrates model knowledge to guarantee a consistent interpretation of the abundance of local features. The detection is based on a selective search and sequential tracking of edges controlled by model knowledge. For this, the edge detection has been adopted [8].

G. O. Williams (1996), “Iris Technology”, This paper states that use of the unique patterns of the human Iris, shows promise of overcoming previous shortcomings and providing positive identification of an individual without contact or invasion, at extremely high confidence levels. The video-based system locates the eye and Iris; evaluates the degree of occlusion by eyelid and spectral reflection; IriScan Inc. has been developing an identification/verification system capable of positively identifying and verifying the identity of individuals without physical contact or a person in the loop [9].

R. P. Wildes, et. al. (1997), “Iris Recognition: An Emerging Biometric Technology,” Here Authors have stated an automated iris recognition as a biometrically based technology for personal identification and verification. They have used an isotropic band-pass decomposition derived from the application of Laplacian of Gaussian filters to the image data also used the first derivative of image intensity to find the location of edges corresponding to the border of the iris (inner & outer boundaries of Iris) [10].

W. W. Boles (1997), “A security system based on human iris identification using wavelet transform.” The zero crossings of the wavelet transform are used to extract the unique features obtained from the grey level profiles of the iris. The recognition process is performed in two stages. The first stage consists of building a one dimensional representation of the grey level profiles of the iris followed by obtaining the wavelet transform zero crossings of the resulting representation. The second stage is the matching procedure for iris recognition. This approach is used only for few selected intermediate resolution levels for matching, thus making it computationally efficient as well as less sensitive to noise and quantization errors. A
normalization process is implemented to compensate for size variations due to the possible changes in the camera to face distance. This technique has been tested on real images in both noise free and noisy conditions [11].

W. W. Boles and B. Boashash (1998), "A human identification technique using images of the iris and wavelet transform," A new approach for recognizing the iris of the human eye is presented. Zero-crossings of the wavelet transform at various resolution levels are calculated over concentric circles on the Iris, and the resulting one-dimensional (1-D) signals are compared with model features using different dissimilarity functions [12].

S. Lim, et. al, (2001), "Efficient iris recognition through improvement of feature vector and classifier," This approach represents the feature extraction method where 2D Haar wavelet had used and quantized at the 4-th-level high-frequency information to form an 87-binary code length as feature vector. For classification purpose authors had applied an LVQ neural network [13].

C. Tisse, (2002), "Person identification technique using human iris recognition," exploited a scale-space filtering to extract unique features that use the direction of concavity of an image from an iris image. Local iris features provides a new concept of instantaneous-phase and/or emergent-frequency, on multi-dimensional Hilbert Transform which is 1D signal. Hamming Distance was used for Matching Purposes [14].

J. Daugman, (2002), "How iris recognition works," The principle that underlies the recognition of persons by their iris patterns is the failure of a test of statistical Independence on texture phase structure as encoded by multi-scale, quadrature wavelets [17].

Li Ma, et. al, (2002), "Personal Identification Based on Iris Texture Analysis," authors have used Spatial Gabor Filters and also Multichannel Gabor filtering for capturing Iris local features for extracting Iris features whose feature vector length 1536. Fisher linear discriminant is first used to reduce the dimensionality of the feature vector. Then the nearest centre classifier is adopted for iris classification [15, 16].

A. Poursaber and B. N. Araabi (2006), "Iris Recognition for Partially Occluded Images Methodology and Sensitivity Analysis," authors have introduced two
different segmentations of iris. The first algorithm, a circle is located around the pupil with an appropriate diameter. The iris area encircled by the circular boundary is used for recognition purposes. The second method, again a circle is located around the pupil with a larger diameter. However, only the lower part of the encircled iris area is utilized for individual recognition. Wavelet-based texture features are used in the process. Hamming and harmonic mean distance classifiers are exploited as a mixed classifier [20].

J. Daugman (2007), "New Methods in Iris Recognition," had proposed more disciplined methods for detecting and faithfully modeling the iris inner and outer boundaries with active contours, leading to more flexible embedded coordinate systems. Fourier-based methods were used for solving the problems in iris trigonometry and projective geometry, allowing off-axis gaze to be handled by detecting it and the eye into orthographic perspective. Statistical inference methods are used for detecting and excluding eyelashes; Exploration of score normalizations, depending on the amount of iris data that is available in images and the required scale of database search [21].

Labati, R. D. Piuri, V. Scotti, F. (2009), "Neural-based Iterative Approach for Iris Detection in Iris recognition systems," the proposed algorithm starts by an initial random point in the input image, then it processes a set of local image properties in a circular region of interest searching for the peculiar transition patterns of the iris boundaries. A trained neural network processes the parameters associated to the extracted boundaries and it estimates the offsets in the vertical and horizontal axis with respect to the estimated centre. The coordinates of the starting point are then updated with the processed offsets. The steps are repeated for a fixed number of times, which yields iterative refinements of the coordinates of the pupils center and its boundaries [22].

Lin Zhonghua Lu Bibo (2010), "Iris Recognition Method Based on the Coefficients of Morlet Wavelet Transform," authors had represented an iris recognition method based on the coefficients of Morlet wavelet transform. Firstly, it locates the iris, then makes normalization to the iris image and gets 512 columns multiplying 64 rows rectangular iris image, ensures the effective iris area. Secondly, it makes one dimension Morlet wavelet transform row by row to the iris image in the effective iris
area, gets a series of coefficients of wavelet transform at different scales and gets the distribution figure of these coefficients of different scales. Thirdly, it makes binary codes to the iris image according to the coefficients of different scales and figures the iris pattern by iris codes. At last, it sorts out the different iris patterns by pattern matching method and gives the recognition results to 99.94% [23].

N. Popescu-Bodorin (2010), "Exploring New Directions in Iris Recognition," author had proposed an approach for iris recognition based on Circular Fuzzy Iris Segmentation (CFIS), and Gabor Analytic Iris Texture Binary Encoder (GAITBE) is proposed and tested here. CFIS procedure is designed to guarantee that similar iris segments will be obtained for similar eye images, despite the fact that the degree of occlusion may vary from one image to another. The result is a circle on iris part, which approximates the actual iris. GAITBE proves better encoding of statistical independence between the iris codes extracted from different irides using Hilbert Transform. Irides from University of Bath Iris Database has been used for binary encoded on two different lengths (768 / 192 bytes) and which is tested in both single-enrollment and multi-enrollment identification scenarios [24].

1.5 Statement of Problem

Iris recognition today combines technologies from several fields including computer vision (CV), pattern recognition, statistical inference and optics. The goal of the technology is bear instant, highly accurate recognition of a person’s identity based on digitally represented image of the scanned eye. It is based upon the fact that no two iris patterns are alike. Iris can therefore serve as a lifelong password which the person must have never to remember. Many Researchers have contributed their work for Iris recognition, such as Algorithms on finding the inner and outer boundaries of Iris (i.e. Iris Localization), Iris Segmentation and Feature extraction Process also on Recognition algorithms.

The study discusses the current methods on locating the pupil and limbus (inner and outer boundaries) assuming that the boundaries are detected correctly. Iris images from the CASIA database are used for this purpose. In addition to this, near-infrared images provided by the Institute of Automation, Chinese Academy of
Chapter 1 - Introduction to Biometric Technology

Sciences (CASIA), the limbus boundaries have insufficient contrast and global search techniques such as the Integro-differential operator are more proper for the extracting the ROI [3].

The main aim and concentration of our problem is to study existing fuzzy neural architectures for the iris recognition and to propose new architectures. Iris recognition as a biometric technology has great advantages as stated above. Further, fuzzy neural networks provides many benefits such as soft decision, nonlinear separability, training time, online learning, adaptability, generalization ability.

1.6 Problem Formulation

Hence, we feel Fuzzy Neural Networks approach for Iris recognition shall yield better results. In this proposed work the human iris recognition process will be divided into following four steps:

Localization: Inner and outer boundaries of the iris are extracted

Normalization: Iris of different people may be of different size. For the same person the size may vary because of changes in illumination and other factors. So normalization is performed to get all the images in a standard form suitable processing.

Feature extraction: Iris provides abundant texture information, a feature vector is formed which consists of the ordered sequence of features extracted from the various representations of the iris images

Fuzzy Neural Classification: Feature vectors are classified through different fuzzy neural architectures.

1.7 Organization of the Thesis

The objective of this work was to study some of the existing fuzzy neural networks and to propose architectures that can be used in pattern recognition problems. The problem chosen is Iris recognition. It is one of the biometric applications for authentication in security systems.
Chapter 1 - Introduction to Biometric Technology

Thesis consists of seven chapters and describes three fuzzy neural network models. In this first chapter the study represents the introduction about biometric technology, and significance of iris recognition.

Second chapter describes Iris segmentation and Normalization Methods of Daugman. It is significantly important in all iris recognition systems proper detection of Iris and pupil boundaries of iris texture which is significantly important in all iris recognition systems.

Third chapter focuses on feature extraction and ANN approach for Iris Images. A feature extraction is done by using Gabor filters and Principal Component Analysis. The ANN approach is discussed for Iris pattern classification. Artificial Neural Network approach for Iris Classification. The objective of ANN learning rule depends upon the applications. For example, the objective in pattern recognition is to classify sample data and predict successfully on new data. In pattern recognition, each cycle of presentation of all sample patterns is usually referred as learning epoch.

Fourth chapter describes This work is an application of Patrick Simpson's fuzzy min-max neural network (FMMN) Classification. It describes the fuzzy min-max classifier neural network implementation. It outlines the learning and recall algorithms and also demonstrates the efficiency of this neural network classifier.

Fifth chapter have projected on MFHSSN classifier with its learning algorithm, which utilizes fuzzy sets as pattern classes in which each fuzzy set is an union of fuzzy set hyperspheres. The fuzzy set hypersphere is an n-dimensional hypersphere defined by a center point and radius, which is characterized by hypersphere membership function.

Sixth Chapter discuss proposed MFHLSNN for Iris recognition The MFHLSNN utilizes fuzzy sets as pattern classes in which each fuzzy set is an union of fuzzy set hyperline segments. The fuzzy set hyperline segment is an n-dimensional hyperline segment defined by two end points with a corresponding membership function. The performance of MFHLSNN algorithm is compared with the other distance measure of FHLSNN algorithms.
1.8. Summary

Biometric refers to the automatic identification of an individual based on his/her physiological or behavioral attributes. This identification method is preferred over traditional methods involving passwords PIN’s (Personal Identification numbers) for several reasons, including person to be identified is required to be physically present at the point of identification and/or identification based on biometric techniques avoids the need to remember a password. Biometric techniques can possibly prevent unauthorized access to ATMs, Workstations, Computer Network, Bank accounts, Smart Cards etc. Iris as a biometric feature, it is found to be the most reliable and accurate for authentication process available today. While most biometric have 13 to 60 distinct characteristics, the iris is said to have 266 unique spots. A biometric system provides 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 available.

There are a number of other factors weigh heavily in iris recognition’s favor for applications requiring large database and real time authentication such as Stable, accurate, stability, fast, scalable and noninvasive.

At the root of iris recognition's accuracy is the data-richness of the iris itself. The Iris Access system captures over 240 degrees of freedom or unique characteristics in formulating its algorithmic template. Fingerprints, facial recognition and hand geometry have far less detailed input in template construction. In fact, it's probably fair to say that one iris template contains more data than is collected in creating templates for a finger, a face and a hand combined. This is one reason why iris recognition can authenticate with confidence even when significantly less than the whole eye is visible.
References


