Chapter 2

BIOMETRICS
2 BIOMETRICS

In this chapter we introduce the basic concepts & definitions related with biometrics, modes of functioning and a possible classification. We compare the most common biometric traits and some measures of the biometrics effectiveness are given.

For iris recognition, we overview the anatomy of the human eye and review the biometric iris recognition state-of-the-art, with particular emphasis to three iris recognition modes, considered relevant and representative of the majority of the proposals. Further, we discuss advantages & disadvantages & process of the iris recognition.

Searching for a definition of biometrics in both specialized and general information sources, leads to several variants, among which are

- The study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.
- A method of verifying an individuals identity based on measurements of the individuals physical features or repeatable actions where those features and/or actions are both unique to that individual and measurable.
- Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes [31].
- Biometrics is the science of measuring physical properties of living beings using suitable body characteristics.
- Any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual [32].
From our viewpoint, biometrics can be regarded as the automated measurement and enumeration of biological characteristics, in order to obtain a plausible quantitative value that, with high confidence, can distinguish between individuals.

2.1 Modes of Recognition Process

A recognition process consists of the following modes,

- In the **enrollment mode**, a user's biometric data is acquired using a biometric read and stored in a database. The stored biometric template is labeled with a user identity to facilitate authentication.

- In the **authentication mode**, involves comparing the acquired biometric information with only those templates corresponding to the claimed identity.

- In the **identification mode**, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database).

2.2 Classification of Biometric Systems

Biometric systems can be classified according to six perspectives[33] as a function of the characteristics of the recognition procedure itself:

**Overt / covert**: If the user is aware about the acquisition of his biometric data, the application is defined as overt; otherwise, is defined as covert. This is clearly one of the most concerning characteristics of a biometric system, regarding the privacy issue.

**Habituated / non-habituated**: When the majority of the people that interacts with the biometric system are every-day users, the recognition is performed
in the habituated mode. If the average frequency of use from each user is low, the recognition is performed in the non-habituated mode. This is relevant to the degree of cooperation and training demanded from the users.

**Attended / non-attended**: If the user is observed and guided by supervisors during the process, the biometric recognition is performed attended; if not, the use is considered non-attended. Obviously, the ease-of-use of the recognition system is much more relevant in the non-attended mode.

**Standard / non-standard environment**: When all the conditions can be controlled and the recognition takes place indoors within constrained conditions, it is considered that the recognition is performed within a standard environment; if not, the use is called in non-standard environment.

**Public / private**: If the users are not employees of the organization that owns the recognition system, the application is public; if the users are employees, the application is called private.

**Open / closed**: If the system uses completely proprietary formats, the application is considered closed. Otherwise, when the system is able to exchange data with others, it is called open and, once again, privacy and legal issues should be addressed.

### 2.3 Biometric Traits

This section describes the most common traits that are presently used for biometric purposes. Although there is some discussion about the potential use of other traits as biometric basis, the presented traits are those with higher acceptability by the research community and have commercial applications based in it, which increases its credibility in the biometric compass.
DNA

The deoxyribonucleic acid (DNA) is represented through a one-dimensional code, unique for each person. The only exceptions are identical twins, which can represent a serious problem, regarding security and forensic applications[34]. DNA identification is based on techniques that use the non-coding tandemly repetitive DNA regions. Humans have 23 pairs of chromosomes containing their DNA blueprint. One member of each chromosomal pair comes from the mother; the other comes from the father. Every cell in a human body contains a copy of this DNA. The large majority of DNA does not differ from person to person, but 0.10 % of a persons entire genome would be unique to each individual, which represents 3 million base pairs of DNA. This method is considered to have some drawbacks, as the easy contamination and sensitivity, the impossibility to perform real-time recognition and severe privacy issues, due to the fact of the DNA can reveal susceptibility to some diseases. Due to many distinguishable characteristics between the DNA and the remaining biometric traits, the discussion about its inclusion as a biometric trait subsists.

Face

The importance of facial features for human recognition cannot be overstated. Facial images are the most common biometric characteristic used by humans to perform personal recognition. This is a non intrusive and suitable trait to perform covert recognition. Three types of feature extraction methods can be distinguished: generic methods based on edges, lines, and curves; feature-template-based methods that are used to detect facial features[35] such as eyes and structural matching methods that take into consideration geometrical constraints on the features. Although performance of commercially available systems is reasonable, there is still significant room for improvement, since false rejection rate is about 10 % and the false accept rate is about
These systems face strong difficulties when the faces are captured under different angles and uncontrolled ambient illumination. Moreover, it is still questioned if a face itself is sufficient basis for reliably recognition of a subject, as, for instance, twins have very similar faces. Another problem could be with counterfeit, as users can dramatically change the appearance of their face, through decorative objects or even through plastic surgeries. As main advantages, it must be enhanced the high acceptability and universality of face recognition. Users perceive the recognition system as an automated mechanism that exclusively performs a trivial task.

**Fingerprint**

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy is acceptable. In the past, patterns were extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. The recognition process starts by capturing the finger image by direct contact with a reader device that can also perform some validation procedures to avoid counterfeit measures (check of temperature and pulse). The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as by the minutiae points. These are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The feature values typically correspond to the position and orientation of certain critical points, known as minutiae points. The matching process involves comparing the two-dimensional minutiae sample and template patterns. Among the main advantages for the use of fingerprints are the higher levels of acceptability and their easy of use, as well the fact that it is a matured technology with several years of proven effectiveness. Also, the fact that its technology is legally accepted and that millions of enrolled fingerprints exist, are important. As disadvantages, it is considered vulnerable to noise and distortion brought on by dirt and twists. Also, since physical
contact between the finger and the scanning device is required, the surface can become oily and cloudy after repeated use and reduce the sensitivity. Hygienic considerations must be considered too.

**Keystroke**

It is believed that each person types on a keyboard in a distinguishable way, such that the analysis of the different rhythms that a subject types in the keyboard can be used for its recognition. This technology examines either dynamics as speed and pressure, the length of time each key is held down, the time elapsed between hitting certain keys and the tendencies to switch between a numeric keypad and keyboard numbers. The extracted features are statistical in nature and specifically designed to characterize the keystroke dynamics over writing samples of 200 or more characters. Most of these are averages and standard deviations of key press duration times and of transition times between keystroke pairs, such as digraphs[37]. The main advantage of the use of keystroke-based biometrics is its potential for continuous monitoring[32]. As opposed to other traits, the keystroke information can be continuously analyzed by the recognition system, decreasing the probability of active counterfeit measures. Moreover, since users are accustomed to authenticating themselves through user names and password, most keystroke biometric methods are completely transparent and are well accepted by users. Among potential disadvantages, privacy concerns must be considered, as the way a subject strokes can be used to infer information about its potential rent ability and work effectiveness, for instance[38].

**Hand Geometry**

Hand geometry for biometric purposes is used since the early 1980s. Since hand geometry is not thought to be as unique as other biometric traits, its use is often related with low security applications and, sometimes, associated with other security
procedures. A variety of measurements of the human hand, including its shape and lengths and widths of the fingers, can be used as biometric characteristics. Feature extraction computes the widths and lengths of the fingers at various locations of the captured image. These metrics define the feature vector of the user's hand. Current research work seeks for new features that could increment the discriminant capacity between different hands, as well the design of a deformable model for the hand, in order to increase robustness. As main advantages, it can be referred that the hand geometry-based biometric systems are easy to use and inexpensive. Additionally, operational environmental factors such as dry weather, or individual anomalies such as dry skin, generally have no negative effects on identification accuracy [39]. However, it should be stressed that its main disadvantage is its relative low discriminating capacity. Also, the hand geometry may not be invariant over the lifespan of an individual, especially during childhood. In addition, an individual's jewelry or limitations in dexterity (e.g., arthritis), may pose further challenges in extracting the correct hand geometry information. Finally, the relative large dimensions of the subject's hands and the requirement of contact to perform recognition makes it unappropiated for certain applications (e.g., laptop computers access).

Hand Vein

It is believed that the pattern of blood veins is unique to every individual, even among identical twins. Moreover, palms have a broad and complicated vascular pattern that has minor variations over lifetime and is not considered intrusive. An individual's vein pattern image is captured by radiating his/her hand with near infrared light. The reflection method illuminates the palm and captures the light given off by the region after diffusion through the palm. The deoxygenated hemoglobin in the vein vessels absorbs the infrared ray, thereby reducing the reflection rate and causing the veins to appear as a black pattern. This vein pattern is then verified against a pre-registered
pattern to authenticate the individual. As veins are internal and have a wealth of differentiating features, attempts to forge an identity are extremely difficult, thereby enabling a high level of security. In addition, the sensor of the palm vein device can only recognize the pattern if the deoxidized hemoglobin is actively flowing within the individual’s veins, which increases the counterfeit difficulty. The main disadvantage of this biometric is requirement of high level of co-operation from the subject and direct physical contact between the subject and some part of the system. Apart from the deterioration in the accuracy, this fact is considered an hygienic concern.

Palm print

Similarly to the widely used fingerprints, the palms of the human hands contain unique patterns of ridges and valleys. Since a palm is larger than a finger, a palm print is expected to be even more distinguishable than a fingerprint. Palm print scanners need to capture a larger area with similar quality as fingerprint scanners, which make them more expensive. Typically, the analysis of the palms principal lines, wrinkles, and textures is performed. These line structures are stable over the human lifetime and normally people do not feel uneasy to have their palm print images captured. Therefore, palm print recognition offers promising future for medium-security access control system. Although this is not as stabilized and matured as the fingerprint technology, several research studies have been made with the purpose of extracting higher discriminating features from the palm print information. Presently, there are two popular approaches to palm print recognition. One transforms palm print images into specific transformation domains and apply texture-based analysis methods (Gabor filters, wavelets decompositions). The other approach applies a technology close to the one used for fingerprint: extract the main lines and creases from the palm and further perform the comparison between the minutia information (e.g., through graph matching).
Compared to other biometric traits, the facts that a higher level of cooperation is demanded to users and the required physical contact between the users and the capturing device should be regarded as disadvantages. Also, the fact that the human hand is a fundamental tool for the majority of the people increases the probability of physical damages or diseases.

Signature

Signature can be regarded as unique and results from both behavioral and hand geometry variations associated to each subject. The way a person signs his or her name is known to be characteristic of that individual since centuries, although the analysis of the signature dynamics is recent. There are two major strategies to perform signature recognition: image-based and dynamics analysis. The first approach is the most classical and is based on the visual appearance of the signature. The latter analyzes both speed, direction and pressure of writing, stroke order and its major weak point results of the specific hardware dependence\cite{40} This metric has, at least, three advantages over other biometric techniques: it is a socially well accepted identification method already in use in bank and credit card transactions, most of the new generation of portable computers and personal digital assistants use handwriting as main input channel and, as opposed to finger, iris or retina patterns, a signature may be changed by the user, similarly to a password. However, the use of signature-based biometrics has several weaknesses. Individuals with muscular illnesses and people who sometimes sign with only their initials might result in high false rejection rates. Often, signatures dramatically change over a period of time and are influenced by physical and emotional conditions of the subjects. Additionally, since many users are unaccustomed to signing on a tablet, some subjects signatures may differ from their signatures with ink and paper, increasing the potential for false rejection.
**Retina**

Retinal scan measures the blood vessel patterns in the back of the eye. The pattern formed by veins beneath the retinal surface in an eye is stable and unique and is, therefore, feasible for recognition. Digital images of retinal patterns can be acquired by projecting a low intensity beam of visual or infrared light into the eye and capturing an image of the retina using optics similar to a retinoscope. The fact that the retina is small, internal, and difficult to measure makes the capturing of its image more difficult and demands higher efforts from the users than most of the other traits. Retina matching is accomplished either through 2D or 3D image processing techniques. Retina information procedures usually apply edge enhancing techniques and vessel crossings localization[41-42]. Other techniques rely on the identification of vessels using adaptive thresholding techniques, followed by graph-matching techniques that find the best match between the vessels localization. Since it is protected in the eye itself, and is not easy to change or replicate the retinal vasculature, this is considered as one of the most secure biometric traits. Retina based systems are used for high security applications, as the access to prisons. Oppositely, because users perceive the technology as intrusive, unfriendly and with high cooperative demands, this type of biometric trait has not gained high popularity. Also, it is accepted that retinal vasculature can reveal some medical conditions (e.g., hypertension or diabetes), which is another factor deterring the public acceptance of retinal scan-based biometrics. The cost of this biometric system is also prohibitive.

**Iris**

The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eighth month. It is the annular region of the eye bounded by the pupil and the sclera (white part of the eye) on either side.
Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette[43]. Each iris is unique and even irises of identical twins are different. Furthermore, the iris is more easily imaged than retina; it is extremely difficult to surgically tamper iris texture information and it is possible to detect artificial irises. Although the early iris based identification systems required considerable user participation and were expensive, efforts are underway to build more user-friendly and cost-effective versions. To obtain a good image of the iris, identification systems typically illuminate the iris with near-infrared light, which can be observed by most cameras yet is not detectable by humans. Among potential disadvantages for its use remains the weak public acceptance of the iris imaging for biometric purposes, due to old-fashioned thoughts about iridology. The available results of both accuracy and speed of iris-based identification are highly encouraging and point to the feasibility of large-scale recognition using iris information. Due to this and to the above described characteristics, it is common to consider iris as one of the best biometric traits, although this evaluation is dependent of the specific purpose.

2.4 Characteristics of a Biometric

The **Uniqueness**, often designated as accuracy, distinctiveness or singleness, is probably the most relevant characteristic of a biometric trait. It measures the degree of dissimilarity of the trait between individuals and its capacity of being separable. This feature strongly determines the probability of false acceptances by the system.

**Universality** measures the scope of the trait, the number of people where it occurs. Obviously, the optimal biometric trait should occur in as many people as possible. Permanence is the quality of being immutable over time, measuring the probability of the biometric trait suffering significant changes over lifetime. This parameter
has strong impact in the false rejection rates of the system.

**Collectability or Measurability** is the characteristic that expresses the technical and human easiness in the capture of the relevant trait information. This value plays a role in the users comfort, which can easily dictate between the biometric system adoption or rejection.

The **Performance** as to do with the time required to perform the biometric recognition, once the data is captured. It is relevant in order to distinguish between the computational requirements of the recognition process. Acceptability or intrusiveness is a measure related with socio-cultural users concerns, as well as with privacy concerns associated with the data capturing.

Finally, the **Circumvention** measures how easy it is to counterfeit the system, which has high relevance in the security compass.

### 2.5 Iris Recognition

This section is totally related with the utilization of the iris for biometric purposes. And overall description of the eyes anatomy followed by the identification of the most important regions of the human iris. Iris recognition refers to identifying people by analyzing patterns of their irises. The human eye anatomy[44], followed by a highly detailed description of the iris, which is the most relevant part of the eye for the purposes of our work.

#### 2.5.1 Eye Anatomy

As with the majority of the mammals, the eye is roughly globular in shape and hollow and can be divided into two main segments - anterior and posterior - which are surrounded by a leathery envelope that acts as a protection: the sclera.
is a tough and fibrous tissue consisting of highly compacted and interweaved fibers and bands. When seen from the front, sclera is commonly, and incorrectly, referred to as the white of the eye. Regarding the anterior eye segment, it extends internally from the anterior hyaloid face forward and is externally demarcated by the limbus. It includes the structures in front of the vitreous humor: the cornea, iris, ciliary body and lens. The cornea acts as a window at the front of the eye and provides about 85% of the focusing power of the eye. It is made up of a tissue similar to that of sclera, with the relevant exception of having no blood vessels. Just beneath the cornea is a fluid-filled space called the anterior chamber, which bathes the whole of the anterior segment providing nourishment and removal products to the lens and cornea. The ciliary body is the source of the above mentioned fluid and houses the muscular fibers that enable the eye to focus. Overlying the lens, there is a structure with an opening in the whole: the iris. It is made of an elastic tissue and its function is to control the amount of light that enters the iris whole: the pupil. Behind the iris is the lens, which role consists in assuring that the light rays some to a sharp focus on the retina. The posterior eye segment comprises the back two-thirds of the eye and includes the vitreous humor, retina, choroid and optic nerve. The first is the the clear aqueous solution that fills the space between the lens and the retina, which is a thin layer of nervous tissue - supplied with oxygen and cleaned by the choroid - that is responsible for gathering the light and perform its conversion to the electrical signals that are sent through the optic nerve to the brain. This process gives us the sense of light and the ability to see and interpret shapes, colors and dimensions.

2.5.2 Iris Anatomy

The iris consists of a pigmented fibrovascular tissue, known as stroma. The stroma connects a sphincter muscle (with the purpose of contract the pupil) and a set
of dilator muscles to open it. It is divided into two major regions: the pupillary and the ciliary zone. The pupillary zone is the inner portion of the iris whose edges form the pupillary iris border. The ciliary zone is the outer portion of the iris, which extends itself into the iris origin in the ciliary body. The region that separates the pupillary and sclerotic portions is designated as the collarette. This is typically the region where the sphincter and dilator muscles overlap. The iris begins to form during the third month of gestation and the structure is complete by the eight month, although pigmentation continues into the first year after birth. The visible features of the iris arise in the trabeculum, which is a mesh work of connective tissues with arching ligaments, crypts, contraction furrows, a corona and pupillary frill, coloration and freckles. Although the anterior layer covering the trabecular framework creates the predominant iris texture seen with visible light, additional discriminating information can be given by the location of all of these sources of radial and angular variation. The average diameter of the iris is approximately 12 mm with an average thickness around 5 mm, and the pupil size can vary form 10% to 80% of the Iris diameter.
Due to the iris pattern uniqueness, iris recognition is considered to be one of the most accurate biometric technologies. A number of other characteristics make it even more attractive for recognition systems:

- External visibility. Under normal conditions, the iris is a visible organ of the human body. Therefore, taking pictures of it is easy and does not raise ethical concerns. Moreover, irises may be used for surveillance purposes when advanced technologies are involved to acquire high-resolution images from a distance.

- Natural protection. Eyes have a natural protection mechanism in the form of eyelids and tears that prevent this fragile organ from being damaged and keep it in a proper condition. Thus, at the moment of sample acquisition, condition related problems rarely occur. Eye irritations, caused by allergies and fatigue, normally do not worsen recognition, since they affect sclera only.

- Stability over long periods of time. It is clinically observed that irises do not change significantly over time. This characteristic is particularly important.
for person identification because it allows recognizing an individual, who was once enrolled in the system, at any moment of their life. As an illustration, we can mention a famous story of an Afghan girl who was identified by comparing irises from her two photographs - one taken in 1984.

2.6 Advantages & Disadvantages of Iris Recognition.

The technology of Iris recognition has some advantages and disadvantages which make it appropriate to used in some applications and not to other applications. The advantages are :

1. Iris is very accurate biometric. It has low False Accepts (FA), which is an important security aspect. Therefore iris might be a good biometric for identification applications.

2. The sensing of the biometric is without physical contact and it is convenient for the users because the iris pattern acquisition process uses unnoticeable and distant cameras.

3. Iris technology has received little negative press and so is more generally accepted biometric identifier.

On the other hand, Iris technology has some disadvantages which should be considered :

1. The iris is small, so sampling the iris pattern requires expensive input devices.

2. The performance of the iris authentication may be distorted by glasses, sunglasses or hard-contact lenses.

3. Some people are missing one or both their eyes.

4. There are few legacy iris databases and the legacy infrastructure does not exist. That makes iris technology expensive to create an iris ID system.
2.7 Iris Recognition Process

A Figure 2.3 summarizes the steps to be followed when doing iris recognition.

*Figure 2.3 – An Efficient Algorithm for Iris Recognition Process*

*Step 1*: Image acquisition, the first phase, is one of the major challenges of automated iris recognition since we need to capture a high-quality image of the iris while remaining noninvasive to the human operator.

*Step 2*: Iris localization takes place to detect the edge of the iris as well as that of the pupil; thus extracting the iris region.

*Step 3*: Image Enhancement is used to be able to transform the iris region to have fixed dimensions, and hence removing the dimensional inconsistencies between eye images due to the stretching of the iris caused by the pupil dilation from varying levels of illumination. The normalized iris region is unwrapped into a rectangular region.
Finally, it is time to extract the most discriminating feature in the iris pattern so that a comparison between templates can be done. Therefore, the obtained iris region is encoded using wavelets to construct the iris code.

As a result, a decision can be made in the matching step.

2.8 Iris Image Databases

In this section we describe the main characteristics of the public and freely available iris image databases for biometrics purposes. Through examples, we illustrate the types of noise that images from each database contain. Based on the analysis of these noise factors, we present the main motivations that led to the construction of CASIA (I, II, III), MMU, and UPOL database and highlight the main distinguishable factors in the comparison with the remaining ones. Further, we detail the optical framework used in both image capturing sessions of the CASIA (I, II,III), MMU, and UPOL database and briefly present some statistics about its images.

2.8.1 Public & Free Databases

The biometrics research and development demands the analysis of human data. Obviously, it is unrealistic to perform the test of algorithms in data captured on-the-fly, due to the enormous uneasiness that this would imply. Moreover, the fair comparison between recognition methods demands similar input data to valorize and contextualize their results. Therefore, when it comes to the test of recognition methods, standard biometric databases assume high relevance and become indispensable to the development process. In the following subsections we describe the main characteristics of their images and the analysis of the noise factors that each database contains. We considered the analysis of these noise factors and the heterogeneity of images as the most important parameters, concerning the terms and purposes of our work. Through
illustration, we exemplify some of the most common types of noise that each database contains.

### 2.8.2 CASIA Database

Iris recognition has been an active research topic of the Institute of Automation from the Chinese Academy of Sciences [45]. Having concluded about a lack of iris data for algorithm testing, they developed the CASIA image database. Apart from being the oldest, this database is clearly the most known and widely used by the majority of the researchers. CASIA iris image database (version 1.0) includes 756 iris images from 108 eyes, hence 108 classes. For each eye, 7 images are captured in two sessions, where three samples are collected in the first and four in the second session.

For version 2.0 which includes 1330 iris images form 70 eyes, 19 images are captured with different sessions, similarly to the above described database. Its images were captured within an highly constrained capturing environment, which conditioned the characteristics of the resultant images. They present very close and homogeneous characteristics and their noise factors are exclusively related with iris obstructions by eyelids and eyelashes. Moreover, the post process of the images filled the pupil regions with black pixels, which some authors used to facilitate the segmentation task. From our viewpoint, this significantly decreased the utility of the database in the evaluation of robust iris recognition methods.

CASIA-IrisV3 includes three subsets which are labeled as CASIA-IrisV3-Interval, CASIA-IrisV3-Lamp, CASIA-IrisV3-Twins. CASIA-IrisV3 contains a total of 22,035 iris images from more than 700 subjects. All iris images are 8 bit gray-level JPEG files, collected under near infrared illumination. Almost all subjects are Chinese except a few in CASIA-IrisV3-Interval. Because the three data sets were collected in different times, only CASIA-IrisV3-Interval and CASIA-IrisV3-Lamp have a small overlap in
Figure 2.4 – Examples of CASIA Iris Database Version I, II, III

subjects. CASIA-Iris-Syn contains 10,000 synthesized iris images of 1,000 classes and the intra-class variations introduced into the synthesized iris dataset include deformation, blurring, and rotation, which raise a challenge problem for iris feature representation and matching.

2.8.3 MMU Database

The Multimedia University[46] has developed a small data set of 450 iris images (MMU). They were captured through one of the most common iris recognition cameras presently functioning (LG IrisAccessR 2200). This is a semi-automated camera that operates at the range of 7-25 cm. The iris images are from 100 volunteers with different...
ages and nationalities. They come from Asia, Middle East, Africa and Europe and each of them contributed with five iris images from each eye. Obviously, the images are highly homogeneous and their noise factors are exclusively related with small iris obstructions by eyelids and eyelashes.

![Iris Images From The MMU Database](image)

**Figure 2.5 – Examples of Iris Images From The MMU Database**

### 2.8.4 UPOL Database

The UPOL iris image database was built within the University of Palackeho and Olomouc[47]. Its images have the singularity of being captured through an optometric framework (TOPCON TRC50IA) and, due to this, are of extremely high quality and suitable for the evaluation of iris recognition in completely noise-free environments. The database contains 384 images extracted from both eyes of 64 subjects (three images per eye). As Figure 2.6 illustrates, its images have maximum homogeneity and inclusively the iris segmentation is facilitated by the dark circle that surrounds the region corresponding to the iris. Obviously, these characteristics make this database the less appropriate for the non-cooperative iris recognition research.
Table 2.1 – Iris Image Database

<table>
<thead>
<tr>
<th>Sl.No</th>
<th>Image database</th>
<th>Image Size</th>
<th>No of Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CASIA I</td>
<td>320x280</td>
<td>756</td>
</tr>
<tr>
<td>2</td>
<td>CASIA II</td>
<td>640x480</td>
<td>1330</td>
</tr>
<tr>
<td>3</td>
<td>CASIA III</td>
<td>320x280 640x480</td>
<td>32,035</td>
</tr>
<tr>
<td>4</td>
<td>MMU</td>
<td>320x240</td>
<td>450</td>
</tr>
<tr>
<td>5</td>
<td>UPOL</td>
<td>768x576</td>
<td>756</td>
</tr>
</tbody>
</table>
2.9 Types of Noise in Iris Images

After studying the above described iris databases, we concluded that, the iris database CASIA Ver II, Ver III, and MMU iris database is suitable for the evaluation of robust iris recognition methods, that can overcome Specular and light reflections, and disturbing features like eyelids and eyelashes. We tried to minimize all the possible noise factors. The observations of the available iris image database and in our experimental imaging process, identified and considered the following factors as noise.

2.9.1 Iris Distributing Feature by Eyelids and Eyelashes

The biological function and natural eyelid movement can obstruct relevant portions of the iris, specially in its vertical extremes as illustrated in Figure 2.7. Noise regions are one of the largest and appear in the lower regions of the segmented and normalized iris images. Eyelashes can obstruct portions of the iris in two distinct forms as they appear isolated or grouped. The existence of multiple eyelashes in the iris regions generates a uniform darker region.

![Figure 2.7 - Noisy Iris Image Due to Eyelids and Eyelashes Obstructions](image)

2.9.2 Lighting Reflections

This type of noise corresponds to reflections from artificial light sources near to the subject, although they can appear in the image capturing within natural lighting
environments. These reflections have high heterogeneity, as they can appear with a broad range of dimensions and localized in distinct regions of the iris.

2.9.3 Specular Reflections

This type of reflections corresponds to reflected information from the environment where the user is located or is looking at. These reflections can obstruct large regions, or even the majority, of the iris. Commonly, they have lower intensity values than the lighting reflections and can correspond to a wide range of objects that the user is surrounded by.

2.9.4 Poor Focused Iris Images

Small deviations (centimeters) in the image capturing distance can propitiate the existence of images with severe focus problems that, almost invariably, lead to the increment of the false rejection rates. A poor focused image is illustrated Figure 2.10.
2.9.5 Partial Captured Irises

The image capturing from a longer distance and with subjects head and body movements results in close-up eye images failing to contain exclusively portions of the iris. Depending on the amount of information missing, this can be obviously a relevant obstacle to biometric recognition, which is illustrated by Figure 2.11.

2.9.6 Off-Angle Iris

Due to rotation of the subjects head and eyes, it is possible to capture iris images with the iris not aligned with the imaging direction, as exemplified by Figure 2.12. These off-angle images have elliptical shape for the region corresponding to the iris.
2.10 Performance of Iris

The performance of biometric identifier is measurable by two rates: False Accept rate and False Reject rate. These two rates show how much secure and efficient is a biometric identification system.

**False Accept (FA):** Deciding that a (claimed) identity is a legitimate one while in reality it is an imposter; deciding 'A' when 'B' is true. The frequency at which False Accept errors are made is called the False Accept Rate (FAR).

**False Reject (FR):** Deciding that a (claimed) identity is not legitimate when in reality the person is genuine; deciding 'B' when 'A' is true. The frequency at which False Rejects occur is called the False Reject Rate (FRR). These two rates are proportional to each other. For example, when the FA rate is high (FR is low) for a biometric system, this results in security breaches with an unauthorized person granted access. When the FR rate is high (FA is low) results convenience problems because genuinely enrolled identities are denied access. The worst case error rates for iris are; FRR: 2 error in 100 (2%) and FAR \( \geq 10^{-5} \) errors (0.0001%). Therefore, and due to its unique and rich properties, iris recognition comes to be the leading biometric identification technology for personal identification.

Figure 2.12 – Off-angle Iris images
<table>
<thead>
<tr>
<th>Algorithms</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avila</td>
<td>0.0300%</td>
<td>2.0800%</td>
</tr>
<tr>
<td>Ma</td>
<td>0.0200%</td>
<td>1.9800%</td>
</tr>
<tr>
<td>Tissue</td>
<td>1.8400%</td>
<td>8.7900%</td>
</tr>
<tr>
<td>Daugman</td>
<td>0.0100%</td>
<td>0.0900%</td>
</tr>
<tr>
<td>Cui</td>
<td>1.2000%</td>
<td>31.500%</td>
</tr>
<tr>
<td>Maheshwari</td>
<td>0.0100%</td>
<td>0.8800%</td>
</tr>
<tr>
<td>Zhonghua Lin</td>
<td>0.3130%</td>
<td>0.2939%</td>
</tr>
<tr>
<td>Ms. Lenina &amp; Manesh Kokare</td>
<td>0.0071%</td>
<td>1.0427%</td>
</tr>
</tbody>
</table>

Table 2.2 – FAR-FRR with Existing Methods

2.11 Summary

This chapter introduced the main biometric concepts, First a definition was given, and justified the choice for the use of iris for the purposes of our work, and we focused in the anatomy of the human eye, with obvious emphasis to the iris. Later we overviewed the main stages of typical iris recognition, discussion of Iris image databases, and identified, through description and illustration, the types of noise that the public and free Iris image databases for biometric purposes. We stress that CASIA Version III database has been well accepted by researchers of the academic and discussed the performance of the existing iris recognition methods.