T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Electrical and Computer Engineering

HUMAN BIOMETRICS DETECTION AND RECOGNITION SYSTEM USING SVM AND GENETIC ALGORITHM IRIS AS AN EXAMPLE

Anfal AL-ZANGANAWI

Master of Science

Supervisor

Asst. Prof. Sefer KURNAZ

Istanbul, 2021

HUMAN BIOMETRICS DETECTION AND RECOGNITION SYSTEM USING SVM AND GENETIC ALGORITHM IRIS AS AN EXAMPLE

by

Anfal Waled Al-Zanganawi

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled “HUMAN BIOMETRICS DETECTION AND RECOGNITION SYSTEM USING SVM AND GENETIC ALGORITHM IRIS AS AN EXAMPLE” prepared and presented by “Anfal AL-ZANGANAWI” was accepted as a Master of Science Thesis in Electrical and Computer Engineering.

Asst. Prof. Sefer KURNAZ

Supervisor

Thesis Defense Jury Members:

Asst. Prof. Dr. Sefer KURNAZ	School of Engineering and Natural Sciences, Altinbas University	___________________
Prof. Dr. Osman Nuri UÇAN	School of Engineering and Natural Sciences, Altinbas University	___________________
Prof. Dr. Mesut RAZBONYALI	School of Engineering and Natural Sciences,, Maltepe University	___________________

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Anfal Waled Al-Zanganawi

DEDICATION

I would like to thank Allah Almighty for the power of mind, health, strength, guidance, knowledge and skills to complete this study.

This thesis is wholeheartedly dedicated to my parents. There are no words to describe what you mean to me; there is nothing that I can repay for what you have done to me. I will continue to do my best to achieve your expectations.

Lastly, I dedicated this to my husband, brothers and sisters, relatives, and friends who have been encouraging me during this study.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Asst. Prof. Sefer Kurnaz for all support during my study. It’s great pleasure to express my deepest gratitude to my friends who have shared with me best moments during my study for the Master degree.

ABSTRACT

HUMAN BIOMETRICS DETECTION AND RECOGNITION SYSTEM USING SVM AND GENETIC ALGORITHM IRIS AS AN EXAMPLE

Al-Zanganawi, Anfal

M.Sc. Electrical and Computer Engineering, Altinbas University,

Supervisor: Asst. Prof. Dr. Sefer Kurnaz

Date: June/ 2021

Pages: (73)

Applying the use of biometric characteristics for identification is increasingly showing itself as a viable idea. Each person has their own characteristics and these differ from the rest of the people. For example, there is no one with the same voice, with the same fingerprint or with exactly identical eyes. Even between twin brothers, there are differences, which makes biometric measurements an excellent reliable means of identification yet the biometric identification process, whatever the characteristic to be used, follows the following model: capture of a biometric sample of data, extraction of characteristics and finally the comparison. The capture consists of acquiring a sample of this characteristic. The feature extraction phase is the phase where properties are used to create a biometric signature. Finally, it is in the comparison phase that the final result is obtained in this paper we present an IRIS recognition system using the features of the iris and a classification scheme.

Keywords: Iris, Classification, Biometrics, Recognition, Deep learning

ÖZET

ÖRNEK OLARAK SVM VE GENETİK ALGORİTMA IRIS KULLANILAN İNSAN BİYOMETRİĞİ TESPİT VE TANIMA SİSTEMİ

AL-zanganawi, Anfal

M.Sc., Electrical and Computer Engineering Altınbaş University

Supervisor: Asst. Prof. Sefer Kurnaz

Date: June 2021

Pages: (73)

Uygulama Biyometrik özelliklerin kimlik tespiti için kullanılması, kendini giderek daha geçerli bir fikir olarak gösteriyor. Her insanın kendine has özellikleri vardır ve bunlar diğerlerinden farklıdır. Örneğin, aynı sese, aynı parmak izine veya tamamen aynı gözlere sahip kimse yoktur. İkiz kardeşler arasında bile, biyometrik ölçümleri mükemmel güvenilir bir tanımlama aracı haline getiren farklılıklar vardır, ancak kullanılacak özellik ne olursa olsun, biyometrik tanımlama süreci şu modeli izler: biyometrik veri örneğinin yakalanması, özelliklerin çıkarılması ve son olarak mukayese. Yakalama, bu özelliğin bir örneğinin elde edilmesinden oluşur. Özellik çıkarma aşaması, özelliklerin biyometrik imza oluşturmak için kullanıldığı aşamadır. Son olarak, bu yazıda nihai sonucun elde edildiği karşılaştırma aşamasında, irisin özelliklerini ve bir sınıflandırma şemasını kullanan bir IRIS tanıma sistemi sunuyoruz.

Anahtar Kelimeler: İris, Sınıflandırma, Biyometri, Tanıma, Derin öğrenme

TABLE OF CONTENTS

Pages

ABSTRACT .... **vii**

LIST OF TABLES .... **xi**

LIST OF FIGURES .... **xii**

LIST OF ABBREVIATIONS .... **xiii**

LIST OF SYMBOLS .... **xiv**

1. INTRODUCTION **1**

1.1 BACKGROUND 1

1.2 MOTIVATION 1

1.3 PROBLEM STATEMENT 2

1.4 CONTRIBUTION 2

1.5 THESIS ORGANIZATION 3

2. LITRITAURE REVIEW **4**

3. MATERIALS AND METHODS **8**

3.1 BIOMETRIC RECOGNITION 11

3.1.1 History Of Biometrics 13

3.1.2 BiometricsIdentification 17

3.1.3 TypesOfBiometrics 17

3.1.4 IrisRecognition 24

3.2 SVM CLASSIFICATION 30

3.3 GENETIC ALGORITHM 32

3.3.1 Basi Cconcept 35

3.3.2 Ga Fundementals 36

4. PROPOSED METHOD 39

4.1 READING THE IRIS 38

4.2 ANATOMY OF THE EYE 39

4.3 IRIS DETECTION 41

4.3.1 Feature Extraction Using Genetic Algorithm 42

4.3.2 Classification Using Svm 42

5. SIMULATION AND RESULTS 46

6. CONCLUSION 49

REFERENCES 50

LIST OF TABLES

Pages

Table 5.1: Properties of the datasets 45

Table 5.2: Comparing our proposed method in terms of error rate and accuracy in recognition. 47

LIST OF FIGURES

Pages

Figure 1.1: Simple Biometrics Recognition system 1

Figure 1.2: Traditional Biometrics Recognition System 2

Figure 3.1: Ancient Fingerprint in Minoan Pottery 14

Figure 3.2 Simple iris recognition system 24

Figure 4.1: Iris readers 38

Figure 4.2: Anatomy of the human eye 40

Figure 4.3: Iris normalization 41

Figure 4.4: Proposed method 44

Figure 5.1: Svm accuracy compared to other methods of classification 46

Figure 5.2: Mse of genetic algorithm feature extraction 47

LIST OF ABBREVIATIONS

SVM: Support vector machine

CNN: convolutional neural network

GAs: genetic algorithms

FMR: False Match Rate

FNMR: False Non-Match Rate

FPR: false positive rates

FNR: false negative rates

DCT: Discrete Cosine Techniques

RHT: Randomized Hough Transform

NLP: natural language processing

LIST OF SYMBOLS

X,Y	:	Coordinates
b	:	Bias
W	:	Weight Vector
(r, θ)		Pair of coordinates

1. INTRODUCTION

1.1 BACKGROUND

Biometrics is a pattern recognition area that studies the characteristics of living beings and their properties. It has been an area in constant expansion, with a major cause the need to increasingly preserve identity and ensure security. Among the most varied physiological characteristics, the use of the human iris as a means of identification has proven to be one of the most promising security methods. An iris, sent as an alternate eye, is quite protected, thus avoiding injuries that may affect her complex structure. This factor, together with stability over time, are some of the characteristics that make the iris a very promising biometric characteristic the figure below shows an example of a biometrics recognition system:

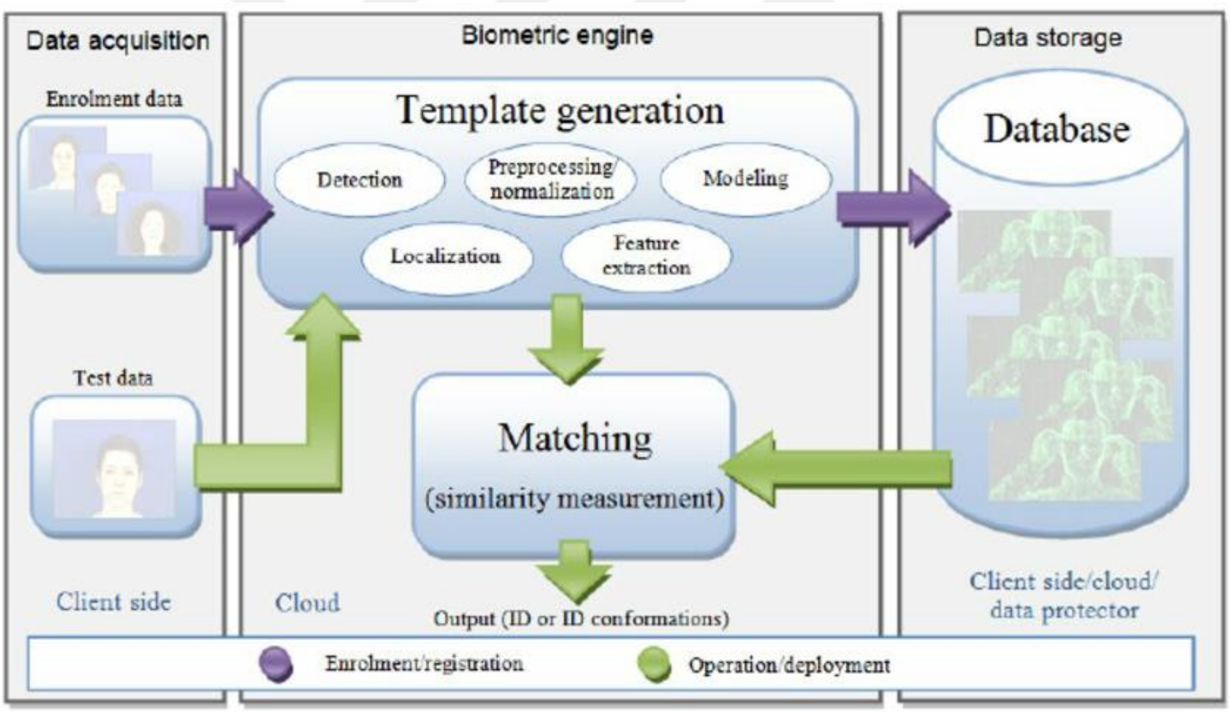

Figure 1.1: Simple biometrics recognition system.

1.2 MOTIVATION

Biometric traits are being used for identification more and more every day. No two individuals are exactly same, which is why traits of each individual are different from those of others. Some people may have the same fingerprints, voice, or eyes, but no two individuals will have the same fingerprints, voice, or eyes. Not just amongst twins, but even amongst identical twins, each one has their own distinct characteristics which make biometric measures a good, trustworthy method of identification.

1.3 PROBLEM STATEMENT

The following methodology is followed while using biometric identification: identification, characterization, and comparison to get a sample of this attribute are part of the capture. During the feature extraction process, features are employed to establish a biometric signature. At long last, the ultimate result is reached in the comparison step. A yes or negative response is delivered based on the system:

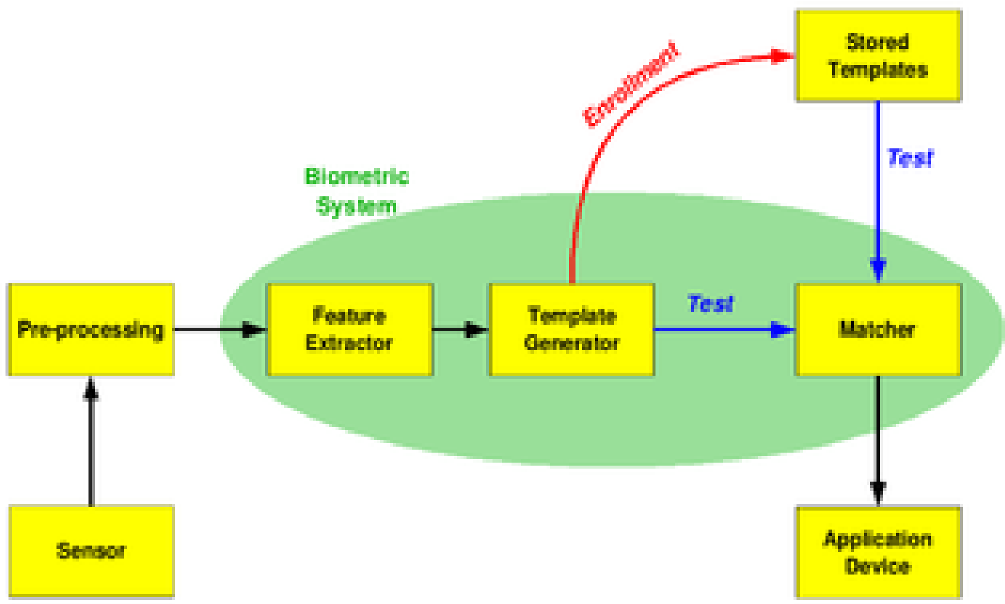

Figure 1.2: Traditional biometrics recognition system

1.4 CONTRIBUTION

This system has been developed and implemented to identify and classify the biometrics of an eye in order to construct a dataset of labeled samples, so that the system will collect the facial features and locate the eye while also extracting the facial features and ultimately classifying the eye.

1.5 THESIS ORGANIZATION

The thesis is structured as follows: Section 2 is where we review some of the previous work and implementation on Biometric detection. Section 3 is where we give a background about all the components. Section 4 is where we explain our model in details and implementation of that model in details, Section 5 is where we simulate our model and record the results obtained. Section 6 is where we conclude our work and put a future scope into perspective.

2. LITERATURE REVIEW

A review of the literature is a primary step in most scientific inquiry. Unless a study is thoroughly comprehensive and unbiased, it has little scientific value. Systematic reviews are essential because they help ensure the quality of subsequent studies. Systematic reviews synthesis previously published information in a fair and credible manner. For example, a preset search technique should be used for systematic reviews. The search technique must enable the search to be evaluated for its completeness. Additionally, researchers conducting a systematic review should be as inclusive as possible in their study findings, including highlighting evidence to the contrary and also promoting evidence in favor of their preferred theory. The first time IRIS was used, Alphonse Bertillon, a French ophthalmologist, categorized offenders based on the color of their eyes. According to a previous report, following extensive investigation and documentation, eye doctors Flom et al. [10] applied for a patent on the possibility of using the iris as an instrument to identify people; these patents were granted in 1987 and 1989, respectively, with algorithms by mathematician John Daugman. One of the big concerns nowadays is gaining access to sites that are prohibited. However, thus far, certain products, such as keys and remotes, are in high demand due to their poor dependability index, since they are easy to steal. To conclude, brainard et. al. (2) shown that biometric approaches are an effective method of reducing security issues since the "keys" are located inside the person. In multiple image segmentation methods by Grady et.al [3] Physical traits (typically, distinctive to each person) are already employed in individual recognition procedures. The results of the research conducted by Viola et. al [4] employed the characteristics of the item or person to identify it, such as voice, hand geometry, IRIS, walking, retina, and iris. The purpose of this research was to find out if people can recognize others based on various traits, and if so, how. Recognition of persons by features of the iris has gained significance in recent years, since this is an innovative approach that is noninvasive and has major advantages such as being stable over time, being shielded from radiation, and being stuffed with countless specificities. Besides the previously mentioned qualities, including texture, pigmentation, intensity, and relief, it is very difficult to find two persons with the identical eye traits. Phillips et. al. [5]. Today we have a large number of algorithms that perform iris recognition, starting from different principles and seeking considerable results, both from the point of view of system reliability and speed in the processing of information and return to the user da Costa et.al [6]. The objective of the work is the development of an algorithm for recognizing individuals through the iris using only the internal region of the iris, since it is in this region that most of the specific characteristics of each iris are found Pauca et.al [7]. Leung et.al [8], describes in, a methodology for the process of translating Cartesian coordinates to the polar coordinate system of non-concentric circles, called the rubber sheet. According to [9] the systematic biometrics recognition is a "method that allows specialists to obtain relevant and quantifiable results, this leads to the identification, selection and production of evidence based on research on a particular topic". For Bondy et.al [10] the literature reviews are intended to summarize, compile, criticize and synthesize the existing research on a thematic area or phenomenon of interest using a process of search, cataloging, ordering, analysis, criticism and synthesis. Woodard et.al [11] Results obtained from preliminary experiments conducted using optical IRIS data and capacitive IRIS data suggest that incomplete IRISs may be utilized to fake multiple users. It was suggested in the study of Park et al. [12] that partial authentication systems using IRISs (e.g., recording numerous impressions per finger) had a possible weakness. It is used to make photographs seem better and provide humans with a set of properties that computers can detect. Valetco et.al [13] The word image that comes from the Latin imago - is the visual representation of an object Zako et.al [14] An image can be defined mathematically as a two-dimensional (x, y) function, defined in a certain region A digital image is formed by an array of dots (pixels) with N rows and M columns, each point takes on a value in the range of [0.4+ 1]. It is usual for M.N and k to be powers of 2, thus the value of (1m.n) of the image at the point (1m, n) is given the name of gray level Mascerenhas et.al [15] The acquisition of a digital image is carried out by sensors and digitizers. Basically, the sensor convert the optical information into an electrical signal and the digitizer will transform the image analog in a digital image.

There are innumerable works that use deep learning to recognize the face. We provide an overview of some of the most promising efforts for facial testing and/or identification in this study. In 2014 Taigman and his collaborators presented in a study dubbed Deep Face [64] one of the first profound learning to recognize face, and they reached state-of-the-art accuracy in the LFW benchmark [65] (Deep Face: 97.35 percent vs. Human: 97.53 percent). Deep Face has been trained on four million face pictures. This study marked the identification of the face, and afterwards numerous researchers began to use deep learning for face identification. Sun et al. presented DeepID (Deep Hidden ID entity Features) in another promising effort in the same year [66] for face verification. DeepID characteristics were collected from a deep-convolutionary network's final hidden layer, trained to identify around 10,000 IDs in the training set. Sun et al. expanded DeepID in their follow-up study to identify and verify the joint face, named DeepID2 [67]. By training the common identification and verifying model, they show that the face identification task increases interpersonal differences by drawing DeepID2 features taken from different identities, while the face verification task reduces intrapersonal differences by combining the DeepID2 features extracted from the same identity. For identification, Cross-entropy is utilized as the loss function (as described for verification, the loss function was used to lower the distances in the intra-class features and increase the distance between the classes Various datasets for iris recognition have been offered in the past. Some of the most popular are: Database: CASIA-Iris-1000 includes 20,000 iris photos of 1,000 participants acquired by IKEMB-100 caméra. CASIA-Iris-1000 Database: The major causes of the CASIA-Iris-1000 intra-class differences are lenses and specular reflections [68]. UBIRIS Dataset: There are two separate UBIRIS databases, UBIRIS.v1 and UBIRIS.v2. The initial edition of this collection consists of 1877 photos taken in two separate sessions from 241 eyes. It replicates less restricted imagery [69]. The second UBIRIS database has more than 11,000 photos (and always expanding) with more realistic noise factors. IIT Delhi Iris Dataset: IIT Delhi Iris Database comprises 2240 photos from 224 individuals. These photos have a resolution of 320x240 pixels [70]. In this data collection, iris pictures have a varying color distribution and various sizes (iris). ND Datasets: ND-CrossSensor-Iris-2013 is made up of two datasets, which are taken using two iris sensors, LG2200 and LG4000. The dataset for LG2200 contains 116,564 iris photos, and for LG4000, 29,986 iris photos of 676 people [71]. MICHE Dataset: The Mobile Iris Challenge Evaluation (MICHE) comprises of iris photographs that are obtained under unrestricted smartphone circumstances. It comprises of almost 3,732 photos from 92 people on three smartphones [72] In comparison with face recognition, deep learning algorithms have taken many years to recognize iris. As one of the first pieces that used deep learning to identify iris, [73] Minaee et al. demonstrated that characteristics taken from an ImageNet trained pre-trained CNN model may reach a very good accuracy rate for the detection of iris.

In the study, the trained model was able to get cutting-edge accuracy using two iris detection benchmarks, CASIA-1000 and IIT Delhi database, by using features from many layers of VGG Net [74], and training a multi-class SVM. They also demonstrated that features taken from the VGG Net mid-layers acquire somewhat more precision from the end layers. In another work [75], Gang war and Joshi proposed an iris identification network based on convolutionary neural network that provides strong, discriminatory and compact data, resulting in an extremely high degree of accuracy and can work quite well in the recognition of iris images by the cross sensor. In [76], Baqar and colleagues suggested a system based on deep faith networks and contour information of iris pictures. Contour-based vectors have been utilized to differentiate between samples from various classes, i.e. the sclerairi and iris pupil contours, and are referred to as the Unique Signature. Once these characteristics have been retrieved, a deep belief network (DBN) with an algorithm-based, modified feed forward-neural network (RVLR-NN) for classification has been applied. In [77] Zhao and Kumar introduced a "Spatially Corresponding Feature" iris recognition model. It is based on a fully convolutionary network (FCN), which provides iris feature descriptors spatially. They also provide a "Extended Triplet Loss (ETL)" feature expressly intended to include the bit shifting and non-iris masking. The three-fold network is shown in Figure 16. They also constructed a sub-network to offer the right information for the identification of significant iris areas, which are key inputs for the newly designed ETL. In a few Iris datasets they were able to execute many conventional and cutting-edge iris recognition methodologies.

3. MATERIALS AND METHODS

In this chapter, we explain and illustrate how we implement the fundamental building blocks of our model, and we provide a quick introduction to those components. Performance requirements of a biometric system are significantly dependent on the application. For example, the FNMR rate (rather than the FMR) is a key design challenge in some forensic applications, such as criminal detection. In an application where the focus is on keeping impostors out, the FMR is among the most important factors (although we are concerned with the possible inconvenience to the legitimate users due to a high FNMR). FMR and FNMR are just two of several civilian efficiency standards with efficiency that falls anywhere between these two extremes. FALSE matches, such as with ATM card verification, may result in losses of several hundred dollars, while high FALSE recognition results in losing a lucrative customer. When it comes to biometric applications, the FMR and FNMR tradeoffs are shown in Figure 2. (b). IV. Research various biometrics various biometric traits are used in a number of different scenarios (see Fig. 3). The choice of a biometric depends on the application, and hence each has its own set of pros and cons. At this time, it is uncertain which biometric will suit all uses. Instead, a “ideal” biometric doesn't exist. Comparing the distance between the pinna and a reference point on the ear yields the distance between the prominent spots on the pinna. In general, one's personality can't be determined by their ear features.

Facial photographs are by far the most often used biometric trait among humans, and face recognition is a nonintrusive technique. Face recognition is widely used for both static identification, such as “mug shot” verification, and more complicated applications, such as face detection in a crowded environment (e.g., airport). Facial characteristics, such as the eyes, eyebrows, nose, mouth, and chin, as well as their spatial connections, are the main factors taken into consideration when using facial detection. Face recognition systems that are available to the public are capable of providing reasonable levels of authentication efficacy, but they set various constraints on the quality of facial photographs, such as limits on lighting and context. However, these gadgets typically have difficulty identifying a face in images that are shot from drastically diverse angles and lighting conditions. The debate about whether or not an individual's face is sufficient for distinguishing a person from several identities is ongoing. To utilize facial recognition technology effectively, three requirements must be met: first, the device must be able to identify whether a face is present in the acquired picture; second, it must be able to locate the face if it exists; and third, it must be able to identify the face from a general viewpoint (i.e., from any pose).

Infrared thermogram of the face, hand, and hand veins, seen by infrared thermography the pattern of heat radiation emitted by a human body is a fundamental property of human beings, and this pattern may be recorded by an infrared camera that doesn't do any harm to the human body. If the technology were utilized for covert identification, it would be conceivable, in uncontrolled situations with heat-emitting surfaces (room heaters and auto exhaust pipes), obtaining a proper picture might be challenging with a thermogram-based device, since there is no requirement for physical contact. Near-infrared imaging is used to detect hand vein function by scanning the back of a clenched fist. Thermograms are not widely utilized because of the price of infrared sensors.

Fingerprint**:** Using fingerprints for personal identification has been around for quite some time, and the reliability of fingerprint matching has been shown to be rather excellent. At around seven months into a pregnancy, the form of a person's fingerprint is determined, and it consists of many ridges and valleys on the fingertips. Fingerprints on identical twins are different, and each of the ten digits on the same guy bears different prints. Buying a fingerprint scanner in bulk is approximately $20, and integrating a fingerprint-based biometric in a device (such as a laptop computer) has now reached a price point where the marginal cost of each additional device may be considered low. Precision of presently available fingerprint recognition technologies is adequate for authentication systems and small- to medium-scale identification systems needing a few hundred users. A large-scale identification-detection process that impacts millions of people is possible because to the extra information included in the individual's numerous fingerprints. There is a potential problem with today's fingerprint recognition systems, and that is that they need a lot of computational resources to work well. The fingerprints of a restricted fraction of the population may be unable to be used for automated identification owing to genetic origins, age, environmental, or occupational considerations (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

Gait**:** is a dynamic spatiotemporal biometric that explains how an individual moves. Verification in some low-security applications is possible thanks to the gait, which isn't very distinctive.

A behavioral biometric that varies over time due to weight fluctuations, substantial joint or brain injuries or intoxication is called gait. This biometric is acceptable since it takes a nearly identical picture of your face. Articulate joint movements need a lot of input and are computationally taxing, as they are dependent on visual video images of a person walking.

The gait of an individual describes all of the spatiotemporal aspects of how they walk. In low-security applications, gait is unique enough to enable verification. Gait is a behavioral biometric that is unstable over time because to changes in body weight, significant joint or brain impairment, or inebriety. A biometric like a photograph of your hands is called a biometric, and gait profiling is comparable to it, but it could be better. Because they demand a lot of data and computing time, gait-based solutions need a lot of input.

The anatomy of hands and fingers the palm and wrist form are included into the hand geometry recognition processes. Industrial hand geometry-based verification methods are developed by hundreds of websites throughout the globe. This is a straightforward procedure, and it is cheap and quick to use. Hand geometry-based systems do not seem to be affected by individual variances, such as dry skin, or environmental conditions, such as dry air. Because the hand's configuration isn't believed to be very unique, hand geometry-based identification systems cannot be scaled up for systems that need to identify one person from a huge number of persons. Additionally, the form of a child's hand might change as they develop. Other problems that the hand geometry may be hard to extract include an individual's jewelry (e.g., rings) or movement concerns (e.g., arthritis). Due to the size of a hand-geometry-based framework, such as Surface, integrating it inside laptops such as Ultrabook is not possible. Another approach to user identification that is focused on verifying a smaller part of the hand (often the index and middle fingers) rather than the whole hand is known as single-digit verification. While hand-sized, these devices are somewhat bigger than the ones used in other biometrics applications, and much smaller than those used in geometrics (e.g., fingerprint, face, voice).

Hand geometry recognition systems analyze the overall shape of the human hand, the breadth of the thumb, and the lengths and widths of the digits. Many commercial hand geometry-based verification methods have emerged over the Internet. It is simple, fast to execute, and cost-effective. Hand geometry-based systems are shown to be resistant to person imperfections, such as dry skin, and the influences of the environment, such as dry air. Hand geometry-based recognition systems can't be scaled up since individuals are more unique to one another than they are to the general population.

Iris: The iris is the ring area around the pupil and extending on all sides to the sclera (white of the eye). In the first two years of life, the optical texture of the iris develops and then stabilizes. Your iris has a complicated pattern, with a lot of subtlety that will assist in your ability to recall your identity. Iris-based recognition systems that are operational today are promising, indicating that iris data may be used to create large-scale identifying systems. While irises are unique to each person, fingerprints are just as distinctive. Iris size, shape, and color are unique even among identical twins. It is exceedingly difficult to control the iris texture surgically.

3.1 BIOMETRICS RECOGNITION

Linguistic approaches such as decomposition using the Greek roots of the terms “bio” and “metric” are able to deconstruct the term biometrics. One might describe bio as a statistical study of the physical qualities of living creatures and their quantifiable features by associating the word bio with the prefix that implies "life" and metric with the word "measure." We know through extensive research that people have several qualities that can be measured and evaluated for study purposes, which causes us to categorize them into distinct identities. Every individual is different, and these differences may be utilized to distinguish one individual from another. One of the major reasons biometric measures are used is for the protection of personal identification. Printing was well known as early as the early 1900s, and still is now, thanks to digital printing. Notably, however, there are several other forms, some of which focus on the qualities of the living creature, while others focus on how these traits are used to help distinguish a distinctive identity.

One condition that has to be satisfied in order for a biological measure to be defined as a biometric characteristic is universality: individuals must have this characteristic.

To acquire the best biometric characteristic, these criteria are required. This requirement also ensures that all individuals must possess this attribute from the beginning. The collected sample of that attribute cannot identify more than one person. There must be a nearly equal connection between persons, since proving a guarantee's reliability is difficult, and hence a differentiation cannot be achieved with absolute certainty. To make sure that the feature cannot be changed is to determine whether over time and with the natural body changes, there are no alterations to the qualities to impact the system. The quantitative sample must be able to be captured and stored using this property.

But in order for these features to be successful, there must be biometric systems that meet the following requirements:

Vulnerability**:** the capacity of a system to be infiltrated by fraudulent means;

In order to maintain system stability, it is necessary to ensure that the procedure is not time-consuming. In addition, you must describe the consequences of the work, and carry it out in a reasonable amount of time. Additional influences which may have an impact on these traits must also be considered. In some situations, some features are not appropriate to use on a regular basis, thus the biometric system is responsible for verifying that the process does not compromise the user's physical or moral integrity, and the user is ready to use it on a regular basis. A functional biometric system should also be resistant to attempts to break it.

For thousands of years, human beings have been able to identify persons via their physical traits, such as the face, the voice, and the walk. French police commander Alphonse Bertillon developed and implemented the notion of using a wide array of body measurements to identify criminals in the mid-nineteenth century. Human fingerprints proved to be unique in the late 1800s, and this was obscured by the appearance of the notion. According to this research, a number of significant law enforcement agencies thereafter implemented the practice of keeping suspects' fingerprints in a database and "booking" them (actually, a card file). Locating the culprits after the fragmented fingerprints are left at the crime scene is often referred to as "lifting latent fingerprints" and matching them with fingerprints in the database. It might be said that biometrics had a meteoric rise as a consequence of its wide-scale employment in law enforcement to identify criminals and inmates, as well as in criminal forensics to confirm suspect identities. Biometrics is the collection of biological measures such as fingerprints and palm prints. Biometrics is distinct traits that may be used to identify individuals based on several physiological and/or behavioral characteristics.

The property of universality is something that should be present in every person.

Distinctiveness: there are two distinct persons for every two individuals.

Constancy**:** throughout time, the characteristic should be fairly steady (in relation to the matching criterion).

Collectability**:** This characteristic may be assessed as a numerical score. However, while taking into consideration additional factors, it's crucial to have a biometric device that encompasses a number of problems, such as:

efficiency**,** which relates to the feasible recognition accuracy and pace, the resources needed to obtain the desired recognition accuracy and speed, as well as organizational and environmental considerations that influence recognition accuracy and speed. A functional biometric device should satisfy the specified recognition precision, pace, and resource specifications, be safe for consumers, be recognized by the expected population, and be reasonably resilient to numerous malicious methods and system attacks.

3.1.1 History of Biometrics

In a brief and simple historical approach to the evolution of biometrics, it can be said that the first use dates from the 14th century, as portrayed by explorer João Barros, considered the first great Portuguese historian [26]. In one of his writings, he describes that Chinese traders printed children's palms and feet on paper to differentiate themselves from the rest [13].

Around 1890 an attempt was made to find a solution to the problem of identifying convicted criminals, making biometrics a possibility for this problem and the study process started. It was then that Mr. Alphonse Bertillon, a French anthropologist and policeman, developed a set of body measurements. But this solution quickly failed when it was discovered that there were people who shared the same measures and, consequently, analyzing only those measures, there was ambiguity in the identification of the individual. After this failure, the police started using fingerprints, a method developed by Richard Edward Henry, just as it had in Chinese methods years before [13].

More recently, in biometrics, only systems based on fingerprinting have been used and investments have been made in others that are already in practice, and there are also many others in case of study. Numerous companies continue to invest in the study of new biometric solutions as advanced technology advances. In the same way that the industry is advancing, there is also a marked concern with legal issues and privacy rights, with new laws and regulations being legislated [27], [13].

Figure 3.1 Ancient fingerprints in Minoan pottery

The first of the philosophical meanings of identity according to which identity is the property of ìmesmoî has purely speculative relevance. The essence of being is unattainable for human reason. So too, the concept of the same, as already mentioned above, is indefinable. The other meanings, however, are close to the common sense of identity on the concrete plane. For human reason, the realization of identity originates from the multiplicity and variability of beings. H · living beings if there are lifeless ones, h · human beings if there are beings that are not human. Therefore, when talking about identity, it also refers to difference. It is necessary to discuss the relationship between identity and difference. Identity is a concept perceived by comparisons between beings. Only a woman can be identified in relation to the group of individuals who are not women. When you say ìele È argentinoî, it is also said that he is not a Brazilian; he is not a Bolivian and so on. Therefore, beings are identified by both affirmative and negative characters. The strongest impression, at first, seems to be that identity determines the difference, since identity designates the nature of the thing. However, the process of identifying something starts with the recognition of its differences with others. If there are no distinct characteristics between them, they are indistinguishable. For this reason, identity appears at the same time that the difference appears. Another example: no one feels the need, except in rare situations, to declare themselves to be human, since this characteristic is common to all communicating beings20. In addition to being simultaneous, the concepts of identity and difference are constructed by language. Since language is confused with culture, it can be said that identity and difference are cultural products. There is no identity based Reflecting on the mechanism of identity formation based on differences, one must question whether in any determination of an identity there is actually a dose of exclusive power embedded in the process. This reflection seems pertinent even in relation to identification processes apparently based on objective criteria, such as those involved in the determination of biological or speculative identity. The term biometrics is derived from the Greek words bio which means life and metria which means measure [2]. According to the National Science and Technology Council (NSTC) [5], biometrics is a general term used as a measurable physiological or behavioral characteristic that can be used for automatic recognition of individuals. The ability to uniquely identify people and associate personal attributes with an individual is crucial in today's society. The explosion of population growth, coupled with increasing mobility in modern societies has impacted the development of sophisticated identity management systems that can efficiently store, maintain and obliterate individuals' identities. This management is critical in applications such as regulations for the transition of people between countries, restriction of physical access, control of access to resources, among others In this scenario, biometric recognition has been widely used and can be defined as the science of establishing an individual's identity based on the person's physical and / or behavioral characteristics, whether automatically or semi-automatically [1]. Biometric systems are used for verification and identification [6]. In the verification, the biometric trace is presented by the user together with an identification code of the same, after that the system checks if that biometric trace belongs to the person it is claiming to be. In the identification, the user provides only the biometric trace and the system is responsible for identifying who is the person who provided the biometric trace. 3 The main biometric systems developed use digital, iris, face, signature, voice, among other characteristics. Any human physiological or behavioral characteristic can be used as a biometric characteristic as long as it meets the following requirements [6]:

A. Universality: each person must have this characteristic.

B. Uniqueness: the biometric characteristic must be unique for each individual, that is, there cannot be two individuals with identical characteristics.

C. Permanence: the characteristic must be sufficiently invariant for a period of time.

D. Feasibility of collection: it is necessary that the characteristic can be quantitatively measurable [51].

Behavioral biometrics refers to the measurement of data derived from actions performed by the user and, therefore, measures the characteristics of the human body in an indirect way. Below are some examples of behavioral biometrics:

A. Signature.
B. Way of walking.
C. Way of writing.
D. How to type.
E. How to use the computer mouse.
F. Voice.

Physiological biometrics is based on the direct measurement of parts of the human body, such as the fingerprint or iris scanner. Below are some examples of behavioral biometrics:

A. DNA.
B. Retina.
C. Fingerprint.
D. Iris.
E. Ear.
F. Face.

In this, Work we focus on physiological biometrics, more specifically the iris biometry that will be introduced in the next section.

3.1.2 Biometrics Identification

The biometric identification model regardless of the biometric measurement being used, there are two distinct procedures: registering a person in the database using a new identity and identifying an individual by comparing them with the others in the database.

In the procedure of registering a new identity, a digital biometric representation is captured through a sensor, which varies depending on the biometric characteristic that is extracted, then follows the feature extraction phase, one of the most relevant in the entire process [29]. To facilitate identification and storage in the database, a biometric signature is created from the digital representation that is representative only of the person who made the registration.

In the case of identification, that is, recognition of a person who already has a previous registration in the database, the initial process of capturing and extracting characteristics is identical to that of the registration. It differs from registration because instead of being stored in the database, the biometric signature is involved in the comparator phase and will be compared with other signatures. The result of this comparison is the degree of similarity of the signatures that indicates the identity of the individual.

In the biometric recognition phase, the comparison stage can be classified according to the number of checks. A person can claim to be the character X, and the comparator will use the database and then compare the captured biometric with the biometric measurement of the person who claims to be who he is. This mode is also called as positive recognition, as it only checks if a person is who he says he is. The other way is to try to identify who the person is, comparing the obtained signature with all the existing ones in the database, giving an answer of the identity, or simply.

3.1.3 Types of biometrics

A. Fingerprint

Fingerprints are a set of details, namely arcs, loops and forks, existing at your fingertips. Its use is done by creating a fingerprint with ink on a flat surface so that skin imperfections are legible. More modern systems capture the image through a sensor, passing the finger over the reading part of the sensor. Its performance, ease of use and precision make digital printing one of the most used and reliable measures to be implemented in a biometric system. Wounds, dirt and skin problems are disadvantages for a good fingerprint reading [3].

B. Handwritten Signature

Although a forger may be able to perfectly imitate the design of a signature, it is almost impossible for him to repeat the dynamics with which it is made. The rhythm of writing, the pressure exerted on the paper, the speed, the acceleration, the movements exerted in the air and the angle of inclination of the pen, are examples that make the act non-reproducible [3].

The digital signature is quite common. Most documents are completed with a signature, whatever the purpose of that document. Another advantage of using this measure is that it can be changed. With regard to the drawbacks, this measure requires physical stability of the members for a reliable subscription. There is also the possibility that the signature may change over time, as well as being affected by the physical and emotional conditions of individuals [38].

Biometrics is a general term used as a measurable physiological or behavioral characteristic [1]. Studies related to biometrics started several centuries ago, but automatic biometric systems have only been developed in the last few decades due to significant advances in technology [2]. This advancement in technology coupled with population growth has impacted the demand for the development of sophisticated identification systems. In this scenario, biometric recognition has been widely used and can be defined as the science of establishing the identity of an individual based on physical and / or behavioral characteristics [1]. Physiological biometrics is based on the direct measurement of parts of the human body, such as the fingerprint or iris scanner. Behavioral biometrics refers to the measurement of human body characteristics in an indirect way, such as a person's signature, or the way of walking [3]. Iris identification is suitable for high-level security systems, as the structure of the iris is formed in the first years of a person's life, is not genetically determined and remains unchanged over time [1]. The iris is well protected and despite being an easily visible body part, it is an internal component of the eye. The probability of having two people with identical irises is practically zero [4], that is, it is practically impossible to have people with the same irises. Even the irises of identical twins are different, or in the same person the iris on the right side is different from the iris on the left side [4]. Iris recognition can be used to unlock a cell phone, make bank transactions, free access to private locations, unlock computers, and various other functions. The efficiency of systems based on iris recognition is greater than several other biometric systems, such as fingerprints, voice recognition; among others Human identification has always been a necessity and a challenge. The recognition of an individual among his peers may depend on security in a commercial transaction or the security of a group of people against an aggressor. Being identified is essential to have your rights recognized. Identifying someone is also essential to demanding that a duty be performed. Whether for a man or for an institution, identifying people means relating to security. Someone identifies himself by the characteristics of his body. Man as a living or dead organism is distinguished as an individual by biological characteristics, including patterns of behavior and response to external stimuli. The history of his habits and activities is written on his body, also serving for his recognition. Trusting some characteristics to remain over time, ancient or more recent civilizations marked the bodies of some to be more easily recognized later. Forensic Medicine has always been concerned with the identification of man, his parts, and his remains. The ways of accomplishing this identification have evolved side by side with technological evolution in different times. If in the past the skin was marked to identify condemned or slaves, today, through molecular analysis, a body or an individual can be recognized. In a computerized society in which important decisions can be made in seconds and communications bring individuals together without considering distances, new forms of identification have become necessary. The information technology itself and the electronics provided the answers to this need, with the creation of biometric techniques:

C. Face shape

It is by looking at someone's face that you can identify people. This identification is made according to the strokes and curves that each face presents. This is one of the most promising methods; however it still has error rates high enough to be continuously implemented [2]. As it is possible to acquire the biometric sample at a distance, it does not require the direct interaction of the subject.

Within several advantages, facial recognition identifies individuals through the features of the eye, nose and chin fittings, which are the ones that remain uniform for the longest age. However, when the capture is not frontal and exceeds the 20o, some problems in the identification begin to appear [53].

D. Iris

Iris reading is one of the most accurate existing biometric processes. It is the most visible and colorful part of the eye and begins to be formed from an early age without suffering any changes, saving rare diseases. Its function is to control the entry of light into the eye. The high detailed patterns of the iris make it quite distinctive (even both irises of a person are different) and therefore a good biometric measure. For a better use of these characteristics the individual must cooperate to capture a clear and unobstructed iris. Reading is not affected by glasses or contact lenses. To illuminate the iris, an infrared light illuminator is used. This light is not part of the visible spectrum and is not captured by the human eye; however it is captured by the camera's sensor. Poor image qualities are a disadvantage in this type of biometric solution.

E. Retina

The retina is the part of the eye responsible for imaging. When the retina is read, an image is captured with the patterns of blood vessels in the back of the eye. For this capture, the individual needs to remove the glasses and place the eye close to the retinal reader, focus on a certain point and remain immobile for 10 to 15 seconds [31].
The retinal reading cannot be faked and it is impossible to forge a human retina and has a high reliability rate. However, this process is too cumbersome and slow.

F. Hand Geometry

Length, width, thickness and areas are characteristic not only of the palm of the hand but also of the fingers, which are evaluated by a biometric system of this type, which captures an image of the hand. At the 1996 Olympic Games, hand geometry was used to control athletes' access to the Olympic Village [44]. The fact of creating a small biometric signature, being of low cost and guaranteeing reliability and performance, among other characteristics, makes this biometric measure credible.
Changes such as aging and weight loss or gain can influence the results, as well as their shape and structure with advancing age, especially when going from children to adults.

G. Voice

The length of the neck, the size of the nasal cavities and the shape of the mouth affect the sound of the voice. The harmonic patterns of the voice are stored in a database instead of pre-recorded phrases. Thus, imitation is impossible, as the aspects measured by the system are not perceptible to the human ear [3].

Noises picked up around during the reading of the voice can influence the captured sample, as well as badly pronounced words. Once again, emotional conditions can affect the good performance of a voice recognition system [8].

H. Vascular Pattern

Through the use of infrared light it is possible to obtain the map of blood vessels in the hand. The vascular pattern, unchanging throughout life, is developed before birth and is individual even for identical twins [3].

It is an advantage that the veins are inside the skin and therefore are not subject to change. Its use is very simple and practical and the analysis time is around 2 seconds. However, these systems are a little financially expensive and require a sizeable sensor [22]. There are several types of blood vessel recognition, including veins in the fingers, wrist, palm, and back of the hand. However, the recognition process is the same for all situations. Vein recognition has a FRR of 0.01% and a FAR of 0.0001%.

I. Ear Shape

It is a difficult task to try to accurately describe what someone's ears are like, mainly because they don't have the vocabulary to describe their shapes. Interested speech therapy has been around for more than 100 years, but it is still debated whether the organ is unique enough to serve as a password. The most famous study was done in 1989, in the USA by Sheriff Alfred Iannarelli, who collected images from 10,000 ears and found that they were all different. However, in real twins, although different, they were quite similar, which questioned the performance of the ears as a biometric measure [5].

It is an advantage that the shape of the ear remains fickle and it is extremely simple to acquire a biometric sample. However, some positioning adjustment is necessary before the sensor that will capture the image.

J. DNA

Deoxyribonucleic acid (DNA), also known as English-derived DNA, is an organic compound that contains molecules and genetic instructions that coordinate the development and functioning of living beings.

The four bases that make up DNA (adenine, thymine, cytosine and guanine) are organized in pairs up to 3 billion forms. For this reason, the system is today considered the most infallible and, therefore, the most difficult to circumvent. Because it is expensive, slow and invasive (it uses blood or tissue samples, such as hair), it can take decades to become reality [3].

After DNA collection, it is not possible to obtain a result immediately, which minimizes the relevance of a biometric system with this characteristic.

K. Odor

Smell is one of the main basic senses of the human being. It is difficult to characterize a person by their odor, using the current vocabulary, as occurs in the biometric measure of the ear [23].

Odors are composed of chemicals. It is based on them that the system captures the smell and classifies each person. However, emotional and dietary factors can alter the recognition process. As you would expect, perfumes are also a setback for this type of biometric measurement.

L. Typing Dynamics

The user's profile is verified based on the mode of his interaction with the keyboard, such as the speed, pressure and time of double clicking on the same key, thus making a set of characteristics difficult to be imitated [3]. In short, it is more important how a person writes on the keyboard than what he writes.

There are two verification techniques: static and continuous. Static verification analyzes the dynamics of typing on the keyboard at a certain time with specific text, such as entering a password. However, it is in continuous verification that the greatest challenge exists, due to factors that can affect the dynamics of writing, such as the type of keyboard, the emotional and physical conditions of the user. With regard to the learning algorithm, the biggest problem lies in the impossibility of training the system from a given number of characteristics, since the amount of data coming from the keyboard is never known [43].

It should be noted that no additional device is needed.

These are the most common existing biometric measures; however there are others that are in the study phase, such as the walk of the human being, more suitable for criminal recognition captured in surveillance circuits. The way we grasp things is also deterministic for each person as is the perspiration, the glow of the skin or the salinity that exists in the human body. The nail matrix, through the epidermal structure of the fingertips, ends this wide range of biometric measures [3].

Biometrics is the science of recognizing someone's identity through physical or behavioral attributes, such as the face, fingerprints, voice and irises using electronic technology and computer resources. The use of biometric techniques has been increasing, for example, in national and international identity documents, control of physical or data access, identity control for 2 purposes of commercial transactions, criminal purposes, etc. The evolutions of this field follow the pace of evolution of contemporary technology, that is, they are extremely accelerated. Biometric techniques include those based on ocular attributes such as the characteristics of the iris and retina. Especially the first, Ìris biometrics, has found an increasingly frequent use in the daily life of the common citizen, and tends to have an increasing use in practice and finally using a trained artificial neural network to identify individuals. Ahmad obtained a hit rate of approximately 96%. Yong Zu et al. [23]. Developed its own image acquisition device. Edge detection is used to locate the iris. After that, the characteristics are extracted using a Gabor filter and a 2-D Wavelet transform.. Finally, the characteristics are compared using the weighted Euclidean distance. Youn zu et al. obtained a hit rate of 93.8% when using Gabor filters and 82.5% when using the Wavelet transform. Based on the works mentioned above, we can see that most of them use a special camera, which makes the monetary cost high, in addition to the techniques used generating a high computational cost as well. A point that can be noted in Ahmad's work [15] was that he applied DCT to the entire image, thus taking part of the skin, eyelashes and other factors that can interfere with the identification. Another interesting point would be the training of the neural network, because as more people were registered, the training would take time, causing a high computational cost. In view of these problems, an algorithm that uses commercial cameras for photo acquisition is proposed, which would reduce the monetary cost, after the acquisition, algorithms with low computational cost would be used, such as the use of SVM instead of neural networks.

3.1.4 Iris Recognition

The process of iris recognition includes a scheme for the segmentation of the iris, which tries to segment the iris in any type of image, including images with noise. The standardization process introduces two distinct strands: one and two dimensions, which will facilitate the following processes. These two strands are independent. After normalization, an analysis is made of the existing noise in the received image and its performance is evaluated for the next phase of feature extraction. This phase applies only to standardized two-dimensional images, and its application is optional. After normalization, the images can go straight to the feature extraction phase. It is then in the feature extraction phase, where the use of wavelets is proposed. This phase ends with the creation of the binary biometric signature, which, compared with the others, will respond to the stage of classification of the iris and consequently to the biometric recognition More specifically for the iris recognition phase, and after capturing the biometric sample, the image of the eye containing the iris is processed in order to separate the iris from the rest of the image. This step is called segmentation. The segmented iris is then normalized, where it has a more favorable shape for the other stages. The feature extraction and classification phases are identical to those mentioned in the previous paragraph. Also, as a result of the classification phase, a quantitative value of similarity can be obtained. This value indicates how similar a subscription is to the one being compared.

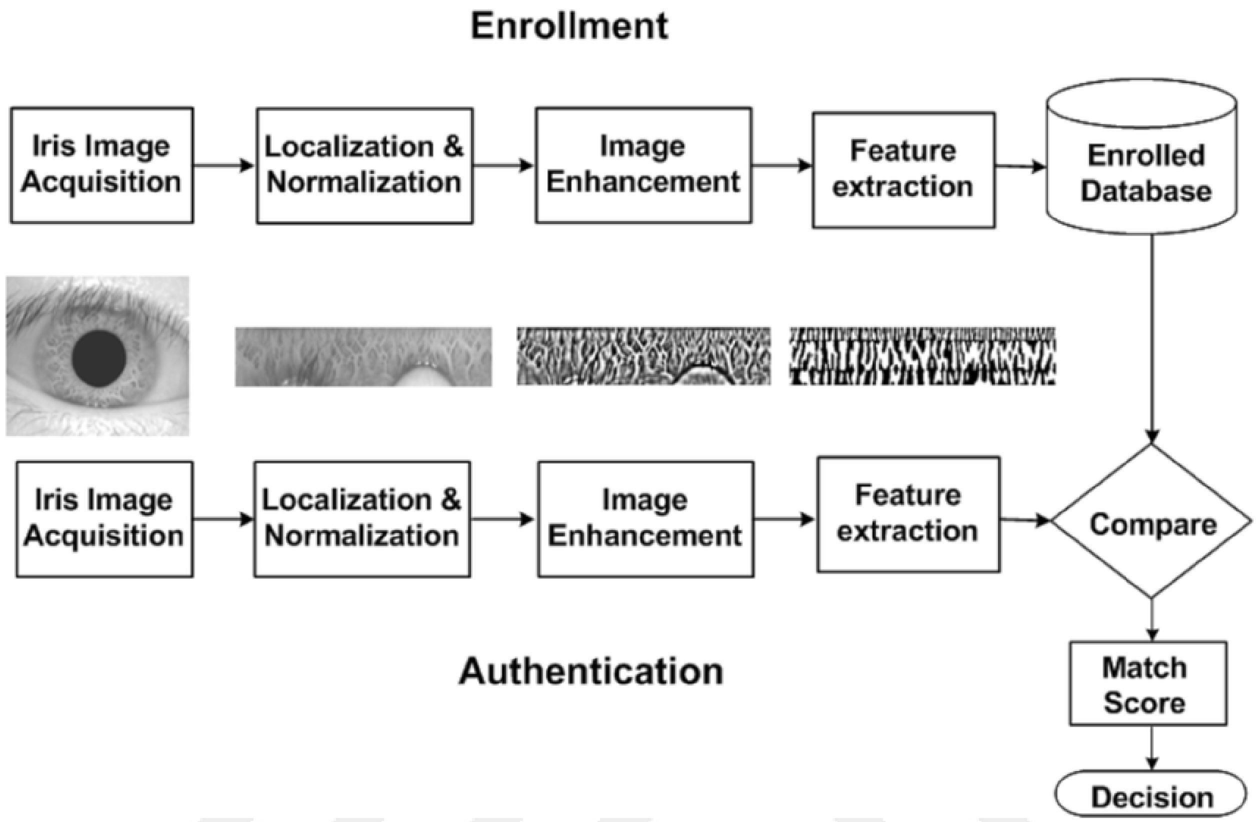

Figure 3.2 Simple iris recognition systems

At present, signatures, passwords or even identification cards are used as means of identification. However, passwords can be forgotten and ID cards stolen. This is how interest in biometric methods arises, in personal identification based on physiological and behavioral characteristics, and individuals do not forget or lose their physical characteristics in the same way as with passwords and identification cards.

The biggest hurdle for the production of a commercial facial recognition model is the inventive spirit responsible for the creation of an alternative system employing approaches not employed in present patented systems. The suggested approaches attempt to evade Daugman's patent, which is the only one that has been effectively incorporated in commercial goods [12]. The degree of precision of the findings acquired must always form an integral part of the individual being recognized. In contrast, such great accuracy of findings is not predicted in quasi-recognition software.

Many past attempts to improve iris identification have had significant success, but they required a lot of extra processing, including segmentation and unwrapping the original iris into a rectangular section (collected under different lightning and environmental conditions). Due to recent efforts, a lot of resources have been put into developing models for simultaneously learning the properties and making predictions. Too far, the best results have been achieved by convolutional neural networks (also known as “Convolutional Nets” or “ConvNets”) in areas such as computer vision and natural language processing (NLP) [12]. Success is attributed in large part to three critical factors: datasets with huge numbers of manually labeled features, processing tools like GPUs, and techniques that help reduce overfitting, such as dropout. Picture classification, picture segmentation, super-resolution, image captioning, emotion analysis, face recognition, and object identification are some of the computer vision problems that deep learning has been used to. It has demonstrated to outperform other approaches [13] to [20]. Additionally, sentiment analysis, machine translation, name-entity-recognition, and question answering (e.g., NLG) are often used to it. As well, the design qualities developed via these creative solutions may be used to many other activities. For example, a trained model for a given task may be leveraged for another task if it is combined with a classifier/predictor. This paper [26] by Minaee et al. followed up on [25] and examined the effectiveness of convolutional features trained on a generic picture classification challenge for iris recognition. A large number of datasets is available, and some of them have a good number of samples, making it possible to train a convolutional neural network from the start; however the majority of datasets have a limited number of examples per class, making it impossible to train a convolutional neural network from the start. When we consider only a few classes, we present a deep learning approach for iris recognition in this research, (few shots learning).

In this study, we propose an iris identification system using transfer learning, which is based on a prior implementation. We fine-tune a pre-trained convolutional neural network using a popular iris detection dataset (trained on ImageNet). To start with, we'll provide a quick review of transfer learning followed by the process of designing the model. A. The transfer of learning the machine learning strategy of transfer learning involves having a model learned on one task moved to a similar task, in which the model is often tweaked to account for the different training context. For example, using an image classification model trained on ImageNet, doing medical picture categorization would be possible. Thus, it would make sense to apply the same abstract representation to a different categorization job. One of the most common ways to use the trained model for a new task is to use a different strategy. In the methodology shown above, the model is first employed as a feature extractor, and then trained to be a classifier/ regressor. In this strategy, the pre-trained model's intrinsic weights are not modified for the new task. One may apply a pre-trained language model as an example of the first strategy, where the language model has already been educated to represent a certain term (such as sentiment analysis, NER, and so on). The second training technique uses pre-trained model weights as beginning values for the current task, which are changed during training.

Biometric security techniques, including iris recognition, are becoming important nowadays. It is called biometrics when we examine biological variation and related phenomena. Biological characteristics vary from person to person, and hence a device that can recognize humans by measuring such variances is referred to as biometric recognition. An identification process that utilizes biometrics verifies (or identifies) a person whose identity has already been registered in a database of "approved" persons. This includes the concept of identifying someone, but also verifying that they are who they say they are. Traditional definitions of the word refer to the term identification as meaning a closed group of people who identify with one other. It indicates that one of the N permitted persons has access to the biometric system, and that it's unnecessary to establish a threshold for the system's usage since one of the N persons is most suited to the user. This "1-among-N" description is often used to identify. Verification occurs in an open group. This means we cannot determine if the system has a complete understanding of the user's identity. When it comes to practical application, the user identifies persons with the database. If it is not recognized as such, it is an impostor. In the context of one-for-one verification, we may use the term "one-for-one." Most of the consumer biometric systems that are being installed are on the outskirts of military and police applications, and are being utilized instead of (or to supplement) the various forms of personal identification, including personal codes, passwords, cards, and keys that currently respond to the diverse authentication demands of consumers. SVM, Random Forest, and HMM [1–3] are widely employed for the detection of human behavior, which is conditioned by the amount of data that has been processed before. It is not especially durable, and it may need quite a bit of processing time and memory space. DNNs are applied immediately to the data flow without any pre-processing or feature selection to many challenges, including gesture recognition and handwriting categorization. We conducted our research in order to better understand how the neural network operates. On the subject of image identification and classification, we may use imageNet and pascal voc, both of which focus on objects in an image. Convolutional neural networks, or ConvNet CNNs, are often applied in computer vision as a result. The CNN technology has found its way into several biometric questionnaires as well. A kind of neural network that specializes in matrix and signal data processing is called a convolutional neural network. Two more convolutional and pool layers are added to the network. Let's examine each of these topics in further depth in the following sections. Dividing the image, normalizing it, segmenting the data for each eye image, and finally Classification is the process of completely automated processing via four distinct steps. We use deep learning using neural networks to demonstrate a methodology in this paper. Both automatic segmentation and feature extraction take place in the beginning and final stages of the deep neural network model. This integration offers an all-encompassing technique that utilizes the outputs of several deep neural networks of varied sizes (input size). Iris recognition is now using deep learning because of a number of reasons. The machine learning subfield known as deep learning is part of deep learning. Algorithmic computation, or learning by algorithm, involves programming computers to test, create, and learn new algorithms. Machine learning has existed for decades. During the preceding two decades, many artificial intelligence techniques, such as neural networks, have been produced. In computer vision and recognition difficulties, neural network-based algorithms play a vital role in making use of deep learning. Neural networks are built around the cells found in the human brain. They create several connected layers by integrating many layers of interconnected neurons. A neural network might be useful for identifying photographs that include a single person's eyes, such as this one. The characteristics of iris recognition systems may vary depending on the varying colors, sizes, and forms of eyes, as well as the diverse lighting and backgrounds. It means we'll have to create a training package containing thousands of images featuring eye samples from the masses. This image then provides data to the neural network, which, in turn, helps neurons to communicate through synapses. In the end, all of this data is gathered to calculate the individual's identity. An iris is a membrane found beneath the cornea and is pierced by a circular hole called a pupil, which is governed by a sphincter and a dilator composed of smooth, radiant, and circular muscle fibers that are in direct opposition to each other. Using an optical system to only find macroscopic edges eliminates the ability to find microtubules. In the multicolored rings that surround each eye's pupil, the filaments, hollows, and streaks create a human bar code unique to each individual. In addition, these iridian imprints are hardly noticeable within the body. A neural network, known as multilayer perceptron's (6, 7), was initially described in 1940. In order to demonstrate that every function may be approximated arithmetically or logically, McCulloch and Pitts built multilayer perceptrons. The categorization of the XOR logic gate was hard, since perceptrons in 1969 could only make binary classifications. The re-propagation technique (as developed by David E Rumelhart et al. [8]) was completed in 1980. Geoff Hinton and a team of academic researchers from the University of Toronto, Canada, were able to solve the neural network optimization problem by identifying a new method that prevents it from being trapped in the local minima [9]. Picture editing on the PC became simpler with the arrival of GPUs, also known as graphics processing units (GPUs). This was previously done using supercomputers for image learning technology experimentation. A decade ago, Faye Leigh, a computer scientist at Stanford University, and Lee, a computer scientist at Princeton University, released ImageNet, a collection of pictures that was made up of millions of images that had been described by users. The LeNet character recognition neural network was developed by Yann LeCun and popularized by him as well. Gartem (arithmetic equation) machine learning methods were used to recognise faces in real-time photographs in 2001 by Paul Viola and Michael Jones of Mitsubishi Electric Research Laboratory in the United States. Instead of employing neurons of variable weights, such as if the image contains a light-colored point between the black sections, which may represent the tip of the nose, we apply the notion of passing photos via a succession of fundamental judgements. Are there two black patches, each surrounded by a large expanse of white? White skin with dark eyes and cheeks are common in black and white pictures. Mechanical Turk, an Amazon program that pays pennies every description of a photo, was used to describe images that were very difficult to explain. Now that CPU and graphics processor computing capacity has increased, Deep Learning [4] has gotten a lot more affordable. It has shown to be a useful tool in many situations, as shown by the results obtained, with specific regard to Krizhevsky's [11, 12] use of ImageNet 4 and Cifar 5 images. SVM is more effective when feature generators use image-pre-trained networks rather than expert features. Lagrange et al. [14] used superpixels and deep features to obtain strong mapping results in the Data Fusion Contest 2015 [15]. Convolutive convolutional neural networks were used for the development of this first method. Fully-convolutional networks (FCN) not only learn the semantics of individual pixels, but also learn spatial relationships, making them an excellent choice for mapping images. As a recent number of studies has revealed, fully convolutive neuron networks are effective in this situation, as outlined in the research paper written by Long et al. [18]. Classical classifier networks allow one to generate a vector of probabilities or heat maps representing the probability of separate classifications. Reducing the number of subpixels reduces the number of adjustments that must be made later on, resulting in fewer features being reworked. For example, subsampling [19] and layer expansion convolutive [20] have been proposed in an effort to save resolution. Convolutional auto-encoders are used by several machine learning models such as DeconvNet [22] and SegNet [23], both of which have a symmetrical architectural encoder/decoder. To this end, random Markov models, such as these two, were also examined [24,25]. To improve on the previous fundamental transfer of learning CNN, as well as new algorithms that combine a CNN with an RNN, researchers at Hassan et al. [26] created a model which is based on the visual attention concept.

3.2 SVM CLASSIFICATION

For the linearly separable case, SVMs determine the optimal hyperplane that separates the data set. For this purpose, linearly separable requires finding the pair (w, b) such that it correctly classifies the example vectors xi into two classes yi that is, for a hypothesis space given by a set of functions fw, f(xi) = sign (wT xi + b) the following restriction is imposed:

A good strategy for presenting the theory of SVM consists of recalling some aspects of the theory of conventional sets (which we will call concrete sets), and from there on there is an extension to SVM classes: ' A frequent DOtación has been implemented. en donde el signo DO means divided by. A concrete set is defined as a collection of elements that exist within a universe. So, if the universe consists of negative numbers less than 10:

U={O,1,2,3,4,5,6,7,8,9}

With these definitions we have established that each of the elements of the dataset does not belong to a certain class. Therefore, each set can be completely defined by a dependency, which operates on the elements of the universe, and which assigns a value of 1 if the element belongs to the dataset. Taking as an example the set C listed above, its udx) would be of the following form:

A={O, 2,4, 6, 8} B={l,3,5,7,9} C={l,4,7}

The first differences that are evident between SVM classification and linear classification are as follows:

A. The function of belonging associated with concrete sets can only have values: 1 or 0, but in dataset can have any value between 0 and 1.

B. An element can belong (partially) to a dataset and simultaneously (partially) belong to the complement of this set. Previously, it was not possible in concrete sets, which constituted a violation of the principle of exclusion.

C. The edges of a concrete set are accurate, while the edges of a class set are, precisely, the same class, since there are elements in the same borders, and these elements are in turn and together. What sense can it have to partially belong to a group? In many cases it may have more sense that it belongs to a whole. We see some examples:

Example 1: a hypothesis that is intended to define the set of students of the electrical engineering class at the Universidad Nacional de Colombia who are attending the fifth semester of the course. How can I classify a student studying the subjects of his fourth semester, three of fifth and one of sixth? Is there another one that takes a fifth semester and five sixth? Evidently both are part of the fifth semester student group, but only partially.

Example 2: a hypothesis that is intended to classify the members of a soccer team according to their stature in three sets, low, medium and high. It could be planted that if it is low if it has a stature less than, for example, 160 cm, that if it is average if its stature is greater than equal to 160 cm and less than 180 cm. and if the height is greater than 180 cm, as a result of which a classification would be achieved in concrete sets. No embargo. How big is the difference that exists between the players of the team, one with a height of 179.9 cm and another of 180.0 cm? This millimeter of difference between quizzes does not represent anything significant in practice, but without the classes of the players who have been labeled with distinct labels: one is average and the other is tall. If one chooses to perform the same classification with datasets, these abrupt changes would be avoided. due to the fact that the borders between them. When a SVM has an interlocking mechanism, it is said that it is an adaptive SVM system. The mechanisms of internment are algorithms that allow the system to change its design to adjust (these, to adapt) to some specific requirements. Generally speaking, the algorithms for design are only part of the SVM, generally the basis of classes, the definition of linguistic variables, and in some cases both. Other parameters must select the user. At a global level, these are one of the topics on which more is currently being investigated within topics of SVM. There are several algorithms and different strategies depending on the use that is giving us the SVM, what justifies this effort on a global level? There are at least less of the following reasons: First, are there some SVMs? They are universal approximators, if you decide, satisfying a property according to which it is known that any real function can still be approximated with the degree of precision that is desired by one of these approximators. This property is safe then the existence of a system of SVM with which it can be represented, as well as if it wanted, any function in the linear continues. However, even if it is known that such a system exists; do not use an exact procedure to find out how. In general, the training algorithms are logical procedures that try to design a system of SVM that approximates some unknown function.

3.3 GENETIC ALGORITHM

Three key issues affect optimization problems: a problem solving, a function that may maximize or minimize the size of solution spaces, and an issue related to implementation. A problem to solve may be seen as a black box with many dials and buttons. Each dial or button represents a parameter of the issue, and an output value that verifies whether a collection of solutions works to satisfy the objective function.

Slight differences between two samples collected from the same person with the same biometric trait can occur as a result of imaging conditions (e.g., sensor noise and dry fingers), variations in the user's anatomical or behavioral features (e.g., wounds and bruises on the finger), atmospheric conditions (e.g., temperature and humidity), and user contact (e.g., finger placement). Because of this, the biometric matching device provides the matching score (usually a single number) that represents the similarities between the input and prototype representations. To know for sure, you must be quite high in the rankings. When the threshold is crossed, the system has made a choice. When two biometric samples give scores higher than or equal to each other, it is assumed to be a pair of mates (two people who are each other's partner). In contrast, when two biometric samples give scores lower than each other, it is assumed to be a nonmate pair (two people who are not each other's partner) (i.e., belonging to different persons). The original distribution is shown in Fig. 2(a), whereas the imposter distribution is the distribution shown in Fig. 2(b).

Biometric authentication devices can generate two types of errors: 1) a false match, when two people's biometric measurements are confused as being the same (also known as a false match), and 2) a double match, when two different people's biometric measurements are mixed up (referred to as a double match) (called false nonmatch). One way to explain these two sorts of blunders is with the phrases "fake embrace" and "false denial." Between the false positive rates (FPR) and the false negative rates (FNR), a tradeoff exists (FNMR). While FNMR does rise as the system's tolerance to input fluctuation and noise is lowered, the opposite is true with FMR. In order to make the machine more stable, FNMR grows in parallel with increasing the on the opposite side.

To draw a ROC curve, the device's overall performance at all operating points is assessed (thresholds). A ROC curve is known as a plot of FMR against (1-FNMR).

A sensor module that contains biometric data collects the information of a person. As another example, a fingerprint sensor may provide a diagram that shows the curvature of a user's eye.

An extraction module that uses biometric data is used to pull out a set of identifiable or prejudiced features. For example, the position and orientation of the minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric device.

The Matcher module is sometimes called the feature comparator, and it does just what the name implies. It compares the features that were recorded during recognition to the models that were saved, in order to provide matching scores. To compute the matching minutiae and record a matching score, such as is done in the matching module of a fingerprint-based biometric device, the quantity of matching minutiae between the input and template fingerprint pictures is computed. Also known as the verification or identification module, the matcher module contains a decision making module that uses the matching score to check a user's claimed identity or to establish a user's identity.

The biometric machine stores the biometric models in the system storage module. The registration module handles registering individuals into the biometric framework database. To identify a person and ensure he or she is who he or she claims to be, a biometric reader captures the person's biometric feature, generating a digital picture of the feature. During the enrollment time, humans may or may not need to be involved in data collecting, depending on the application. In order to guarantee that the received sample can be handled properly during later steps, a consistency assessment is generally done. The digital representation (input) is processed using a function extractor in order to create a prototype which is then used to encourage matching.

These forms are used to maintain the information connected to the solution of the issue, and use a chromosomal technique and the application of selection and crossover operators. An ordinary GA project is considered a function optimizer, even if there are several applications of GA.

Unlike traditional search and optimization procedures, which often start with a single potential solution and are repeatedly altered by applying certain trial-and-error (dynamic) methods relevant to the issue to be addressed, search and optimization methods are just as conventional as the problem itself. These non-algorithmic, heuristic procedures are allowed, and the complexity of the simulation on computers may be high. While these techniques are not often used, this does not mean they are ineffective. However, they are often used, effectively, in a variety of settings.

One way to think about how evolutionary computing approaches function on a population of parallel candidates, is to consider it to be like natural selection in action. By designating a suitable number of members to search in numerous regions, they are better able to search in numerous sections of the solution space. The four major differences between standard search and optimization techniques and genetic algorithms are:

i. GAs operates with an encoding of the parameter set, they don't deal with the parameters that have been specified.

ii. Identifying individuals, not a single point, using GAs.

iii. With GAs, information about costs or rewards is used, as opposed to derivatives or any other additional knowledge.

iv. To support probabilistic and non-deterministic transitions, GAs employs probabilistic and non-deterministic transition classes. In conventional search techniques, many of the search modifications are made, therefore genetic algorithms have a high success rate for identifying optimum solutions and approximation answers to a broad range of problems.

They are able to uncover and examine environmental and convergent aspects for optimum or roughly ideal solutions, while keeping costs low.

According to this fundamental notion of biological genetic evolution, individuals that better adapt to their environment would have a higher chance of surviving and passing on their genes. It is also related to population genetic and genetic algorithms, which apply to the nearby biological location. Rather of calling AGs "genetics algorithms," researchers say "genetic algorithms" or "a genetic algorithm.

3.3.1 Basic Concept

Before analyzing the genetic algorithm principles, it is first important to provide some foundational principles, which may be explained organically while the genetic algorithm operates.

A. Chromosome (genotype) - a string of bits that may or may not solve the issue.

B. Gene - gene is a map of each parameter, using the corresponding letter (binary, integer or real).

C. The coded chromosome is known as the phenotypic.

D. Populace - collection of search points (individuals).

E. Generation, in its entirety, refers to a whole iteration of the AG that is capable of generating a new population.

F. Gross fitness, which is the goal function for a single person in the population, is the total output created.

G. The input to the selection algorithm is a normalized aptitude

H. Maximal fitness: the fitness of the maximum member of the existing population.

I. Average fitness – of the current population

While a solution point in the optimization problem corresponds to each chromosome, it should be emphasized that each chromosome corresponds to a solution point in the GA. To come up with a high number of people, referred to as population, which enables a thorough scan of the solution space, the solution process followed in genetic algorithms utilizes the generation of several populations, one of which is called a population.

3.3.2 GA Fundamentals

If we were to envision an initial population, consisting of random people, we might see them as potential answers to the issue. Each individual's capacity to adapt to various environments is taken into consideration throughout the evolutionary process.

The chosen few are the ones who survived, while the others were dismissed (Darwinism). The working idea of AGs is that, over time, the starting population will, via the application of selection criteria, yield more appropriate people. A good selection process selects people with better aptitude ratings, but not solely. The Roulette Method is one of the most popular selection techniques in use today. It is used when new generations are created by spinning a roulette wheel to pull people from a previous generation.

This strategy treats every person in the population according to their aptitude index (Figure 20). Because of this, the system distributes more of the roulette wheel to those with higher aptitude, and less chips to those with lower aptitude. Finally, the roulette wheel is spun many times to provide a set of individuals who will be the following generation. Memberships established in the selection may experience mutations and genetic recombination (crossover) or genetic recombination, resulting in future generations of offspring. Until a good answer is discovered, the process of reproduction is repeated.

The crossover operator ensures that parents' features are recombined to produce the following generation. The Pc crossover rate must be larger than the mutation rate in order for this operator to be used. The most commonly-used methods for this operator are:

A. Unmarked: at the intersection, one point is selected and then the parents' genetic information is passed from one to the other. Prior to this time, one parent is connected to the other by information, generalization: this concept refers to sharing genetic material through several crossing locations.

B. Uniform: calculates the chance of each variable being transferred between parents by a global parameter rather than using crossing points.

C. One or more components of a structure may be freely altered using the mutation operator to introduce new members to the population. This mutation is used to make it impossible for the chance of reaching any location in the search space to be zero, while also avoiding the issue of local minima when the search direction somewhat shifts.

The mutation operator is applied to people, and the chance of applying it is determined by the Pm mutation rate. This value is chosen to be modest to avoid frequent usage of the mutation operator.

These algorithms are complex enough to produce effective and resilient adaptive search engines, even if they may look basic from the biological point of view.

This process is performed several times. The genetic algorithm at the bottom shows a good example of a genetic algorithm. Efforts in this procedure should be made to ensure that the best persons as well as some data from the analysis are kept and saved for future use. This makes it difficult to find an effective solution, since the population gives just a limited range of the issue area. The greater the population, the more representative of the issue area the numbers are, and the less the chance of converging on solutions localized rather than global. Computational resources are necessary in order to operate with larger populations, and the algorithm must run for a significantly longer length of time.

The crossover rate New structures are introduced into the population the faster the greater this population growth rate. But if the limit is too high, high-skilled structures may be eliminated rapidly at a high value, but most of the people would be replaced. The slower the algorithm runs, the lower the value that may be returned.

Frequency of Mutation, In addition to not enabling a particular location to stagnate at a particular value, a low mutation rate also promotes rapid search space exploration. The search rate becomes quite high, resulting in searches that are effectively random. An inter-generational view, Reflects the number of individuals who will be replaced during the course of the next generation. Highly adept structures may be lost when the value is large. Low values result in sluggish algorithms.

4. PROPOSED METHOD

4.1 READING THE IRIS

Iris readers are the hardware (or in this case simulation of the hardware) responsible for capturing images of the human eye in biometric recognition systems based on iris recognition. They are responsible for image acquisition, subject identification, and final identity information. There are several brands on the market with these products, such as Panasonic, LG and OKI. Also, in the way they are used, there is a diversity, which can be fixed, mobile or private use systems.

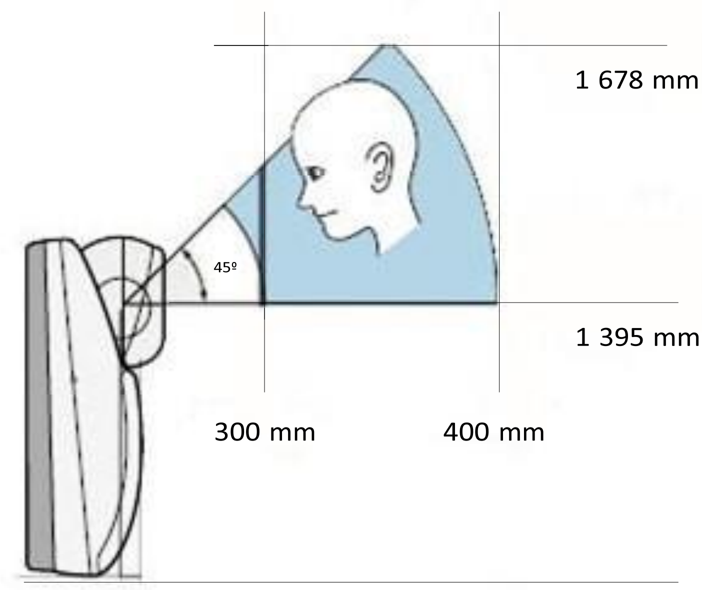

Figure 4.1 IRIS readers

Fixed iris recognition systems are usually located in a position that is easy for the user to cooperate with the iris reader a positional adjustment is necessary so that the captured image is as clear as possible. The iris reader has a proximity sensor that detects when a person is close and that only allows passage if the person under analysis has permissions to do so. You can then define three steps in the identification process: approach, capture and access. This type of systems is normally used, for example, in offices, laboratories, prisons and banks, where there is a need to ensure and restrict access to certain spaces. There is a central computer where communication is made between iris readers and users' databases. These devices are equipped with a camera and an infrared light illuminator, thus achieving better image quality. After capture, the system identifies the iris in the image and sends the final result. Voice commands assist the user if there is a need to approach, distance or in the event of an anomaly in capturing the image [25] [19]. Once the image capture phase is finished, the systems keep only the biometric signature that identifies people, never working with personal images, to also safeguard some legal issues about privacy. The recognition steps will be described in detail in the section. Mobile or portable iris readers are compact and manual devices and are normally used as a simple camera using the iris as a focus point. They may be connected to a computer or have internal memory included. They are normally used in military missions, in the navy, in the army and the like. It is also possible for the average user to protect personal computer data with an iris recognition system. It is a simple device similar.

4.2 ANATOMY OF THE EYE

Vision is one of the five senses of the human being. It is a very important perception for living beings and especially for Man, as it allows distinguishing things through images, including colors and the notion of depth. The eye consists of three layers: external, intermediate and internal. The outer layer acts as a protective layer of the eye, consisting of the cornea, the transparent part of the eye that functions as a lens, and the sclera, popularly called the "white part" of the eye. The middle layer comprises the iris, the choroid (or choroid) and the ciliary body. This layer is also called a vascular tunic. In the inner layer, the nerve layer, is the retina. The retina is made up of nerve cells and is responsible for transporting the image through the optic nerve for the brain to interpret. It can thus be said that it is not with the eyes that we visualize, but with the brain, which are responsible for capturing light and transmitting information to the brain [29]. Figure 4.2 shows the diagram of the human eye. The cornea slightly covers the iris and the pupil where the light passes, and with its sharp curvature it is the main means that makes the parallel rays, which come from the infinite, converge and reach the central fovea together. The iris, located between the cornea and the lens, is a circular and colored membrane with an opening in the center called the pupil, also known as the "apple of the eye", and its function is to control the entry of light into the eye. When exposed to luminosity, decreases its central opening, and likewise, when exposed to low light, it expands, increasing the size of the pupil. The lens is a lens, which, through its diopter variation, makes clear vision possible at all distances. When looking closely, the lens becomes convergent, increasing its refractive power and when looking away, it becomes less convergent, decreasing its diopter power [41].

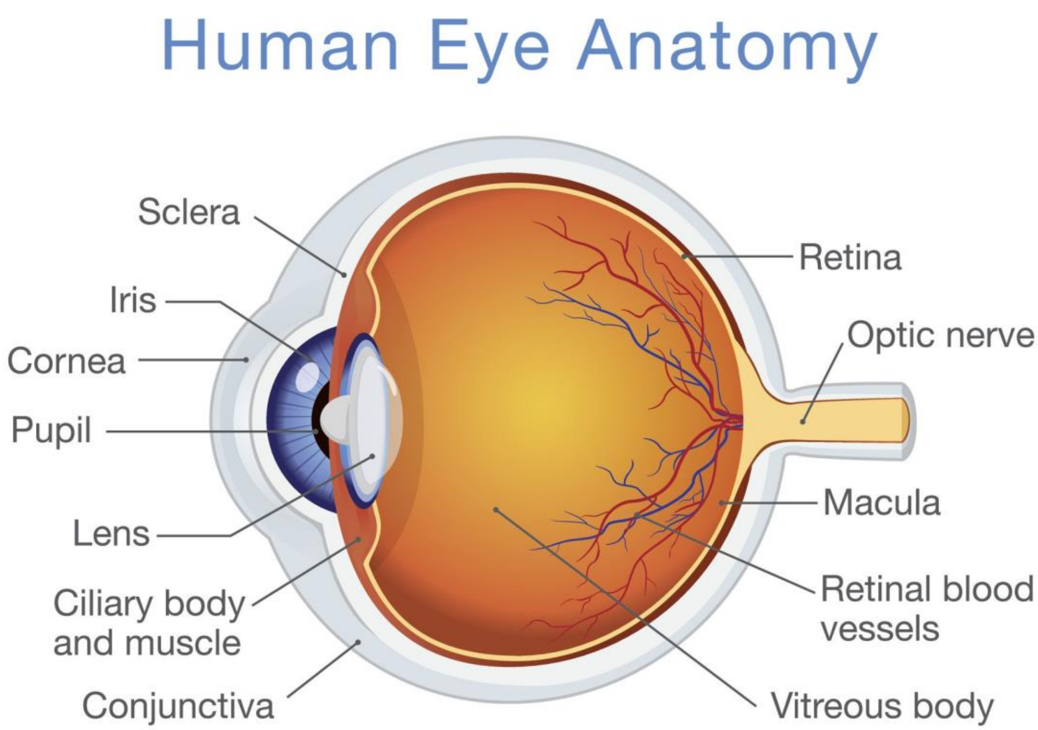

Figure 4.2 Anatomy of the human eye

The iris is the most visible part of the human eye and is the membrane responsible for controlling the amount of light that reaches the retina. You can then divide the iris into two parts: the smaller and larger ring the area of the smaller ring of the iris is the inner part bounded by the pupil boundary, the pupillary margin. In turn, the area of the larger ring comprises the region from its origin, the border with the sclera named in figure 2.6 by the ciliary margin, up to the area of the smaller ring. The section that delimits these two parts is called "iris folds". The iris begins to form from the third month of pregnancy. The structure is completed at eight months of gestation; however, pigmentation continues to be formed until the first year of life. Its color is given through the type and amount of pigments in the iris tissue, with blue being the color with less pigmentation [30]. The iris, being an internal part of the eye but visible from the outside, is well protected and is stable over time. Its complex texture can contain several characteristics such as curvatures, grooves, rings, circles and spots. This complexity contributes to the iris becoming one of the best methods for biometric purposes.

4.3 IRIS DETECTION

After dividing the iris into its internal and exterior borders, the image location in the polar coordinate system is obtained. Because pupil size and image capture distance are not variable, a picture of the iris is obtainable that is unaffected by image capture distance.

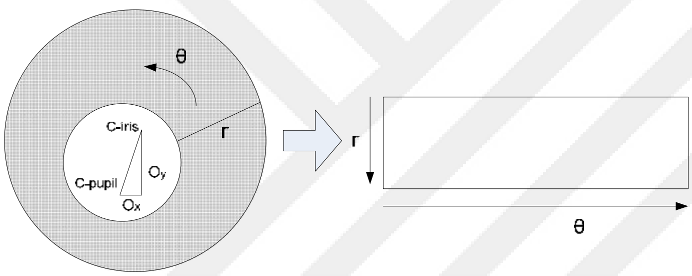

Figure 4.3 IRIS normalization

In this concept, every location in the iris corresponds to a pair of coordinates (r, θ) where r ranges from 0 to 1 and θ ranges from 0 to 2π. A common method of rendering the iris using Image Mapping is to apply Cartesian coordinates (x, y) to non-concentric polar coordinates (r, θ):

$$I\big(x(r,\theta), y(r,\theta)\big) \rightarrow \ I(r,\theta) \ldots (4.1)$$

Linear combinations of both sets of points around the outer perimeter of the iris (xp (θ), yp (θ)) in the segmentation step provide (x, y):

$$x(r,\theta) = \ (1 - \ r)xp(\theta) + \ rxs(\theta) \ldots (4.2)$$

The thing to look for while analyzing the iris is locating the border with the pupil, which is often often referred to as “girl's eye. If pupil segmentation is good, you have a better chance of detecting the boundary with the sclera. This suggested technique uses Wildes' segmentation processes as a clear reference. Pre-processing procedures are applied to the acquired picture, and the LoG edge detector produces the binary edge map. The Randomized Hough Transform has now been used to recognize geometric forms (RHT). When used to Hough transforms, RHT may reduce the number of parameters needed to parameterize a curve.

4.3.1 Feature extraction Using Genetic Algorithm

Biometric signatures are created at the feature extraction step by applying the attributes of the iris to it. The iris structure is characterized by many intricate and varied textures, which may be used to encode the iris. Additionally, we will discuss the most popular feature extraction techniques in this part. The iris's varied textures are found in high concentrations inside the structure. As a result of all of this intricacy and quantity, it is possible to extract the iris' unique features and employ them in the encoding process. This method makes use of the Daubechies family of wavelets for decomposition. The results of Poursaberi et al. [37] are in data mining operations, while many learning algorithms work on finite spaces of discrete or nominal qualities, the objective is to reduce the cardinality of the continuous characteristics in a database. Discretizing continuous properties is beneficial when the range of values is unlimited. The GA was created to divide continuous attributes into goodness intervals in order to assign the maximum possible goodness value to all the intervals in the same way, so that the average goodness of all the final intervals for a particular attribute will be what is ideal, that is, it encompasses the maximum possible number of examples while leaving a good amount of the attribute intact.

4.3.2 Classification Using SVM

To create the art, the eye's iris picture, in full color, was digitally processed and enlarged to include the whole eye. In the beginning, the standard supervised classification process was used, with MAXLIKE a software module utilized as the "hard" classifier. It categorizes a picture based on the data that is stored in a collection of spectral signatures (training samples) (uses and covers without mixtures). Polygons are drawn on the picture, which is understood to indicate that these samples are made digitally from them. For example, samples from the enlarged, thin, and regular pupils are used for training. This will thereafter be referred to as a "soft" classification system, which classifies training samples according to their usage and coverage. More information will be provided below.

Applying the first technique, which uses a "hard" classifier, required the following steps:

A. This particular sub-picture is taken out of the original picture. Once the 1, 2, and 3 bands are removed, the color picture is built from the sub-picture.

B. The picture is visually inspected, and class types and locations are defined. Locations are set up for each class type. For this project, we researched forest types that include thick forest, sparse forest, and urban use.

C. To provide high-quality training for our employees, we developed training locations employing the on-screen digitizer.

D. A class or signature is established.

E. Finally, we continue to classify the usage and iris picture using an automated system.

F. After the specified technique is finished, fuzzy signatures are used to finish the supervised categorization.

A. The first stage is to identify the known applications and coverings in the research region (without mixtures and mixes). When viewed from this angle, the picture is MDA

B. In order to represent the usage and coverage for the classes as precisely as possible, they are allocated percentages of SVM function equivalent to each class. For example, on non-mixed locations, the appropriate class is the only thing which will be used, but on mixed locations, if the site includes both non-pure mixes, the corresponding percentages of each class will be used to get that level of coverage. To summarize, by using the aforementioned information, the SVM partition matrix is now prepared, where uses and coverage are listed beside each other with the proportion of each covered and used. The diagram above shows the mechanism of IRIS recognition in additional detail:

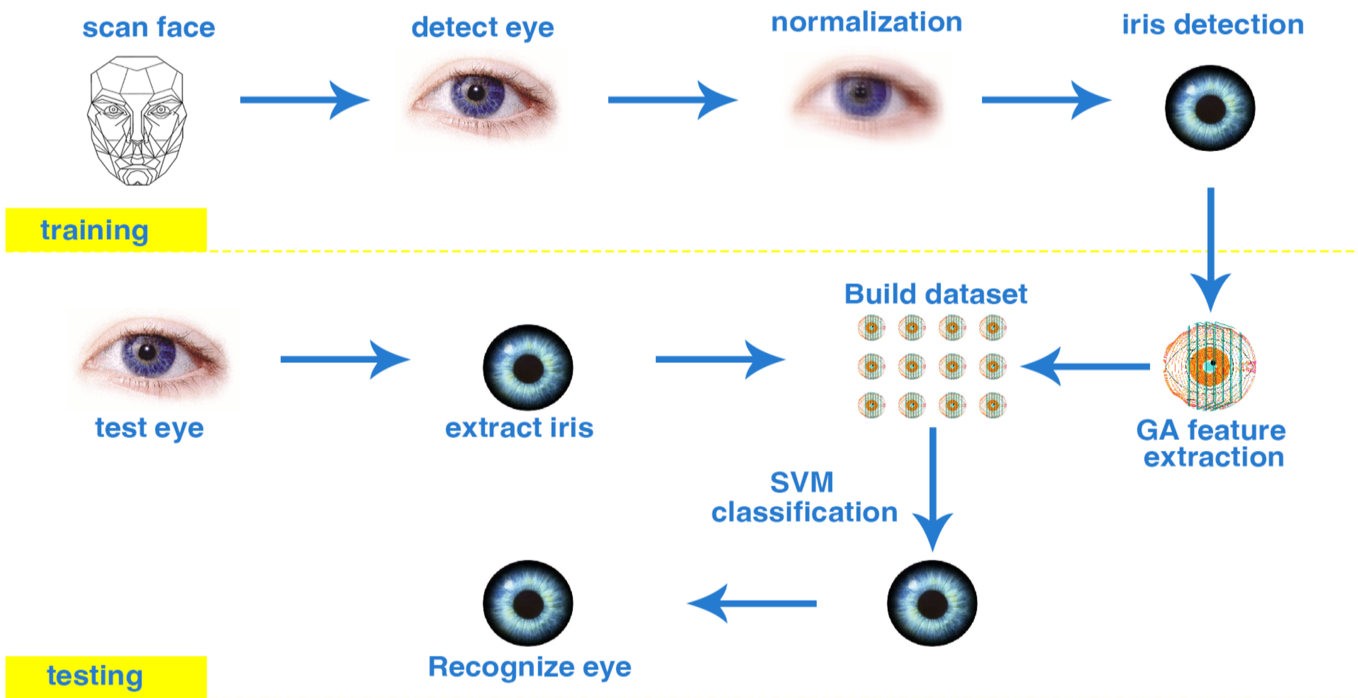

Figure 4.4 Proposed method

Canonical hyperplanes are known as hyperplanes that meet (1). SVM's goal is to discover the single canonical hyperplane (a.k.a. decision boundary) that properly classifies all of the training data, which is known as "minimizing || w || 2." Reducing w2 to find the hyperplane that maximizes the distance between two convex envelopes is similar to finding the separating hyperplane for which the distance between two convex envelopes (two classes of the training data set) is maximized. The edge is 25 miles away.

5. SIMULATION AND RESULTS

The use of the theory of Support Vector Machines (SVM) shows that the findings of the geographic space identified are more accurate. This is due to the fact that from IRIS image classifications, a product provides information about the many uses and coverage regions with mixed classes, which allows you to develop better-quality maps or to provide a wider choice of applications and coverage regions. Table 5.1 below summarizes the attributes of the dataset that was used:

Table 5.1 Properties of the datasets

Property	HMT-IRIS v2	ILTD -IRIS
No. of Classes	342	224
Image size	240*240	240*240
File format	BMP	PNG
No. of images	2025	3246

This suggested GA helps us determine if our eye is recognized, but it also informs us of what variables and features we must change in order to achieve our goal. Also, while making decisions, the support of the categorization classes is used. In contrast, while looking at the 2nd GA, we see that there is a trade-off between the profit it adds and the instances that are NOT categorized, meaning that the coverage decreases as the accuracy gain grows. This chart illustrates the SVM's accuracy when compared to other classification algorithms:

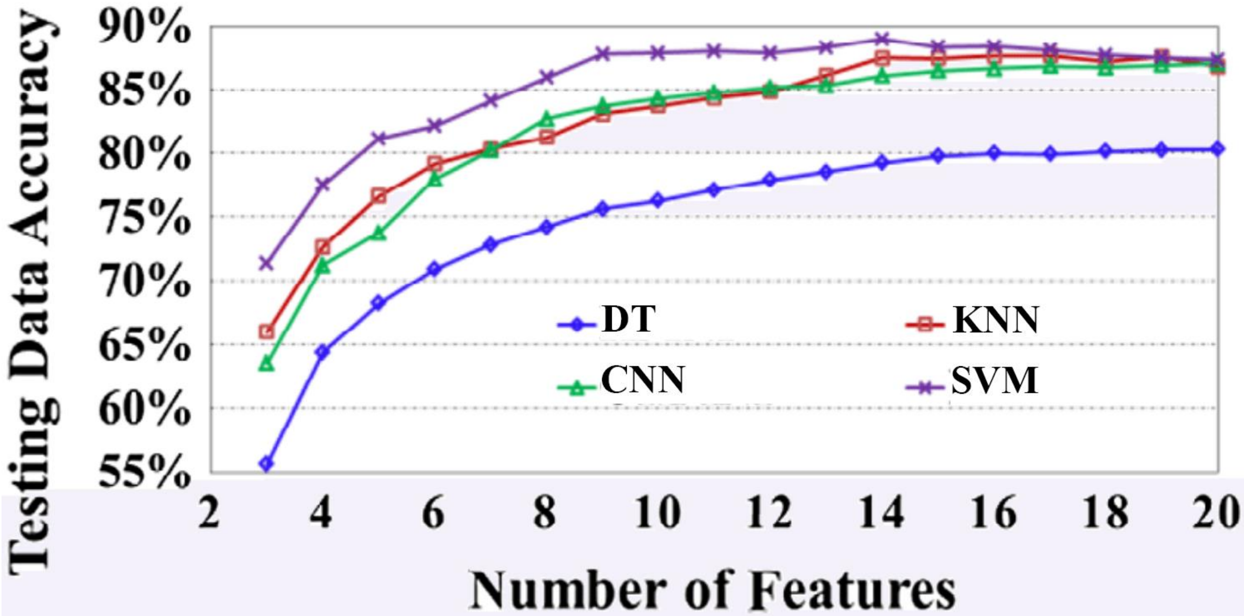

Figure 5.1 SVM accuracy compared to other methods of classification.

If the maps created demonstrate that the uses and coverage don't have exact bounds, then apply this strategy. This approach is excellent for identifying several kinds of plants in the forest, since the many species are intermingled or in the process of transition, and display distinct spectral reflectance.

The working scales will be dependent on the object of study and the extent of the iris area, i.e., if the iris area is expansive, the appropriate working scale may be biometric images taken directly from hardware devices. In the classification of IRIS pictures, the SVM theory may be used at several different levels of labor, and there are no disadvantages to this.

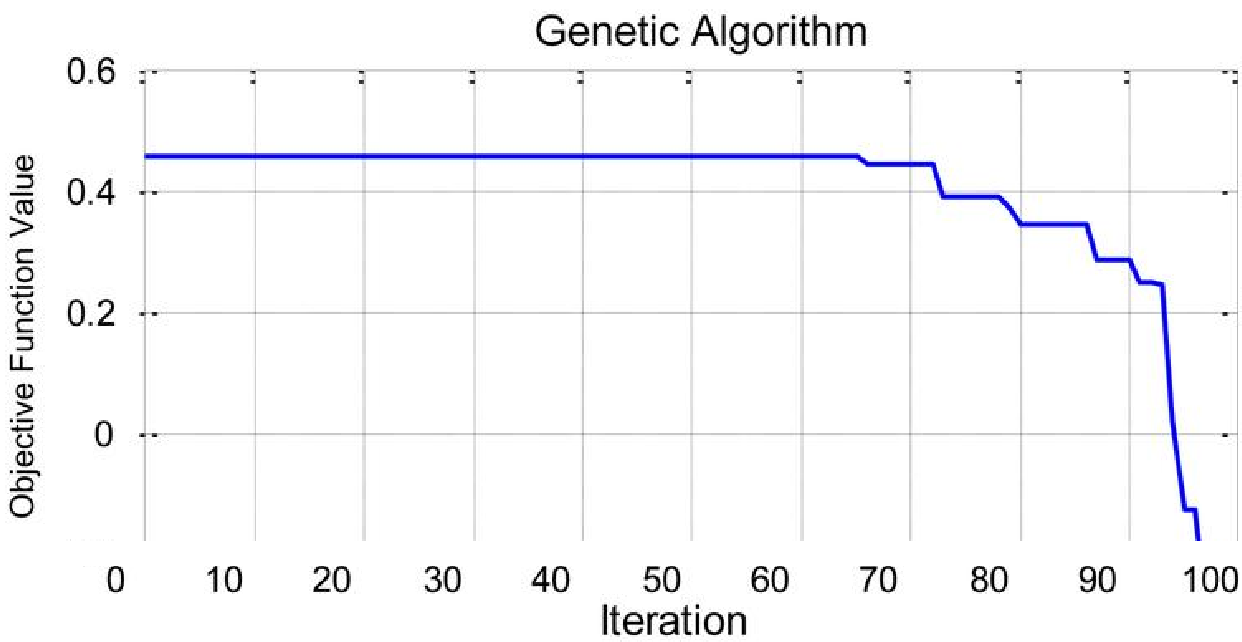

Figure 5.2 MSE of genetic algorithm feature extraction

The table below shows a comparison of some of the methods in the literature:

Table 5.2 Comparing our proposed method in terms of error rate and accuracy in recognition

Method	MSE	ACC
Valetco et.al	0.342	74.63
Mascerenhas et.al	1.453	89.65
Bondy et.al	0.974	91.64
Pauca et.al	0.764	84.65
Viola et.al	0.873	88.54
Proposed	0.257	94.01

6. CONCLUSION

One of the fast-growing fields in biometrics is the subject of behavioral biometrics, and this has been thoroughly examined, researched, and researched. This makes clear that and because the iris is one of the human features with superior circumstances for biometric implementation, this thesis is concerned with formulating the procedures and recommending novel implementations. Due to the extensive existing literature, of course.

Also critical is the perception of each level of iris recognition, as well as the techniques to overcome each problem. Here, we aimed to showcase cooperative iris recognition system implementation alternatives.

Consider, for example, the findings shown in Section 4. The findings indicate that test sets with pictures with noise (such as low-quality photos) provide different results than test sets with pictures without noise (such snapshots of clear skies). In other words, collaboration during the capture phase is very vital to consider.

Because it is important in distinguishing the iris, it was apparent that the segmentation phase is one of the most discussed phases in the literature. Because of effective segmentation, the remaining tasks are advantageous in light of matching findings, and more beneficial system performance.

We predict that in the future we will be able to use a supervised deep learning approach for boundary detection and snake algorithms to provide the edge of the IRIS, as well as use LIDAR for scanning the IRIS for improved accuracy.

REFERENCES

[1] Commission Int'l de l'Eclarirage, "Photobiological Safety Standards for Safety Standards for Lamps," Report of TC 6-38; CIE 134-3-99, 1999.

[2] D. H. Brainard and B. A. Wandell, "Analysis of the retinex theory of color vision," J. Opt. Soc. Am. A:, vol.3, no. 10, pp.1651–1661, 1986

[3] Štruc V. and Pavešić N., "Performance Evaluation of Photometric Normalization Techniques for Illumination Invariant Face Recognition," in Advances in Face Image Analysis: Techniques and Technologies, Y.J. Zhang (Ed.), IGI Global.

[4] Štruc V. and Pavešić N., "Gabor-Based Kernel Partial-Least-Squares Discrimination Features for Face Recognition," Informatica (Vilnius), vol. 20, no. 1, pp.115–138, 2009.

[5] L. Grady, "Random Walks for Image Segmentation," IEEE Trans. Pattern Anal. Mach. Intell., vol.28, no.11, pp. 1768–1783, 2006.

[6] J.A. Bondy and U.S.R. Murty, Graph Theory. Springer, 2008.

[7] M. Sonka, V. Hlavac and R. Boyle, Image Processing, Analysis & and Machine Vision, Thomson, pp. 144–146, 2008.

[8] G. Bradski, "The OpenCV Library," Dr. Dobb's Journal of Software Tools, 2000.

[9] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," Proc. CVPR 2001, no., pp. 511–518, 2001.

[10] Face Recognition Grand Challenge – Overview. http://www.frvt.org/FRGC/.

[11] P. Phillips, P. Flynn, T. Scruggs, K. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W.Worek, "Overview of the face recognition grand challenge," in Computer Vision and Pattern Recognition, 2005. CVPR 2005. 2005.

[12] Biometrics Ideal Test. http://biometrics.idealtest.org/dbDetailForUser.do?id=4.

[13] Ground truth masks for iris segmentation. http://www.comp.polyu.edu.hk/~csajaykr/myhome/research/GT.zip.

[14] Johanson, "Mean shift: A feature space analysis robust approach toward feature space analysis IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, pp. 603–619, 2013.

[15] V. Vezhnevets and V. Konouchine, "Grow-Cut - Interactive Multi-Label N-D Image Segmentation," Proc. Graphicon, pp. 150–156, 2005.

[16] D. L. Woodard, S. Pundlik, P. Miller, R. Jillela, and A. Ross, “On the Fusion of Periocular and Iris Biometrics in Non-ideal Imagery,” Proc. Intl. Conf. Pattern Recognition, ICPR 2010, Istanbul (Turkey), pp.201-204, 2010.

[17] S. Bharadwaj, H.S. Bhatt, M. Vatsa, and R. Singh, “Periocular biometrics: When iris recognition fails,” Proc. BTAS 2010, pp.1–6, 2010.

[18] U. Park, R. R. Jillela, A. Ross, and A. K. Jain, “Periocular biometrics in the visible spectrum,” IEEE Trans. Info. Forensics & Security,vol. 6, no. 1, pp. 96– 106, 2011.

[19] R.M da Costa and A. Gonzaga, “Dynamic Features for Iris Recognition,” IEEE Trans. Syst. Man Cybern. Part B Cybern., vol. X, no. X, pp.1–11, 2012. (available online)

[20] V. P. Pauca, M. Forkin, X. Xu, R. Plemmons and A. Ross, “Challenging Ocular Image Recognition,” Proc. of SPIE (Biometric Technology for Human Identification VIII), vol. 8029 80291V-1 – 80291V-13,2011.

[21] Oliva and A. Torralba, “Modeling the Shape of the Scene: A Holistic Representation of the Spatial Envelope,” International Journal of Computer Vision, vol. 42, no. 3, pp. 145–175, 2001.

[22] T. Leung and J. Malik, “Representing and recognizing the visual appearance of materials using three-dimensional textons,” International Journal of Computer Vision, vol. 43, no. 1, pp. 29–44, 2001.

[23] D. G. Lowe, “Distinctive image features from scale-invariant keypoints,” International Journal of Computer Vision,vol. 60, pp. 91–110, 2004.

[24] VLFeat: An Open and Portable Library of Computer Vision Algorithms. http://www.vlfeat.org/.

[25] T. Ojala, M. Pietikainen and T. Maenpaa, “Multiresolution gray-scale and rotation invariant texture classification with local binary patterns,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 971–987, 2002.

[26] N. Dalal, B. Triggs, “Histograms of oriented gradients for human detection,” Proc. CVPR 2005, pp.886–893, 2005.

[27] E. d. Os, H. Jongebloed, A. Stijsiger, and L. Boves, “Speaker Verification as a User-Friendly Access for the Visually Impaired”, Proc. of the European Conference on Speech Technology, pp. 1263-1266, Budapest, 1999.

[28] Eriksson and P. Wretling, “How Flexible is the Human Voice? A Case Study of Mimicry”, Proc. of the European Conference on Speech Technology, pp. 1043-1046, Rhodes, 1997.

[29] Andreu and Rinnhofer, Suspect Documents, Their Scientific Examination, Nelson-Hall Publishers, 2003.

[30] D. A. Funt, “Forgery Above a Genuine Signature”, Journal of Criminal Law, Criminology and Police Science, Vol.50, pp. 585-590, 1962.

[31] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of Artificial Gummy Fingers on Fingerprint Systems”, Proc. SPIE, Vol. 4677, pp. 275-289, San Jose, USA, Feb 2002.

[32] L. Hong, A. K. Jain, and S. Pankanti, “Can Multibiometrics Improve Performance?”, Proc. AutoID'99, pp. 59-64, Summit(NJ), USA, Oct 1999.

[33] Funt, “Integrating Faces and Fingerprints for Personal Identification”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, pp. 1295-1307, Dec 1998.

[34] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, “Is Independence Good for Combining Classifiers?”, Proc. International Conference on Pattern Recognition (ICPR), Vol. 2, pp. 168-171, Barcelona, Spain, 2001.

[35] Sobel Som and S. Ivanon, “The Voting as a Way to Increase the Decision Reliability. Foundations of Information/Decision Fusion with Applications to Engineering Problems, pp. 206-210, Washington D.C., USA, August 1996.

[36] R. Brunelli and D. F alavigna, “Person Identification Using Multiple Cues”, IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol. 12, No. 10, pp. 955-966, Oct 1995.

[37] E. S. Oja, J. Bigun, B. Duc, and S. Fischer, “Expert Conciliation for Multimodal Person Authentication Systems using Bayesian Statistics”, Proc. International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA), pp. 291-300, CransMontana, Switzerland, March 2000.

[38] Grundberg and Grönlund “Bioid: A Multimodal Biometric Identification System”, IEEE Computer, Vol. 33, No. 2, pp. 64- 68, 2012.

[39] Wells, Som, “Decision Combination in Multiple Classifier Systems”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 16, No. 1, pp. 66- 75, January 1994.

[40] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, “On Combining Classifiers”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 3, pp. 226-239, Mar 1998.

[41] S. Prabhakar and A. K. Jain, “Decision-level Fusion in Fingerprint Verification”, Pattern Recognition, Vol. 35, No. 4, pp. 861-874, 2002.

[42] U. Dieckmann, P. Plankensteiner, and T. Wagner, “Sesam: A Biometric Person Identification System Using Sensor Fusion”, Pattern Recognition Letters, Vol. 18, No. 9, pp. 827-833, 1997.

[43] P. Verlinde and G. Cholet, “Comparing Decision Fusion Paradigms Using k-NN Based Classifiers, Decision Trees and Logistic Regression in a Multi-Modal Identity Verification Application”, International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA), pp. 188-193, Washington D.C., USA, March 1999.

[44] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, “Fusion of Face and Speech Data for Person Identity Verification”, Research Paper IDIAP-RR 99-03, IDIAP, CP 592, 1920 Martigny, Switzerland, Jan 1999.

[45]] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2020: Fingerprint Verification Competition”, Proc. International Conference on Pattern Recognition (ICPR), pp. 744-747, Quebec City, Canada, August 2019.

[46] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies”, International Journal of Image and Graphics, Vol. 1, No. 1, pp. 93-113, 2017.

[47] United Kingdom Biometric Work Group (UKBWG), “Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01”, August 2002, Available from http://www.cesg.gov.uk/technology/biometrics

[48] R. Cappelli, D. Maio and D. Maltoni, “Indexing Fingerprint Databases for Efficient 1:N Matching”, Proc. International Conference on Control Automation Robotics and Vision (6th), 2019.

[49] M. Golfarelli, D. Maio and D. Maltoni, “On The Error-Reject tradeoff in Biometric Verification Systems”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.19, No.7, pp. 786-796, July 2017.

[50] K. Jain and A. Ross, “Learning User-specific Parameters in a Multibiometric System”, Proc. International Conference on Image Processing (ICIP), Rochester, New York, September 22-25, 2002.

[51] J. Clark and A. Yuille, Data Fusion for Sensory Information Processing Systems, Kluwer Academic Publishers, Boston, 2010.

[52] D. Zhang and W. Shu, “Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching”, Pattern Recognition, Vol. 32, No. 4, pp. 691-702, 2016.

[53] Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, “Personal Verification using Palmprint and Hand Geometry Biometric”, 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, June 9-11, 2013.

[54] P.J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, “FRVT 2002: Overview and Summary”, available from http://www.frvt.org/FRVT2002/ documents.htm.

[55] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2012: Fingerprint Verification Competition”, Proc. International Conference on Pattern Recognition (ICPR), pp. 744-747, Quebec City, Canada, August 2012.

[56] J. L. Wayman, “Fundamentals of Biometric Authentication Technologies”, International Journal of Image and Graphics, Vol. 1, No. 1, pp. 93-113, 2011.

[57] United Kingdom Biometric Work Group (UKBWG), “Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01”, August 2002, Available from http://www.cesg.gov.uk/technology/biometrics/.

[58] R. Cappelli, D. Maio and D. Maltoni, “Indexing Fingerprint Databases for Efficient 1:N Matching”, Proc. International Conference on Control Automation Robotics and Vision (6th), 2019.

[59] M. Golfarelli, D. Maio and D. Maltoni, “On The Error-Reject tradeoff in Biometric Verification Systems”, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.19, No.7, pp. 786-796, July 1997.

[60] K. Jain and A. Ross, “Learning User-specific Parameters in a Multibiometric System”, Proc. International Conference on Image Processing (ICIP), Rochester, New York, September 22-25, 2002.

[61] J. Clark and A. Yuille, Data Fusion for Sensory Information Processing Systems, Kluwer Academic Publishers, Boston, 2010.

[62] D. Zhang and W. Shu, “Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching”, Pattern Recognition, Vol. 32, No. 4, pp. 691-702, 2019.

[63] Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, “Personal Verification using Palmprint and Hand Geometry Biometric”, 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, June 9-11, 2013.

[64] P.J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, “FRVT 2002: DeepFace”, available from http://www.frvt.org/FRVT2002/ documents.htm.

[65] Quanzeng You, Hailin Jin, Zhaowen Wang, Chen Fang, and Jiebo Luo. Image captioning with semantic attention the LFW benchmark. In IEEE conference on computer vision and pattern recognition, pages 4651–4659, 2016.

[66] Matthew D Zeiler and Rob Fergus. Deep Hidden IDentity Visualizing and understanding convolutional networks. In European conference on computer vision. Springer, 2014.

[67] Sun Simonyan and Andrew Zisserman. Very DeepId2 convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014.

[68] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. CASIA-Iris-1000 Database for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 770–778, 2016.

[69] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. Going deeper with convolutions. UBIRIS.v2 In IEEE conference on computer vision and pattern recognition, 2015.

[70] Andrew G Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam. Mobilenets: IIT Delhi Iris Dataset. arXiv preprint arXiv:1704.04861, 2017.

[71] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. Densely connected convolutional networks. ND Datasets: ND-CrossSensor-Iris-2013 In IEEE conference on computer vision and pattern recognition, pages 4700–4708, 2017.

[72] David E Rumelhart, Geoffrey E Hinton, Ronald J Williams, et al. The Mobile Iris Challenge Evaluation (MICHE), 5(3):1, 1988.

[73] Minaee et.al http://colah.github.io/posts/ 2015-08-Understanding-LSTMs/.

[74] Pascal Vincent, Hugo Larochelle, Isabelle Lajoie, Yoshua Bengio, and Pierre Manzagol. VGGNet Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. Journal of machine learning research, 11(Dec):3371–3408, 2010.

[75] Gangwar and Joshi. Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114, 2013. 75. https://github.com/hindupuravinash/the-gan-zoo.

[76] Baqar ahmed, Jiani Hu, and Jun Guo. In defense of sparsity based face recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition, pages 399–406, 2013.

[77] Zhao and Kumar. Similarity metric learning for face recognition. In Proceedings of the IEEE International Conference on Computer Vision, pages 2408–2415, 2013.

APPENDIX OF ALL THE CODES USED IN THIS WORK

```
      function [z] = GOASwarmDistance(m, X)

          % Calculate Distance Matrix
          g=reshape(m,3,4)'; % create a swarm center matrix
          d = pdist2(X, g); % create a distance matrix of each data
points in input

          % Assign swarms and Find Closest Distances
          [dmin, ind] = min(d, [], 2);
          % ind value gives the swarm number assigned for the input =
[(s1*s2)x1]

          % Sum of Within-swarm Distance
          WCD = sum(dmin);

          z=WCD; % fitness function contain sum of each data point to
their corresponding center value set (aim to get it minimum)
          % z = [1 x 1]
      end
      clc;
      clear;
      close all;

      %% input images and read pixel intensity or gravity (first
element)
      folder = 'C:\Users\JZ\Desktop\nasrallah\practical\STARE';
      myImages = imageSet(folder);
      for f=1:40;
      img = read(myImages,f);
      [s1,s2,s3]=size(img);
      Rplane = img(:,:,1);
      Gplane = img(:,:,2);
      Bplane = img(:,:,3);
      X1 = (Rplane-min(Rplane(:)))/(max(Rplane(:))-min(Rplane(:)));
      X2 = (Gplane-min(Gplane(:)))/(max(Gplane(:))-min(Gplane(:)));
      X3 = (Bplane-min(Bplane(:)))/(max(Bplane(:))-min(Bplane(:)));
      % taking R-plane, B-plane, G-plane values as features
      X = [X1(:) X2(:) X3(:)];
      k = 4; % initial no. of swarms (each pixel will be a singe
insect then they will be assigned to swarms just like in image
segmentation)

      DistanceFunction=@(m) GOASwarmDistance(m, X);     % Distance
(second element)

      VarSize=[k size(X,2)];
      nVar=prod(VarSize);

      VarMin= repmat(min(X),1,k);      % Lower Bound of Variables
```

```
[4x1] of[1x3] = [4x3]
      VarMax= repmat(max(X),1,k);      % Upper Bound of Variables
[4x1] of[1x3] = [4x3]

      goa_opts =
optimoptions('grasshopperswarm','display','iter','MaxTime',600);
      [centers, err_ga] = particleswarm(DistanceFunction,
nVar,VarMin,VarMax,goa_opts);


      m=centers; % wind ( thrid element) each center will draw the
nearby insects and form a swarm

          % Calculate Distance Matrix
          g=reshape(m,3,4)';
          d = pdist2(X, g);

          % Assign swarm
          [dmin, ind] = min(d, [], 2);
          % ind value gives the cluster number assigned for the input
= [(s1*s2)x1]
          WCD = sum(dmin);

          z=WCD; % fitness function contain sum of each data point to
their corresponding center value set (aim to get it minimum)
          % z = [1 x 1]

      outimg=reshape(ind,s1,s2);

          for i=1:s1
              for j=1:s2
                  if outimg(i,j)== 1
                      outimg(i,j)= 0;
                  elseif outimg(i,j)== 2
                      outimg(i,j)= 85;
                  elseif outimg(i,j)== 3
                      outimg(i,j)= 170;
                  elseif outimg(i,j)== 4
                      outimg(i,j)= 255;
                  end
              end
          end
          figure;imshow(uint8(outimg));
      end
      clc;
      clear;
      close all;

      %% Problem Definition

      X = [1 1.5;2 2.5;3 3.5;1 1.5;2 2.5;3 3.5;1 1.5;2 2.5;3 3.5;1
```

```
1.5;2 2.5;3 3.5;1 1.5;2 2.5;3 3.5]; % [15x2]
      k = 3; % no. of clusters

      CostFunction=@(m) ClusteringCost(m, X);     % Cost Function m =
[3x2] cluster centers

      VarSize=[k size(X,2)];  % Decision Variables Matrix Size = [3
2]

      nVar=prod(VarSize);     % Number of Decision Variables = 6

      VarMin= repmat(min(X),1,k);      % Lower Bound of Variables
[3x1] of[1x2] = [3x2]
      VarMax= repmat(max(X),1,k);      % Upper Bound of Variables
[3x1] of[1x2] = [3x2]

      % Setting the Genetic Algorithms

      ga_opts = gaoptimset('display','iter');

      % running the genetic algorithm with desired options
      [centers, err_ga] = ga(CostFunction,
nVar,[],[],[],[],VarMin,VarMax,[],[],ga_opts);


      m=centers;

          g=reshape(m,2,3)'; % create a cluster center
matrix(3(clusters) points in 2(features) dim plane)=[3x2]
          d = pdist2(X, g); % create a distance matrix of each data
points in input to each centers = [15x3]

          % Assign Clusters and Find Closest Distances
          [dmin, ind] = min(d, [], 2)
          % ind value gives the cluster number assigned for the input
= [15x1]

          % Sum of Within-Cluster Distance
          WCD = sum(dmin);

          z=WCD; % fitness function contain sum of each data point to
their corresponding center value set (aim to get it minimum)
          % z = [1(inputs combinations) x 1]
```