PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

Ministry of Higher Education and Scientific Research

Echahid Hamma Lakhdar University of El-Oued

FACULTY OF TECHNOLOGIES

DEPARTMENT OF ELECTRICAL ENGINEERING

FINAL STUDY DISSERTATION

In the aim obtaining of

MASTER DEGREE

Domain:Sciences and Technology

Option: Telecommunication

Specialty: Systems of communications

THEME

KINSHIP VERIFICATION BASED ON LOCAL BINARY PATTERN FEATURES

Presented by:

- BELOUL Mohammed Nadjib
- BOUGHEZALA Mohammed Faissal
- MECHRI Ismail
- TEDJANI Noureddin

Framed by:

- Dr.TEDJANI Amina

Academic year :2021/2022

بسم الله الرحمن الرحيم

﴿ رَبَّنَا لاَ تُؤَاخِذْنَا إِن نَّسِينَا أَوْ أَخْطَأْنَا رَبَّنَا وَلاَ تَحْمِلْ عَلَيْنَا إِصْرًا كَمَا حَمَلْتَهُ عَلَى الَّذِينَ مِن قَبْلِنَا رَبَّنَا وَلاَ تُحَمِّلْنَا مَا لاَ طَاقَةَ لَنَا بِهِ وَاعْفُ عَنَّا وَاغْفِرْ لَنَا وَارْحَمْنَا أَنتَ مَوْلاَنَا فَانصُرْنَا عَلَى الْقَوْمِ الْكَافِرِينَ﴾ **سورة البقرة : الآية286 .**

" صدق الله العظيم"

ACKNOWLEDGEMENTS

First of all, I thank Almighty God -ALLAH- for giving me courage and patience during all these years of study.

I would like to express my gratitude and sincere thanks to Mr.

Dr: HETTIRI Massoud and Dr: TEDJANI Amina, Doctor at EchahidHammaLakhdard'ElOued University, for directing this work.

My sincere thanks to the members of the jury for the honor they do me by participating in the judgment of this work.

We would like to sincerely thank all those who have helped us to elaborate and carry out this dissertation, as well as to all those who have helped us directly or indirectly to accomplish this work.

Finally, I especially thank my parents for their unconditional support throughout these long years of study.

DEDICATION

I dedicate this modest work:

To my very dear parents who supported me throughout my studies.

To my very dear sisters and to my great family.

All my friends.

To all those who love me and whom I love

To you.

Abstract

Résumé

الملخص

Abstract

Kinship Verification via facial images is an emerging research topic in the field of biometrics, pattern relations have certain similarities in their facial appearances. These similarities in the facial appearance are a result of inherited facial features from one generation to next generation, especially from parents to children.

In This work aims to learn the effect of extracted facial features between pair of facial images to perform Kinship Verification. In our study we proposed Local Binary Pattern (LBP) for face representation. we performed kinship verification experiments on the challenging KinFace W-II.

IndexTerms Biometrics, Kinship Verification, local binary pattern, feature extraction and feature Classification

Résumé

La vérification de la parenté via des images faciales est un sujet de recherche émergent dans le domaine de la biométrie, les relations de modèle présentent certaines similitudes dans leurs apparences faciales. Ces similitudes dans l'apparence du visage sont le résultat de caractéristiques faciales héritées d'une génération à l'autre, en particulier des parents aux enfants.

Dans Ce travail vise à apprendre l'effet des traits du visage extraits entre une paire d'images faciales pour effectuer la vérification de la parenté. Dans notre étude, nous avons proposé un modèle binaire local (LBP) pour la représentation du visage. nous avons effectué des expériences de vérification de la parenté sur le difficile KinFace W-II.

Mots clés Biométrie, vérification de la parenté, modèle binaire local, extraction de caractéristiques et classification des caractéristique

الملخص

التحقق من القرابة عبر صور الوجه هو موضوع بحثي ناشئ في مجال القياسات الحيوية ، وعلاقات الأنماط لها بعض أوجه التشابه في مظاهر الوجه. هذه التشابهات في مظهر الوجه ناتجة عن ملامح الوجه الموروثة من جيل إلى الجيل التالي , خاصة من الآباء إلى الأطفال.

يهدف هذا العمل إلى معرفة تأثير ملامح الوجه المستخرجة بين زوج من صور الوجه لأداء التحقق من القرابة. في دراستنا اقترحنا النمط الثنائي المحلي (LBP) لتمثيل الوجه. أجرينا تجارب التحقق من القرابة على KinFace W-II الصعبة.

الكلمات المفتاحية ,القياسات الحيوية ، التحقق من القرابة ، النمط الثنائي المحلي ، استخراج الميزات وتصنيف الميزات

University of El- OuedEchahidHammaLakhdar4

TABLE OF CONTENTS

List of Figures

LIST OF FIGURES

Page

LIST OF TABLES

LIST OF TABLES

Abbreviations

Abbreviations

ISO	The International Standardization Organization
PINs	personal identification numbers
IEC	International Electrotechnical Commission
JTC1	underJoint Technical Committee 1
SC37	Subcommittee 37
CBEFF	the Common Biometric Exchange Formats Framework
INCITS	InterNational Committee for Information Technology Standards
FKP	Finger knuckle print
ERR	Equal Error Rate
F-S	father-son
F-D	father-daughter
M-S	mother-son
M-D	mother-daughter
AAM	Active Appearance Model
DL	Deep Learning
mRMR	Minimum Redundancy Maximum Relevance
DNNs	Deep Neural Networks
CDNNs	Convolutional Deep Neural Networks
RNNs	Recurrent Neural Networks
LBP	Local pinary pattern
MB LBP	Multi block
ML LBP	Multi level
COS SIN	Cosine distanse

General Introduction

General Introduction

Kinship verification is one of the major research topic in image processing, computer vision, and pattern analysis. In the past few decades, face verification and people recognition problems have been the focus of considerable attention. findings, several scientists have investigated the ability of human raters or perception of recognizing kinship from human facial images. In addition, the biological relationship and similarities between traits found in the same family inspire us to exploit this fact to develop a computer system that will be able to recognize kinship and apply it in a variety of applications. The present thesis is organized as follows:

Chapter I gives general background information on biometrics. It provides a detailed description of the biometric-based recognition process and discusses in details how biometric systems performance are established.

Chapter II gives background information on kinship verification task, and give an overview of automatic kinship verification form faces by presented some notions, definitions and terminology required for understanding this topic. Then we describe the system desine of facial kinship verification. On this chapter presents also some application and challenge related to facial kinship verification.

Chapter III we obtained the results of checking the kinship of the face we propose the method based on local binary pattern (LBP) descriptors and multi-block(MB) and multi-level (ML) representation, we first extract features using the descriptors, then we paplied MB and ML for increasing the features number. In order to select the best features,and we investigate the effect of different features representation for kinship verification, Moreover, a used(cos-sin) for the kinship classification. Our approach consists of five stages: (1) features extraction , (2) face representation (3) features representation, (4) features selection and (5) classification. Our approach is tested on database (KinFac W-II).

Chapter I

Biometrics defined

I.1. Introduction

Biometrics are body measurements and calculations related to human characteristics. Biometric authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics, which are related to the shape of the body. Including (fingerprint, DNA and iris…).Including behavioral characteristics represented in walking, signature and voice ....

I.2.Definition

The International Standardization Organization (ISO) defines the term biometrics, or biometric recognition, as being “the automated recognition of individuals based on their biological and behavioral characteristics” (ISO/IEC2382-37, 2012). The definition uses the word ‘automatic’ to imply the design of algorithms to be executed by a machine system to recognize individuals. The system could be assisted by a human to get better results. The ‘recognition’ aims to associate an identity with an individual based on some physical characteristics exhibited intrinsically by his body parts and/or some behavioral characteristics created by the body. These characteristics are called “identifiers” or “traits”. Examples of physical characteristics include among others: fingerprints, face, iris, etc. On the other hand, behavioral characteristics may include: signature, voice, keystroke dynamics, etc. Differently to the classical identification systems that establish the identity of an individual based on what he knows (secret information such as passwords) and/or what he has (possession of objects such as tokens, smartcards, licenses, …); biometric systems are based on what the person is (biological attributes) and/or what he does (behavioral attributes). These identifiers are directly related to the individual, thus cannot be forgotten, neither copied nor transmitted. Biometric systems exploit a variety of biometric characteristics (or modalities) including fingerprint, face, ear, iris, retina, palmprint, vein, voice, signature, gait, odor,…

I.3. Brief history of biometrics

According to Ashbourn (1999) [1] future biometric identification applications could include ATM use, workstation and network access, travel and tourism, Internet transactions, telephone transactions, public identity cards, etc. 5.3 A brief history of biometrics According to Ashbourn (1999) personal identification numbers (PINs) were one of the first automated recognition identifiers. However, the actual PIN was recognized and not the individual who provided the PIN. The same pitfalls apply to the use of cards and other tokens. Using a card or token together with a PIN provides a slightly higher confidence level, but it is seemingly easily compromised if one is determined to do so. Biometrics, on the other hand, cannot easily be transferred between individuals and represents a unique identifier, which means that verifying an individuals identify can become more accurate and streamlined. Ashbourn (1999) states that it is tempting to think of biometrics as being a scifi futuristic technology that will be used some time in the near future, but in actual fact the basic principles of biometric verification were understood and practiced somewhat earlier. Thousands of years ago people in the Nile region routinely employed biometric verification in a number of everyday situations. Their techniques included identifying individuals via unique physiological parameters such as scars, measured physical criteria or a combination of features such as complexion, eye colour and height. The people of the Nile did not have automated electronic biometric readers and computer networks, and they were not dealing with the numbers of individuals that exist today, but the basic principles were similar. Later, in the nineteenth century, researchers attempted to relate physical features and characteristics with criminal tendencies, resulting in a variety of measuring devices being produced. In parallel to this, fingerprinting became the international methodology amongst police forces for identity verification. The absolute uniqueness or otherwise of fingerprints is often debated, nevertheless, this was the best methodology on offer and still the primary one for police forces. With this background, it is hardly surprising that for many years a fascination with the possibility of using electronics and the power of microprocessors to automate identity verification had occupied the minds of individuals and organizations, both in the military and commercial sectors. Various projects were initiated to look at the potential of biometrics and one of these eventually led to a large and rather ungainly hand geometry reader being produced. Eventually, a much smaller and considerably enhanced hand geometry reader became one of the cornerstones of the early biometric industry. This device worked well and found favour in numerous biometric projects around the world. In parallel, other biometric methodologies such as fingerprint verification were being steadily improved and refined to the point where they would become reliable, easily deployed devices. In recent years, much interest has been seen in iris scanning and facial recognition techniques, which offer the potential of a non-contact technology, although there are additional issues involved in this respect. The last decade has seen the biometric industry mature from a handful of specialist manufacturers struggling for sales, to a global industry shipping respectable numbers of devices and poised for significant growth as large scale applications start to unfold (Ashbourn 1999).

Moreover, it is utilised to recognise a person among others inside monitored environments such as searching for wanted criminals among thousands of people across a city (e.g. face, voice or gait recognition).

Bill Gates, declared: “Biometric technologies, those that use voice, will be one of the mostimportant IT innovations of the next several years”. It is a science thatdepends on human’s physiological or behavioural features in order to identify him/her [2]. Whilst many definitions exist, they tend to focus on similar aspects, such as the automated method of identifying or verifying an individual. With some also highlighting thedifferent fundamental approaches of physiological and behavioural [3] .

To better understand the mechanisms of human biometric identifiers and its applications inthe daily life, almost all studies have classified the biometric characteristics into two distincttypes namely: physiological (traits related to people physical appearance, e.g. fingerprintrecognition or face recognition) and behavioural (refers to the way people behave, e.g. voicerecognition or mouse dynamics) characteristics.

I.4.Biometric Systems

I.4.1. Biometric Standards

Given that there are specific kinds of data collectors (sensors/readers) and algorithms for eachbiometric modality (each is possibly developed by different vendors), it is obvious thatimplementingmultibiometric approach (e.g. multimodal and multi-algorithmic) is apparently complicated.

For such approaches to exist in a vendor- and modality-independent manner,agreed upon standards are crucial to be developed and conformed with. Usually, havingseveral biometric each uses different structure metrics and data format would lead toindividuals being locked-in with a particular vendor irrespective of the diversity of performance and cost afforded (NSTC, 2011b) [4]. Irrespective.

The standards of biometrics have been developed internationally regarding specific modalityor the entire biometric system, allowing interoperability between different systems thus, forinstance, identifying consolidated biometric data interchange formats. Interoperability is a key aspect for implementing multiple biometric approaches, such as images collected by one device need to be compatible with those collected by another device. Moreover, it must bepossible that both of these collected images are interpreted by a third provider product.

International Standards Organisation (ISO) and International Electrotechnical Commission(IEC) have developed main standards supporting the generic goals of biometric standards:interoperability and data interchange among applications and systems. ISO and IEC underJoint Technical Committee 1 (JTC1) Subcommittee 37 (SC37) define that the key aspectscovered by these standards are (Podio, 2011; JTC 1/SC 37, 2013) [5]

- common file frameworks (ISO/IEC 19785);
- biometric application programming interfaces (BioAPI) (ISO/IEC 19784);
- biometric data interchange formats (ISO/IEC 19794);
- related biometric profiles (ISO/IEC 24713)
- methodologies for performance testing and reporting (ISO/IEC 19795)
- cross jurisdictional and societal aspects (ISO/IEC 24779).

Deploying ISO standards such as ISO 19794, 19785, 19784 might avail combining any chosen biometric methods – particular devices will not be able to accomplish this because ofthe very high costs and processing requirements (ISO, 2006a, b, 2011).[6]

In order to promote interoperability of multiple biometrics-based devices applications andsystems, the Common Biometric Exchange Formats Framework (CBEFF) standard (thefundamental standard in the field) has been developed by national and international standardsdevelopment bodies (InterNational Committee for Information Technology Standards(INCITS) Technical Committee M1 – Biometrics and ISO/IEC Joint Technical Committee 1 (JTC 1) Subcommittee SC 37 – Biometrics) (NIST, 2008) [7], thus, enabling the exchange ofbiometric information efficiently between system components (NSTC, 2011b) [8].

I.4.2. Biometric Requirements

Each biometric has its strengths and weaknesses and therefore several factors should be takeninto account when selecting a particular biometric for use within a specific application.

Theappropriateness of the potential biometric authentication technique is determined based onthe availability of the following seven requirements on the associated trait:

- Universality
- Performance
- Uniqueness
- Acceptability

- Permanence
- Circumvention
- Measurability

Universality means that each individual uses the application should have the chosenbiometric feature, for instance, if all users have hands, it would be possible to use handgeometry as biometric technique. Uniqueness, to differentiate each person from one another,the given trait should be appropriately different for persons in the relevant population.

Thereby, more distinctive features will permit more successful discrimination of anindividual from a larger population than methods with less uniqueness. For example, whilstface trait would be suitable for accessing a smartphone, accessing military informationrequires a more unique trait such as iris. Permanence, the biometric trait of any person shouldbe sufficiently stable over the time, as the more the frequent changing of a trait, the more theneed to update the biometric template and hence the cost of maintenance (Clarke, 2011) [9].

For instance, whereas individual retina scan remains invariant, their keystroke behaviourvariesdue to device, mode, and text familiarity. Measurability, or the ease of acquisition anddigitalization of a particular biometric trait utilising convenience and suitable devices, as wellas the ease of extraction of the feature set from the raw trait. Collecting some biometrics isvery intrusive – it requires specialised devices and/or explicit user interaction, such as theretina. Conversely, others can be collected easily with normal daily devices and interactions,such as capturing face samples while interacting with the computer. Performance refers to theaccuracy and scalability of the technologies required to acquire the feature’s samples shouldbe considered with their applications and constraints. Acceptability means the end-users of an adopted biometrics should be willing to provide their traits and utilise the technique, in termsof, for instance, privacy and convenience. Otherwise, they would resist or avoid using it.

Circumvention means how easy it is to duplicate the feature using an artefact or fakealternative, for instance, iris scan is almost impossible to imitate, unlike silicon fingerprints ora photograph of a person (Clarke, 2011).

It can be deduced that a perfect biometric trait to be deployed in an authentication systemshould meet all the above-mentioned requirements. Nevertheless, there is no biometriccurrently and highly likely in the future will meet all the above seven characteristics precisely(Jain et al., 2008). Therefore, some studies have suggested the use of multimodal approachesto increase the difficulty of simultaneously forging multibiometrics (Ceccarelli et al., 2014) [10]

I.4.3. Verification and Identification

It is noteworthy to highlight that there are two modes that a biometric system can operate in,namely: verification and identification (Nanavati et al., 2002) [11].

- **Verification:** seeks to verify that a claimed identity is matched with that on the database.
- **Identification:** seeks to determine whether the identity exists on the database.

From classification perspective, verification is simpler than identification Clarke (2011).

During verification mode the matching process is between sample(s) of claimed individualand the stored template of that individual; thus it is a one-to-one (1:1) comparison. While thecomparison is one-to-many (1:N) in identification mode; anonymous sample(s) is comparedwith every stored template to decide whether there is a match. This means that there is apossibility that the user's template does not exist at all in the database. Hence, the result ofthe former mode confirms that claimed identity is true or false while the latter decides whether the user is identified or not.

Both these two different modes rely on the application context; if the individual has claimedhaving enrolled in the system by providing an identity, for example, a username or token witha biometrics, the former mode operates, otherwise the latter does so (VallabhuandSatyanarayana, 2012) [12]. Furthermore, other aspects should be considered when deploying either of the two modes – they are different regarding performance and privacy (Clarke, 2011; Nanavati et al., 2002) as well as cost and user-friendliness. Additionally, due to the involvement of more complexity and computation, identification process typically needs longer time. Consequently, identification needs higher level of system's accuracy and trait's uniqueness than verification.

I.4.4. Components of Biometric System

The biometric process consists five components that can be classified into (Clarke, 2011)

- Capture
- Extraction
- Template Database
- Classification
- Decision

Sample capturing (acquisition), is the stage of obtaining the biometric samples from the person using some form of sensor depending upon the biometric system, such as optical finger scanner for fingerprint recognition, a microphone for voice recognition, or a web camera for facial recognition. In feature extraction (processing) stage, deploying particular algorithms, the unique characteristics of the captured sample(s) are processed aiming at generating a feature extraction template.

For example, in facial recognition, after an image sample is captured, a number of algorithms are performed to extract its distinctive features, such as the distance between the eyes and nose, areas around cheekbones and the sides of the mouth, to create the template.

The output of the extraction phase is called a feature vector.

The template database is not the raw biometric sample but the template resulted from theaforementioned feature extraction process is stored in a database perhaps along with otheruser's information. This stored template is utilised as a reference in the matching processafterwards. Therefore, the user enrolment process is completed by the end of the third step.

The fourth component is theclassification (matching) phase, when a person attempts to have access by providing currentbiometric samples, the features of these samples are extracted and subsequently compared to the stored reference template(s) (resulted from the enrolment process) using a matchingalgorithm. Accordingly, a match score is given representing their degree of similarity, basedupon which the authentication decision is followed. Finally, in the decision stage, acomparison between the matching score and the set threshold is performed – if the formerequals or exceeds the latter, the access is approved; otherwise, access is denied/rejected orrestricted. Therefore, it is also vital to ensure capturing high-quality samples in the enrolmentprocess, because the low-quality samples might lead to errors and misclassification error inthe verification process of the legitimate user, or even authorising the wrong person into thesystem. The whole previous stages are illustrated in the following Figure (I.1).

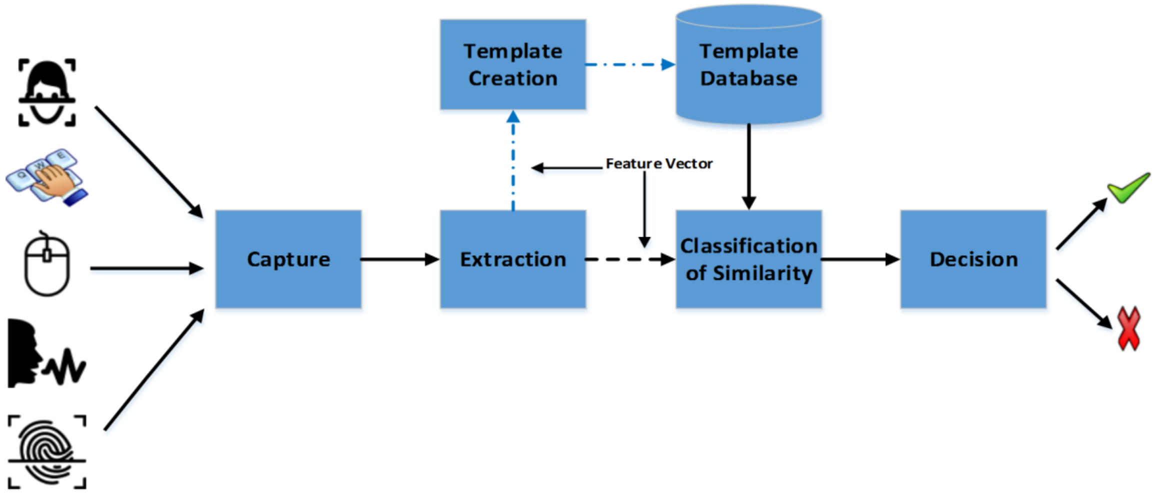


Figure I.1: The Biometric Process

I.5. Biometric Performance evaluation

Biometrics is the scientific term for body measurements and computations. It indicates to metrics belonged to human traits. Biometrics verification (or realistic authentication) is utilized in computer vision as a form of matching identity and accessing control. We refer that also utilized to identify persons in groups that are under surveillance. Biometric recognizers are the discriminatory, measurable traits utilized to describe and label persons. Biometric recognizers are overwhelmingly classified as physiological against behavioral traits. Physiological traits are belonged to the the body shape. Examples involve, but are not limited to palm veins, fingerprint, facial recognition, palm print, DNA, hand geometry, retina and odour/scent, iris recognition. Behavioral traits are belonged to the modality of behavior of a individual, involving but not limited to typing rhythm, gait, and voice. Some researchers have used the term behaviometrics to characterize the latter class of biometrics. More conventional means of accessing control comprise token-based recognition systems, such as a driver's license or passport, and knowledge-based identification systems, such 14 Introduction as a password or personal identification number. Since biometric identifiers are singular to each person, but they are highly reliable in the identity verification than token and knowledge-based methods; furthermore, the set of biometric identifiers elevates privacy issues about the integral utilize of this information traits.

- **False rejection rate (FRR):** proportion of authentic users that are incorrectly denied. If a verification transaction consists of a single attempt, the false reject rate would be given by:

  $$FRR(\tau) = FTA + FN\,MR(\tau) * (1 - FTA) \qquad \text{I.1}$$

- **False acceptation rate (FAR):** proportion of impostors that are accepted by the biometric system. If a verification transaction consists of a single attempt, the false accept rate would be given by:

  $$FAR(\tau) = FMR(\tau) * (1 - FTA) \qquad I.2$$

- **Equal Error Rate (EER):** this error rate corresponds to the point at which the FAR and FRR cross (compromise between FAR and FRR). It is widely used to evaluate and to compare biometric authentication systems. More the EER is near to 0%, better is the performance of the target system.

I.5.1. Biometric Modalities

As stated previously, based upon the nature of the deployed discriminative trait, studies haveclassified biometric techniques into: physiological and behavioural. According to the results of the Biometrics Institute Industry 2013 Survey, the former category is more established than the latter and have the biggest user adoption to date. For instance, the survey revealed that the order of which biometrics the respondents are involved in begins with fingerprint, face, iris, multimodal (i.e. more than one biometric modality in one system), and finally speaker recognition [13]. Notably, speaker recognition is the only behavioural biometrics of the list and it is at its end.

✓ **.Physiological Modalities**

These methods aim at differentiating an individual based upon particular physicalcharacteristics. Given that the stability and reliability of them, many systems rely on them forboth identification and verification.

- **Fingerprint:** Fingerprint Recognition includes taking a fingerprint image of a person and records its features like arches, whorls, and loops along with the outlines of edges, minutiae, and furrows. Matching of the Fingerprint can be attained in three ways, such as minutiae, correlation, and ridge.

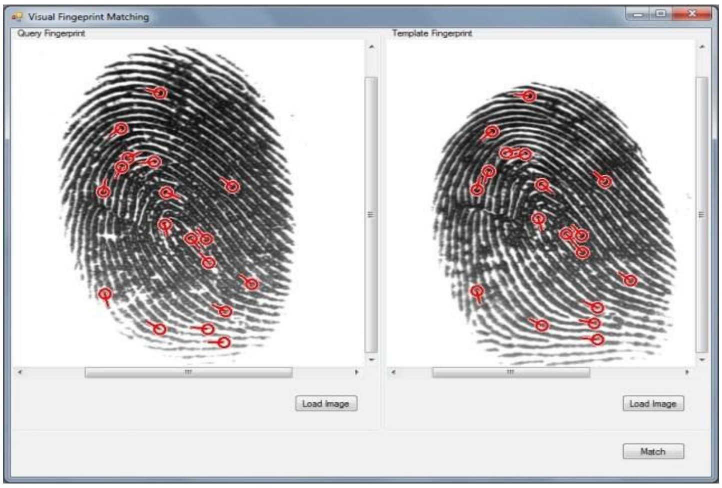


Figure I.2: An Example of Fingerprint Recognition Showing the Patterns on theUneven Surface of Tip of a Finger

- **Face Recognition:** A face recognition system is one type of biometric computer application that can identify or verify a person from a digital image by comparing and analyzing patterns. These biometric systems are used in security systems. Present facial recognition systems work with face prints and these systems can recognize 80 nodal points on a human face. Nodal points are nothing but endpoints used to measure variables on a person's face, which includes the length and width of the nose, cheekbone shape, and eye socket depth

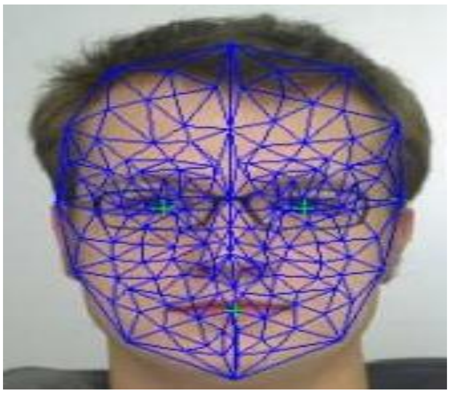


Figure I.3: Example of 2D Facial Recognition

- **Iris Recognition :** Iris recognition is one type of bio-metric method used to identify the people based on single patterns in the region of ring-shaped surrounded the pupil of the eye. Generally, the iris has a blue, brown, gray or green color with difficult patterns that are noticeable upon close inspection.

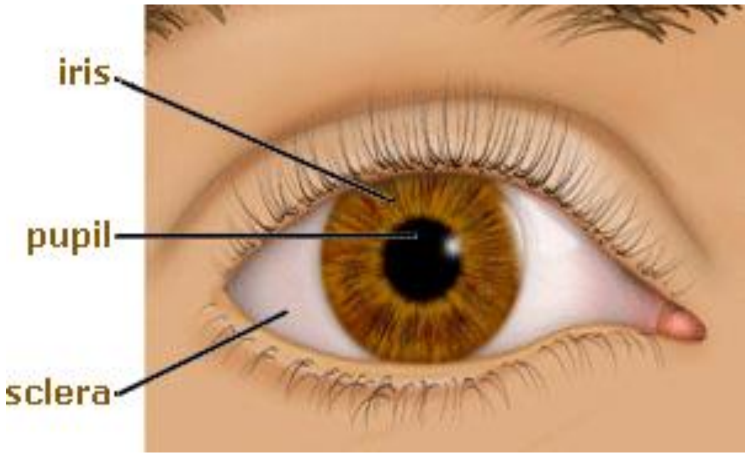


Figure I.4: Anatomy of an Iris

- **Hand Geometry:** The actual shape and dimensions of your hand are sometimes used for access control and time-and-attendance operations in the workplace. However, they are not as unique as fingerprints, so aren't viable in high-security applications.
- **Finger knuckle print (FKP):** is one of the emerging biometric traits. The region of in terestis the area where the maximum information is centered, for a finger knuckle it is the area surrounding the knuckle region. [14]
- **DNA:** is an emerging biometric trait that can be used for recognizing individuals. The specific area of the long DNA sequence is observed to find the identical feature. DNA itself is unique for each individual, except the identical twins. Therefore, it achieves high accuracy. DNA can be acquired easily from hair, saliva, skin follicles etc.

✓ **Behavioural Modalities**

Behavioural biometrics a differentiate people based upon measuringcharacteristics and pattern of their way of usage [15]. Despite the lessdegree of uniqueness and permanence caused by the erratic nature of these behaviouralfeatures because of different reasons, for instance, changing mood, health, and environment,they tend to be more universal, transparent, and hence usable than the physiological ones.

- **Voice Recognition:** Voice recognition technology is used to produce speech patterns by combining behavioral and physiological factors that can be captured by processing speech technology. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence. Voice recognition can be separated into different categories based on the kind of authentication domain, such as a fixed text method, in the text-dependent method, the text-independent method, and conversational technique

- **Signature Recognition:** Signature recognition is one type of biometric method used to analyze and measure the physical activity of signing like the pressure applied, stroke order and speed. Some biometrics are used to compare visual images of signatures. Signature recognition can be operated in two different ways, such as static and dynamic.

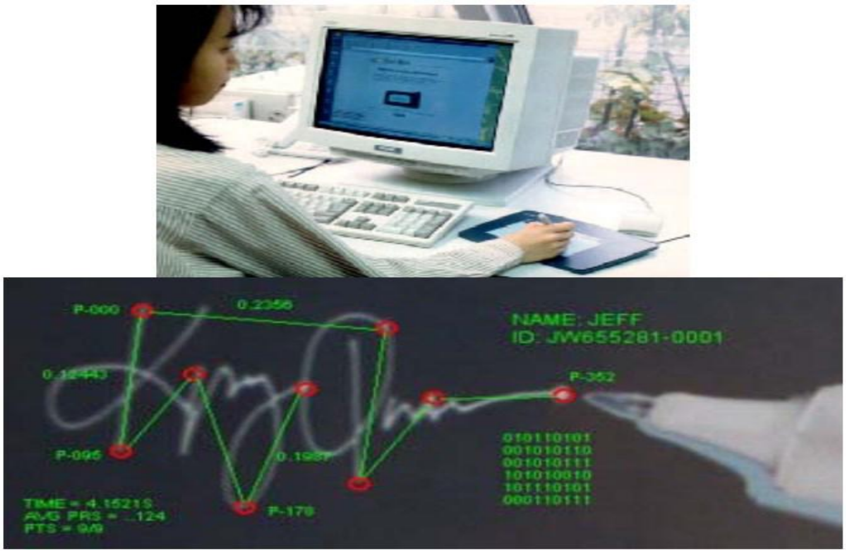


Figure I.5: Dynamic Signature Depiction

I.5.2. Biometrics market and applications

Biometrics has successfully convinced wide range of applications to be adopted not only as a fundamental component in their security architecture, but as an economical tool that can lead directly or indirectly to saving costs and reducing financial risks [16]. It had advanced quickly and significantly over the two decades. Recent researches confirm that the market of biometrics would grow from 8,7 billion dollars in 2013 to nearly 27,5 billion dollars by 2019 registering an annual growth of 19,8% between 2014 and 2019 [17]. Fingerprint modality will still dominate the market as shown in Figure 7. This acceleration is justified by the proliferation of the electronic services that necessitate identification, along with the rise of fraud acts and identity theft that must be fought. In addition

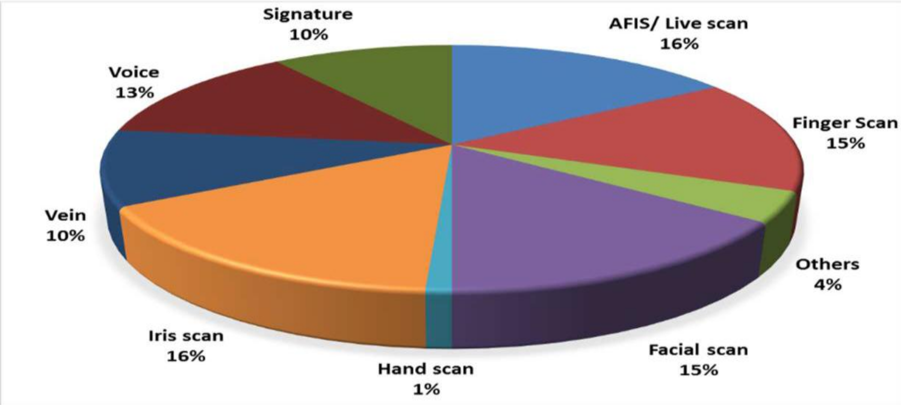


Figure I.6: Biometrics Market by modality (2015) (Wright &Kreissl, 2014) [18]

To that, the adoption of the electronic documents, especially biometric passports and national ID cards, by major governments will participate to largely increase its use. Biometrics is now adopted in, but not limited to:

- **Governmental applications:** biometric national identity card, biometric passport, border control, social security, e-voting …
- **Access control:** it can be physical such as time-attendance systems and door security, or logical such as accessing remote computer resources and information systems.
- **Mobile applications:** recent mobiles are equipped with biometrics technologies that allow identifying the owner, to unlock the device, to make commercial transactions, etc. For instance, Apple iPhone 5s and Samsung Galaxy A5 are delivered with a built-in fingerprint reader along with smart software that are attended to recognition purposes.
- **Commercial applications:** most products integrate biometrics to enhance the user’s experience. Access to computers, internet applications, e-commerce, banking transactions, etc.
- **Forensics applications:** forensic laboratories usually use biometrics in their criminal investigations and parenthood determination as well as to identify corpses. New researches have confirmed the possibility to determine a person’s ancestor origin based on his fingerprint.
- **Military applications:** these include identification systems for use in the field, access control and monitoring applications to sensible areas, as well as large database deployments.

I.6. Conclusion

In this chapter, we presented biometrics, their history, requirements for their measurements, and their applications. In the second chapter, we will discuss the check of the face and the kinship using the image of the face.

Chapter II

Facial Kinship Verification

II.1. Introduction

Kinship verification is a process that uses facial features to validate a person's relationship. Recognizing people in pictures is a good example of this capacity. The background information and concepts needed to understand the kinship verification topic are discussed in this chapter. We also offer an overview of the problems associated with kinship verification using human facial images, as well as the key solutions suggested by state-of-theart study.

The definition of kinship verification in computer vision is introduced first, followed by a discussion of kinship terms. The disparity between a facial verification system and a kinship verification system was highlighted.

II.2.Kinship in theory

II.2.1.Kinship terminology

Before embarking on the nature of the problem and the solutions, we need to be familiarwith different kinship terms, which will determine the course and ambit of this study. Ingeneral, kinship may indicate similarity, familiarity, or closeness between entities on thebasis of some or all of the basic traits or features. Kinship is a broad term that has differentmolds of meaning based on the framework or context in which it operates. Kinship can beformulated or labeled as kin relationship. In the anthropological context, kinship refers tothe network of social relationships between people that form an important part of the livesof most humans in most societies [25].

Nevertheless, in other contexts, kinship may have different meanings. In biology, kinshiptypically refers to the degree of genetic relatedness or coefficient of relationship betweenindividual members of the same species [24]. Moreover, different societies classifykin relationships differently and therefore use different systems of kinship terminology [24].

II.2.2.Kinship types

Kinship is one of the universals in human society. In any society, kinship systems establish relationships between individuals and groups on the model of biological relationshipsbetween parents and children, between siblings, and between marital partners. By contrast, the adoptive child is excluded from this relationship. “Adoption” is the term that isoften used to describe a person who has no biological link with the parents. Relationshipsestablished by marriage form alliances between groups of persons related by blood (or consanguineous ties) [20, 30]. These two aspects of human life are the basis for the followingtwo main types of kinships in society [27]:

- Blood ties (consanguineal): Relationships or connections based on blood or genetic ties, that is, the relationship between parents and children and between siblings are the most basic and universal kin relationships.
- Marriage ties (affinal): Relationships formed on the basis of marriage. The most basic relationship that results from marriage is that between husband and wife.

II.2.3. Kinship classes (degree)

Any relationship between two individuals is based on the degree of closeness or distance ofthat relationship. The degree of closeness or distance of any relationship depends on howindividuals are related to each other. Kinship basically has three degrees [27],namely, primary, secondary, and tertiary kinship.

i. Primary kinship: This degree refers to kin that are closely and directly related to one another. The eight types of primary kinship include mother-son, husband-wife, fatherson, mother-daughter, father-daughter, sister-brother, younger sister-elder sister and younger brother-elder brother.
ii. Secondary kinship: This degree refers to the primary kin of the first degree kin (also known as secondary kin), such as father’s brother, sister’s husband, and brother’s wife.
iii. Tertiary kinship: This degree refers to the secondary kin of the primary kin (also known as tertiary kin), such as brother of sister’s husband and wife of brother-in-law.

II.3.Kinship in computer vision

Kinship is a genetic relationship between two family members, including parent-child,sibling-sibling, and grandparent-grandchild, this is the application of kinship in computervision so far. Therefore, in automatic kinship recognition using computer vision techniques,the machine is able to discriminate kin from unrelated people and determine the degree ofkin relationship based on an inspection of their images [28]. In other words, it is a task oftraining a machine to recognize the blood relation between a pair of kin and non-kin faces(verification) based on features extracted from facial images and to determine the exacttype or degree of that relation (recognition).

The automated kinship verification method uses only photos of people's faces to attempt to identify their relationships. Kin recognition is the job of teaching a computer to identify genetic kin and non-kin based on features extracted from digital images andattempting to decide whether or not kinship occurs between a pair of faces [19]. Kinship verification is a difficult problem in computer vision since it faces many obstacles similar to face recognition issues, such as low-resolution images, lighting shifts, pose variations, aging effects, mixed ethnicities, and different age groups. Furthermore, the kinship system is a classification system for people who are related by kinship based on patterns such as theirfaces (see Figure II.1). For example, the inputs may be two faces (Face A and Face B), with the expected output being a determination of whether Person A is Person B's father, sister, mother, or brother.

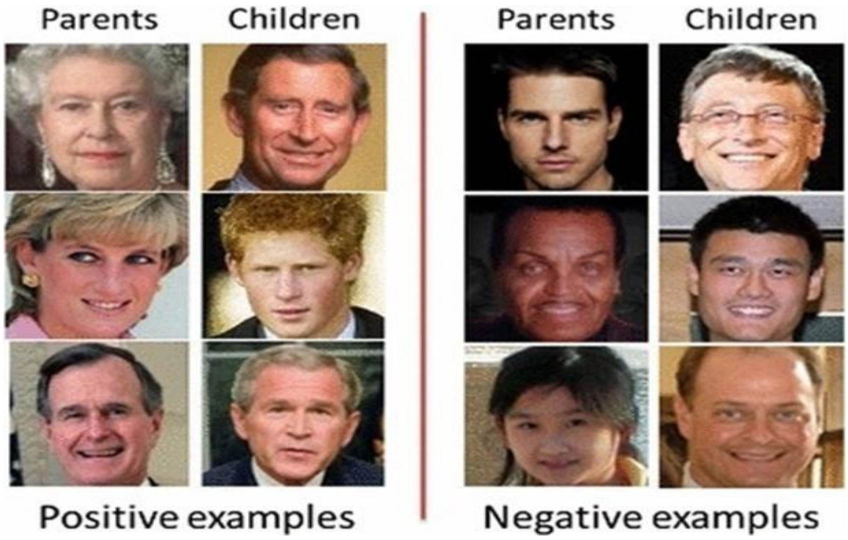


Figure II.1: An example of kinship verification via face images. [52]

II.4Face recognition and kinship recognition

At first glance, the process of face verification and recognition may seem similar to that ofkinship verification and recognition. In fact, face verification and recognition and kinshipverification and recognition are two different things. We might say that kinship verificationand recognition is the highest level of face verification and recognition. At the same time,we cannot ignore the existence of common factors between them, such as the challengesor even the techniques used. The following describes remarkable differences between thefacial recognition and kinship recognition based on seven criteria which are definition andtarget, mode, challenges, applications, features, processes, and accuracy.

- ✓ **Modes**

Both systems encompassing the mode of verification and identification, with a discrepancyin the style of implementation. Figure 2 shows identity (face) and kinship modes.

- **Face verification:** Is this same person? (1:1)
- **Face identification:** Who is this person? (1:N)
- **Kinship verification:** verifies the existence of kin relationship between a pair of images or more (1:N).
- **Kinship identification:** identifies the degree of kin relationship (1:N).

In kinship, we observe the existence of a link between verification and identification mode,which means that the system cannot proceed in determining the degree of kinship withoutresorting to verify the existence of kinship. This leads us to declare that the mode of identification adopt on verification. In contrast, identity or face recognition, verification andidentification modes are uncorrelated practically. In other words, the verification mode doesnot depend or adopt on the identification and vice versa.

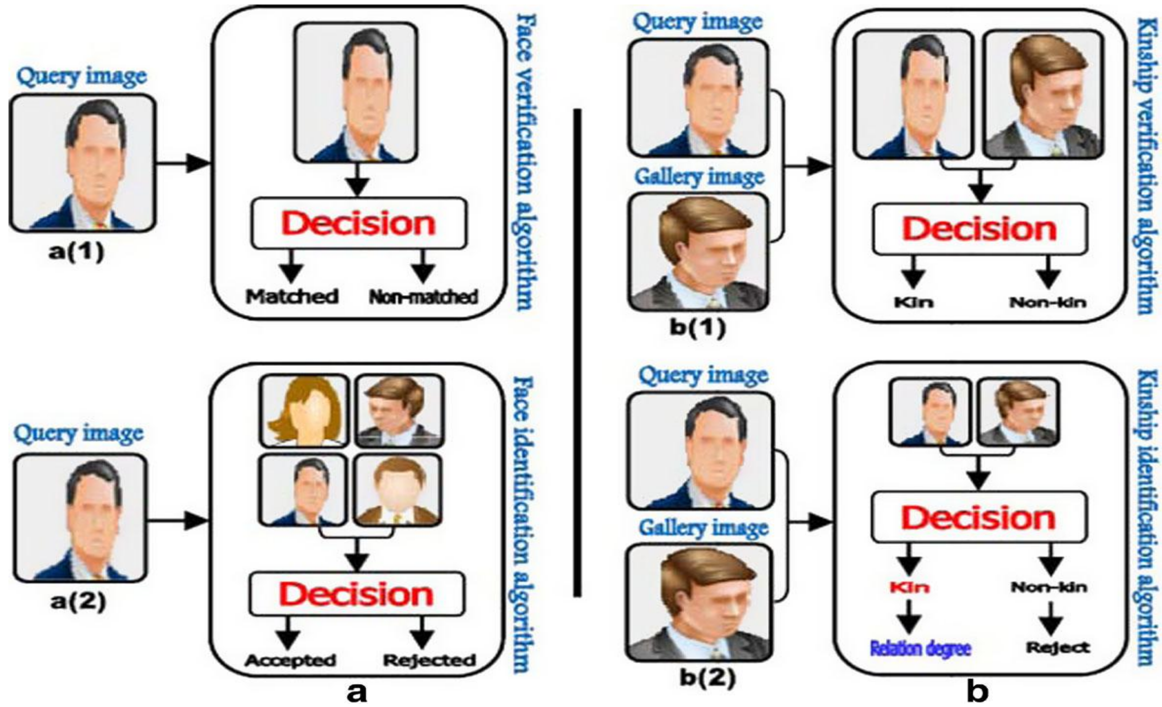


Figure II.2: Modes of identity (face) and kinship. a identity (face verification a(1) and face identification a(2)), and b kinship (kinship verification b(1) and kinship identification b(2)) [52]

✓ **Processes**

The process of the identity or face recognition and kinship is carried out by examiningof critical and dominant features found in facial features and comparing them with thosethat have been derived from another faces, this also is one of the obvious things in common between the two concepts. Moreover, there is almost a clear convergence between thesuccessive steps in order to achieve the purpose of two different goals. In addition, the processes of verification and identification mode steps for both systems are almost equal. Thedifference occurs at classification step.

The essential stages for both systems can be pass through: (1) acquiring the images,next (2) pre-processing and face detection, then (3) extracting the inspiring face features,followed by (4) comparing between the targeted image and the rest of the images locatedin the database as a prelude to classify, concluded with (5) presenting the consequence ofcomparison which will be either:

– Identity recognition: matched or non-matched when the context is in the verificationmode, or accepted or rejected when the context is in the identification mode.
– Kinship recognition: kin or non kin when the context is in the verification mode, oridentifies relation degree or rejected (non-kin) when the context is in the identificationmode.

II.5.System design

The automatic detection of kinship from facial images is a difficult problem that recently received attention from the computer vision and pattern recognitionresearchcommunity. Kinship is a genetic relationship between two family members.

Specifically, there are four different types of kinship relations: Mother-Daughter (M-D),Father-Daughter (F-D), Mother-Son (M-S) and Father-Son (F-S) kinship relationssee Figure II.4.

The kinship verification has been studied in psychology and sociology [36]and [41]. The findings from the literature include that:

- Humans are able to recognize kinship relationships between unknown individuals.

- The mechanism of kinship perception is probably different from identity recognition.
- Human faces can convey some important cues to identify the kin relations of persons.
- Even attempted to identify the facial features providing kinship clues.
- Facial appearance is a useful cue for genetic similarity.

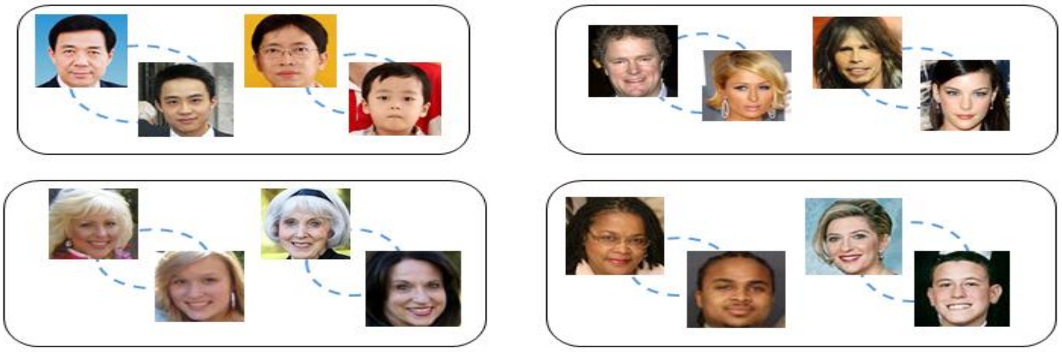


Figure II.3: KinFaceW-II database. Four type relationships: (F-S), (F-D), (M-D),and (M-S) [52]

Inspired by this observation, researchers started to investigate this problem from facialimages, where the objectives are to develop computational models and algorithms toverify human kin relations.

The aim of kinship verification is to recognize the genetic kin or not-kin relationship based on image feature. In recent years, several methods have been proposed toinvestigate this problem using computer vision and machine learning. In 2010, Fanget al. [20] was tackle the first attempt of kinship verification; they proposed a methodto automatically verify parent-child image pair relationships through the analysis offacial features. His method works according to the following steps:

- **Step 1:** Parent-child database collection. Over on-line search, they collected the databases that contain facial pairs image (parent-child) from celebrities and public figures.
- **Step 2:** Inherited facial feature extraction. They used a set of low-level image features extractions including, facial parts, color and geometry distances between parts and gradient of the face.
- **Step 3:** Classifier training and testing. Objective of this experiment is to classify the child - parent pairs into two false and true categories. Same number of negative

pairs (no kin relation) as positive pairs (with a kin relation) is created by associating faces from persons which do not have a kinship relation.

The positive examples are the true pairs of parents and children and negativeexamples are each parent with a randomly selected child from the childrenimages who is not his/her true child. Using the extracted feature vectors, theycalculate the differences between features vector of the corresponding parentsand children, and apply different machine for classification.

Figure II.4 presents a general schema of kinship verification based on facial images.This kinship system has the following essential components:

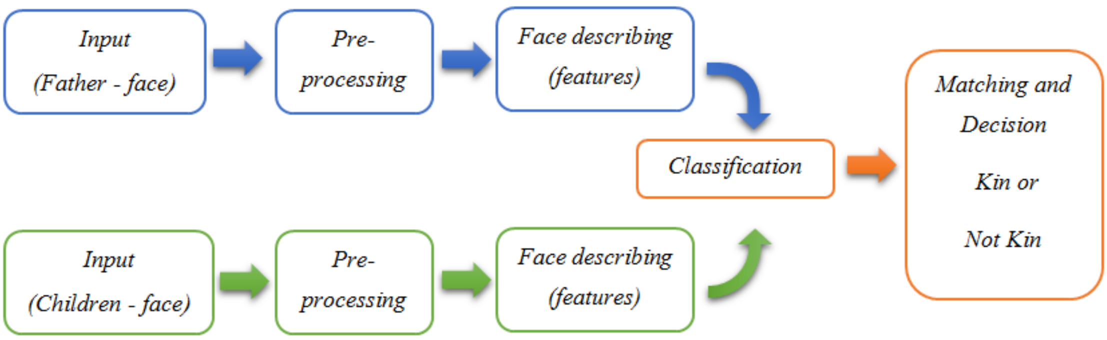


Figure II.4: General schema of kinship verification system. [52]

1. **Input (face datasets):** includes public figure face images of family members. Therefore, the face images are captured under uncontrolled environments with no constraints.
2. **Pre-processing:** is an important component. In order to localize the face of the image, this latter is then cropped, such that the non-facial regions such as the background and hairs were removed and only facial region was used for kinship verification. If those are color images, they converted into gray-scale images. For each cropped image, histogram equalization was applied to mitigate the illumination.
3. **Face describing:** the best way to learn kinship analysis is first to learn how to recognize the different facial features for children, and then learn how to relate them to their corresponding parents. Facial features must be described in a way that enables them to be efficiently descriptors.

4. **Classification and Decision:** kinship Verification is bi-classification problem where the pair of input faces is classified as positive (the true pairs of parents and children) or negative (the false pairs of parents and children).

II.6.Application

Determining if someone is a father, mother, son, or daughter is a complicated task. Itis possible to use the most advanced of methods to determine if two persons are likelyto have the suspected relation or not. Researchers started to investigate the problemof kinship verification, where the objectives are to estimate relatedness between closelyrelated individuals based on face features. There are some potential applications forkinship verification such as family album organization, social media, missing childsearch and entertainment.

II.7 Kinship challenges

In particular, facial kinship verification is very challenging. There are at least twomajor challenges. The first one is related to the environment of the database. Thesecond one is related to kinship itself.

- The face of pairs (parent- child) may look different due to variance in age, gender, and mixed ethnicity environments and also to deal with other factors such as: pose variations, illumination, and expression, especially, when face images are captured in unconstrained environments.
- Secondly, extracting features can be considered as a main problem to determining the relationships. We must initially determine which facial features are most relevant for determine parentchild relationships. It is necessary to describe and extract the most inherited feature in order to perform robust kinship verification system.

II.8.Kinship image databases

The first challenge related to the investigation of kinship recognition arises from thelackofpublicly available databases to work with as mentioned earlier. It is only recently that growing interest in the kinship recognition problem leads to the availability of several databasesof facial images of persons associated by various kinship classes. These databases arecomposed of mixed sets of images, mostly collected from the websites of public figures(entertainment celebrities, sports figures, and politicians). These databases contain imagesunder unconstrained and/or constrained environments in background, illumination, expression, and pose; and of different age ranges, genders, ethnicities, and so forth. Currently, apublicly available facial image database exists for kinship relations such as parent-child andsiblings.

Kinship databases, such as UB KinFace [45], Siblings [40], and Family101 [15, 16],are available sources used to tackle the kinship problem and experiment on the performanceof the proposed algorithm. Most of these databases, such as UB Kinface and Family 101,contain images with only one person in each image. Only one database, group-faces, contains images with more than one person in each image [22]. Some of these databases areavailable online for direct download, and others are available upon request. Figure II.5 showsthe result generated using UB KinFace version2

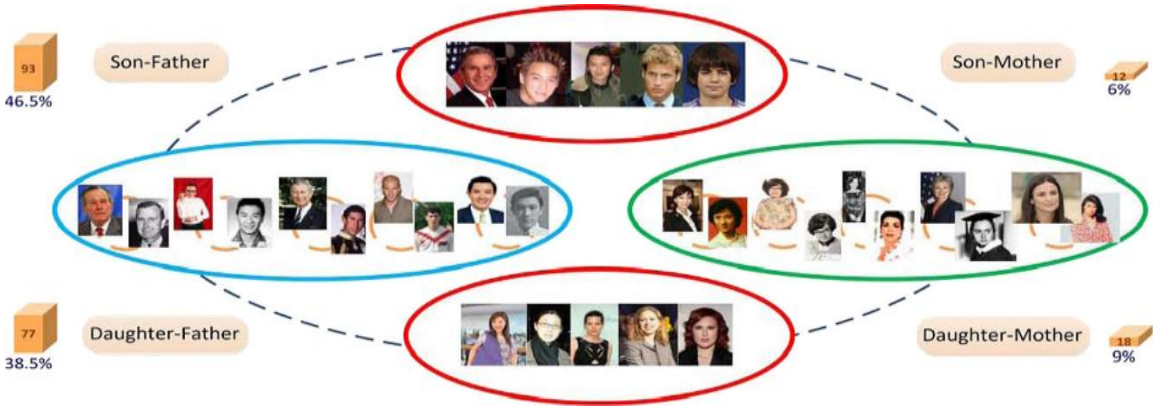


Figure II.5:UB KinFace ver. 2.0 database; four sets of people and four potential relationships. Male parents'images are in the blue ellipse; female parents' images are in the green ellipse; children's images are in thered ellipses [45]

II.9.Conclusion

In this chapter we introduced the concepts of checkface kinship, and explained some terms and types and how to design the system 0. We also presented some applications and challenges which encounter the check face kinship process.

Chapter III

The method kinship virification

III.1 Introduction

Kinship Verification in Computer vision has many applications for real life such as face recognition, age estimation, gender classification, face analysis, object detection, defect inspection. Among them, face analysis receives more attention because it is widely applied. One of the related problems is kinship verification. This process allows to determine the relationship kin or nonkin between two persons quickly. This is a relatively young topic and has still challenging problems because most of the facial images are selected from varied sources and affected by aging, skin color, illumination. Moreover, some people who are related by blood seem like different when they grow up. Thus, kinship verification by computer vision can help people identify and find lost children, determine the kinship or not kinship quickly instead of ADN testing, which take more times.

Many methods have been proposed to improve performance and algorithm for kinship verification in the state-of-the-art

Local Binary Pattern (LBP) is one of the most successful descriptors because of fast and simple computation among the local and global descriptors proposed in the literature. In this presentation, instead of extracting the LBP features from facial images globally, we propose to divide the image into small blocks. It can be expected some regions contain important information than others (such as eyes, cheeks, nose, lips). The feature selection approach is applied to determine the relevant information.

The experimental results and conclusion can be found in last section.

III.2 Shéma of method kinship virification

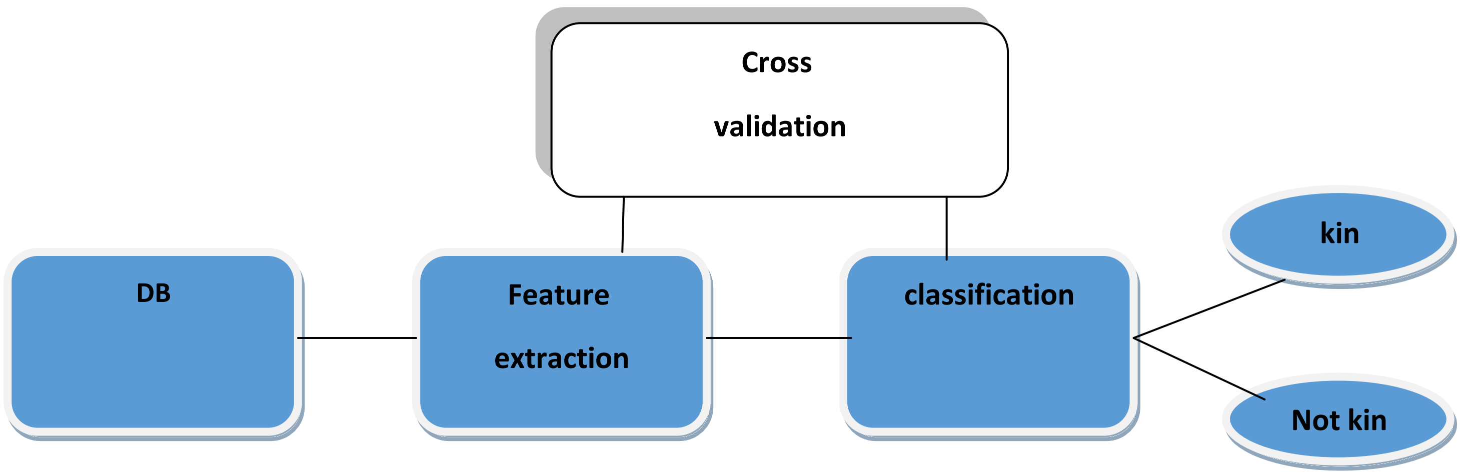


Figure III.1:shéma of method kinfice virification

III.2.1 data base

Kinship Face in the Wild (KinFaceW), a database of face images collected for studying the problem of kinship verification from unconstrained face images. There are many potential applications for kinship verification such as family album organization, genealogical research, missing family members search, and social media analysis.

The aim of kinship verification is to determine whether there is a kin relation between a pair of given face images. The kinship is defined as a relationship between two persons who are biologically related with overlapping genes. Hence, there are four representative types of kin relations: Father-Son (F-S), Father-Daughter (F-D), Mother-Son (M-S) and Mother-Daughter (M-D), respectively. http://www.kinfacew.com/

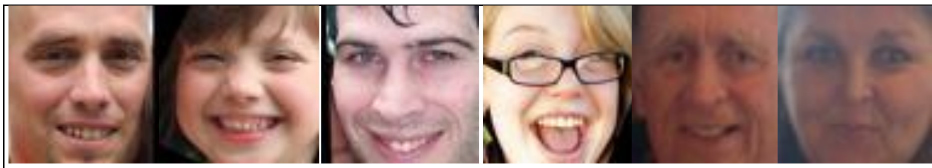
	F-d
	f-s
	m-d
	m-s

Figure III.2:data base kinface-2 kinship f-d f-s m-d and m-s

III.2. 2Feature local binary pattern

✓ Feature local binary pattern

The original LBP operator was introduced by Ojala et al. [5]. This operator works with the eight neighbors of a pixel, using the value of this center pixel as a threshold. If a neighbor pixel has a higher gray value than the center pixel (or the the same gray value) than a one is assigned to that pixel, else it gets a zero. The LBP code for the center pixel is then produced by concatenating the eight ones or zeros to a binary code (Figure III.3)

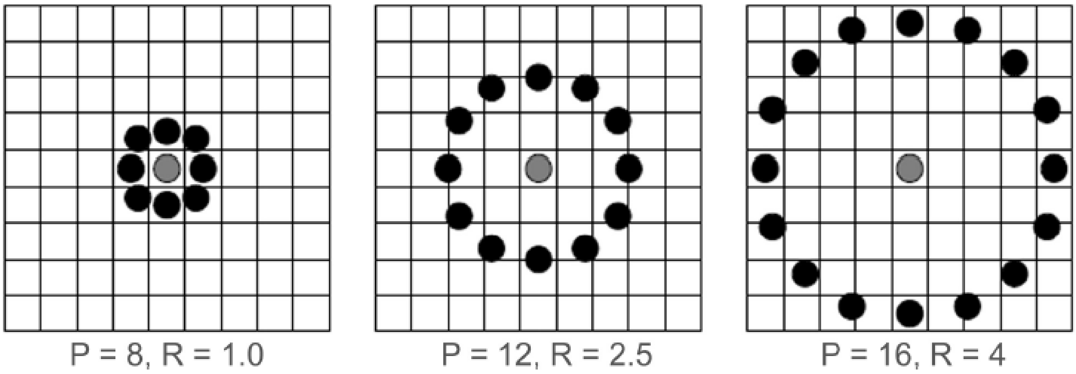


Figure III.3: The original LBP operator. [53]

Later the LBP operator was extended to use neighborhoods of differentsizes. In this case a circle is made with radius R from the center pixel. Psampling points on the edge of this circle are taken and compared with thevalue of the center pixel. To get the values of all sampling points in theneighborhood for any radius and any number of pixels, (bilinear) interpolationis necessary. (The working of bilinear interpolation is explained inappendix A.) For neighborhoods the notation (P,R) is used. Figure III.3illustrates three neighbor-sets for different values of P and R.

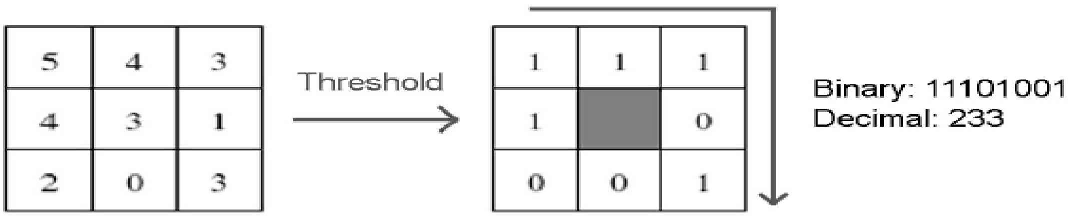


Figure III.4: Circularly neighbour-sets for three different values of P and R. [53]

If the coordinates of the center pixel are (xc, yc) then the coordinatesof his P neighbors (xp, yp) on the edge of the circle with radius R can becalculated with the sinus and cosines:

If the gray value of the center pixel is gc and the gray values of his neighborsare gp, withp = 0, ..., P − 1, than the texture T in the local neighborhoodof pixel (xc, yc) can be defined as:

$$x_p = x_c + Rcos(2\pi p/P) \quad \text{(III.1)}$$

$$y_p = y_c + Rsin(2\pi p/P) \quad \text{(III.2)}$$

✓ Represantation multi level/block

- Multi-Block (MB) [47] is a variant that replaces intensity values in the computation of descriptor with the mean intensity value of image blocks. The MB is a technique that divides the face into (n _ n) blocks. On each block, we apply a texture descriptor to get more features of the face.
- Multi-Level (ML) representation is a technique that combines the features extracted from consecutive di_erent MBs. In other terms, we extract features of the whole image, and then we divide it into di_erent blocks of di_erent sizes and extract features of each block. The entire features are then concatenated into one vector.

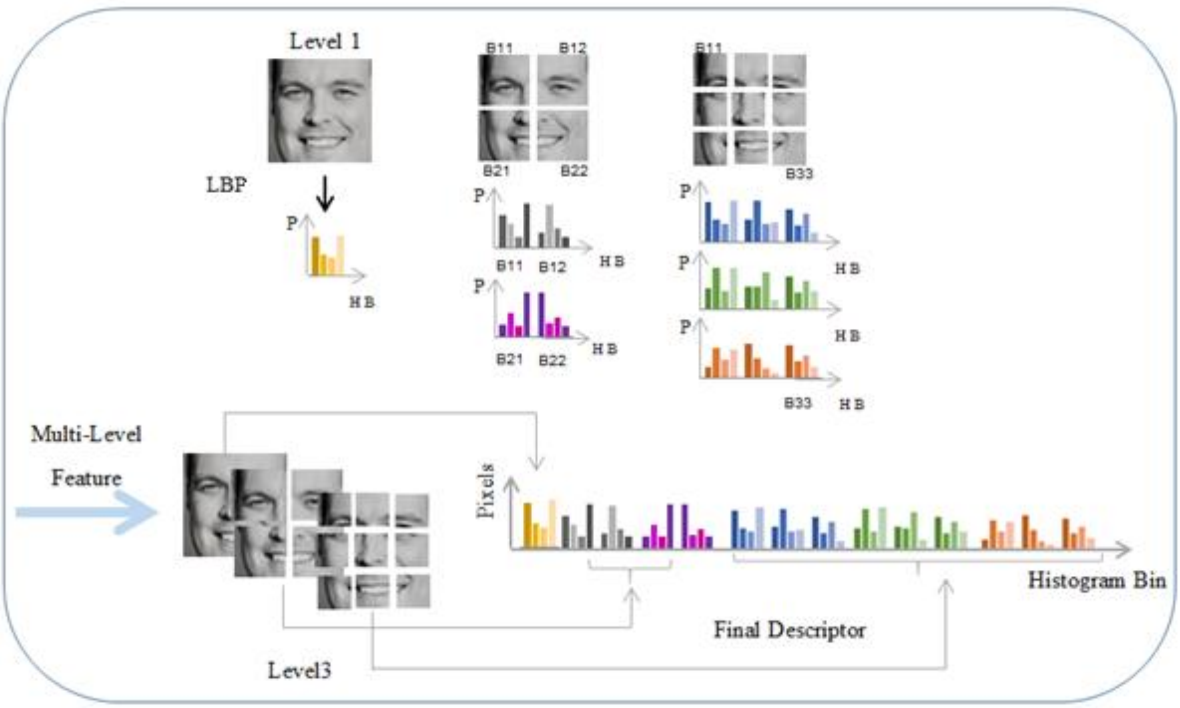


Figure III.5: Example of multi-level features extraction with (n = 3 _ 3 sub-blocks). [52]

III.2.3 Cross Validation

Cross-validation, sometimes called rotation estimation or out-of-sample testing is any of various similar model validation techniques for assessing how the results of a statistical analysis will generalize to an independent data set. It is mainly used in settings where the goal is prediction, and one wants to estimate how accurately a predictive model will perform in practice [46]. It is commonly used in applied machine learning to compare and select a model for a given predictive modeling problem because it is easy to understand, easy to implement, and results in skill estimates that generally have a lower bias than other methods.

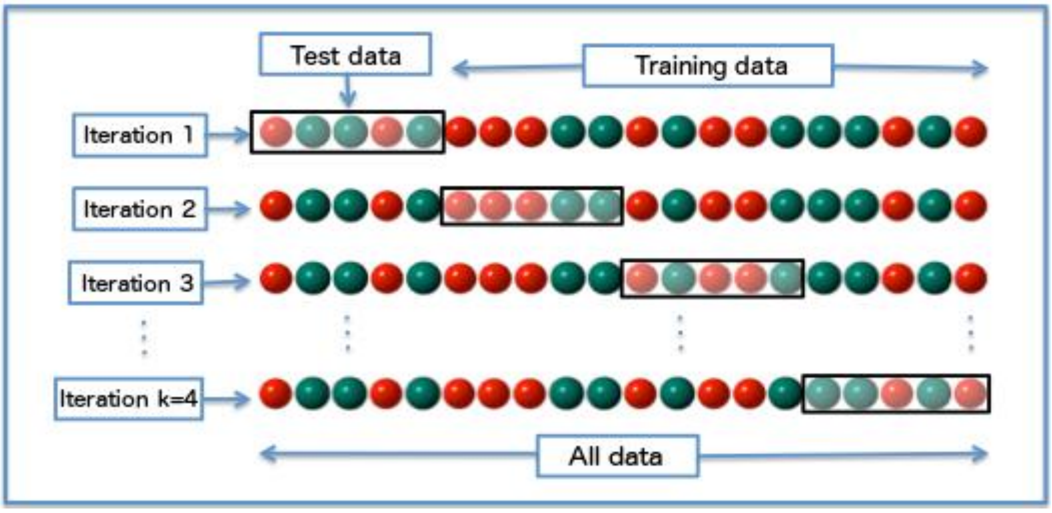


Figure III.6: Example of 4-cross validation. [52]

III.2.4Classification(cos-sin)

After the feature representations are adopted, the next step is image classi_cation. The choice of the classi_er has a great impact on the performance or recognition accuracy of the kinship veri_cation task. In terms of biometrics, classi_cation means _nding a proper identity for the query [48]. Generally, image classi_cation is performed by calculating the similarity between a target discriminating vector of feature and a query discriminating vector of feature [49]. In kinship veri_cation, the facial images are classi_ed into two classes. The _rst class is the true pairs of parents and children and the second one is the false pairs of parents and children. In this work, two classifiers are used:

Cosine distance (cos) [50]: Cosine similarity is a measure of similarity between two vectors and can be computed as:

$$d_{cos}=\sum_i \frac{xi\ yi}{\sqrt{\sum_i xi\hat{}2\sqrt{\sum_i yi\hat{}2}}} \qquad (III.3)$$

III.3Performance evaluation

In machine learning research, Receiver Operating Characteristic (ROC) [51] is an accepted method and widely used to show the e_ectiveness of a recognition system. ROC curve, can de_ned as a function of the decision threshold, it created by plotting the rate of true positive (ie. image classi_ed correctly as positive pairs or negative pairs), against the rate of false positive (ie. image classi_ed incorrectly) at various threshold settings. Each point on the ROC curve represents a positive/ negative pair corresponding to a particular decision threshold. therefore, our evaluation performance is based on ROC curve and accuracy. More speci_cally:

$$Accuracy=\frac{TP+TN}{P+N} \quad (III.4)$$

Where **TP** is the number of image that classied correctly as positive pairs, **TN** is the number of image that correctly classied as negative pairs, **P** is the number of all positive pairs, and **N** is the number of all negative pairs.

✓ Experimental Settings

For the experiments, each face is converted into gray-scale image (64×64 pixels). We aopted the *5-fold cross* validation strategy for experiments. For each of the four ubset, we construct all pairs of positive (true) and negative negative (false) samples for experiments. The positive samples are the true pairs and the negative samples are each parent with the selected child from the children's images who is not his/her true child.

We analysed the performance of *LBP* descriptor on KinFace in the *Wild-II (KinFaceW-II)* dataset. Finally, the cosine similarity of each test pair is computed. We report the mean verification accuracy of the four kinship subsets as the measure of system performance.

III.4Expremantal evaluation

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

- Divide the examined window into cells.
- For each pixel in a cell, compare the pixel to each of its neighbors (on its left-top, left-middle, left-bottom, right-top, etc.). Follow the pixels along a circle (Radius of circular pattern to select neighbors).
- Where the center pixel's value is greater than the neighbor's value, write "0". Otherwise, write "1". This gives an 8-digit binary number (which is usually converted to decimal for convenience).
- Compute the histogram, over the cell, of the frequency of each "number" occurring (i.e., each combination of which pixels are smaller and which are greater than the center). This histogram can be seen as a feature vector.
- Optionallynormalize the histogram.
- Concatenate (normalized) histograms of all cells. This gives a feature vector for the entire window.

- First, we tested the *mean area under ROC* on F-S relationship in with varying the number of different parameters, and then the number who is performed the best performance for all relationships including F-D, M-D, and M-S.
- To achieve the best performance, we tested different values of *Number of neighbors(P)*, *Radius(R)*, and *CellSize*. Finally, was fixed to: size ofeach block is (10 × 10) with neighborhood P = 8, a radius R = 2.The results are shown in Table III.1.

Parametrs		**Accuracy**
(P,R)	**CellSize**	FS
(4,1)	[32 ×32]	70.20
(4,1)	[16 × 16]	74.60
(4,1)	[8×8]	76.60
(4,1)	[4×4]	77.20
(8,2)	[32 ×32]	69.4
(8,2)	[16 × 16]	73.60
(8,2)	[8 ×8]	76.2
(8,2)	[32 ×32]	73.00
(16,2)	[8 ×8]	76.60
(16,4)	[8 ×8]	74.20

TableIII.1: different values of Number of neighbors(P), Radius(R), and CellSize.

III.4.1Analyse and result

We achieved the best results by dividing the face into several sections and changing the parameters each time. The results were obtained as shown in the tables III.2 and III.3.

nembre de block	f-s	f-d	m-s	m-d	Mean
2	81.00%	73.80%	75.20%	73.00%	75.75%
3	81.60%	75.60%	73.00%	73.20%	75.85%
4	82.20%	76.20%	74.60%	74.80%	76.95%
6	81.40%	77.00%	75.40%	75.20%	77.25%
8	80.60%	76.40%	75.60%	71.40%	76.00%
10	81.00%	73.80%	75.00%	71.40%	75.00%

TableIII.2:kinship virifecation accuracy in percentage on LBP using multi block

nembre de block	f-s	f-d	m-s	m-d	Mean
2	81.00%	74.20%	76.20%	75.00%	76.60%
3	82.40%	76.80%	74.80%	74.40%	77.10%
4	82.60%	77.60%	75.00%	75.40%	77.65%
6	82.60%	77.80%	76.80%	75.20%	78.10%
8	82.40%	76.80%	76.60%	73.80%	77.40%
10	81.80%	76.40%	77.40%	73.20%	77.20%

TableIII.3:kinship virifecation accuracy in percentage on LBP using multi level

Considering the average accuracy and the accuracy of all the kinship relations ML-LBP is the best performing method with accuracy equal to 78.10%.

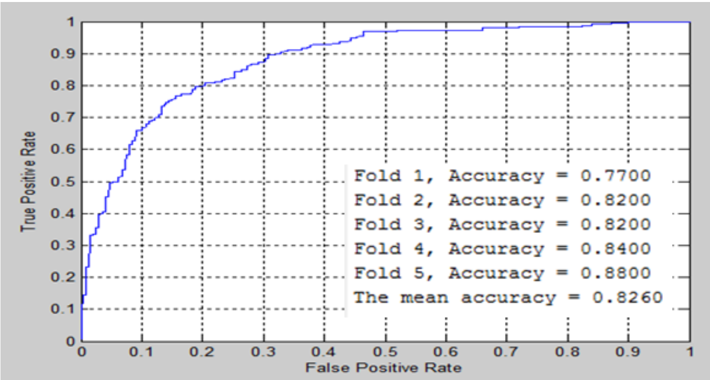
❖ **Multi block:** The results show that the average performance accuracy in the kinship task is (77.25 – 75.00).

❖ **Multi level:** The results show that the average performance accuracy in the kinship task is (78.1 - 76.6).

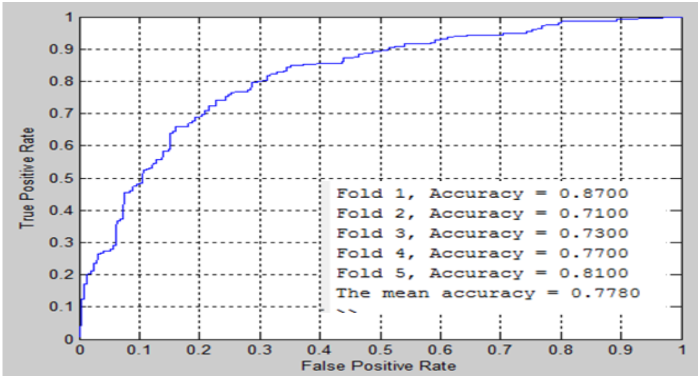
✓ We noticed that multi **level** results are better accurate than multi **block.** This is due that to the fact MLs representation gives more detailed information of the image than the MBs.

✓ It is remarkable that the performance of kinship verification on F-S relationship is better than other relationships.

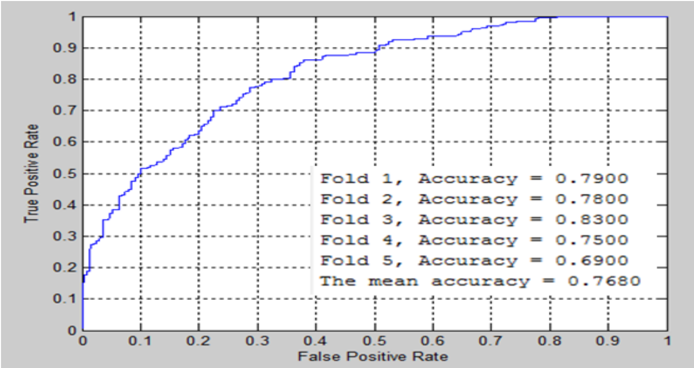
❖ Figure III.7 present the best curves obtained from the MATLAB, after changing the values in the database (kin face W-II).



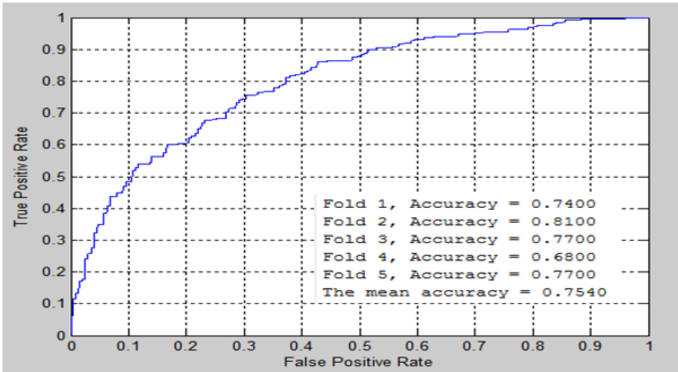
f-s



f-d



m-s



m-d

Figure III.7: the Roc curves of LBP method (multi level) obtained on kin face W-II data base .

✓ We note that when we divided the image on 8 and 10 the resolution was diminished. This is due to the existence of some distortions that appear when the image is divided into many parts (8 and 10).

✓ (The division of the image into many parts leads to the emergence of parts in the non-mission that obstruct the course of the study).

III.5Conclusion

In this study we addressed the automatic kinship verification from facial images of four links: F-S, F-D, M-S and M-D. Faces are described using LBP, Nearest neighbor (Cosine Distance) are used for classification.

For the proposed method, we tested the mean area under ROC on F-S relationship in KinFace in the Wild-II database with varying the number of different parameters, and then the number who is performed the best performance for all relationships including F-D, M-D, and M-S.

General Conclusion

General Conclusion

The purpose of the work presented in this dissertation was the kinship verification from face images. several analytical approaches are proposed in the literature. In our study we presented the kinship verification based on LBP features.

These methods have been validated on the basis of Kin Face in the Wild-II (KinFaceW-II) data, and have been implemented in Matlab.

More research to the parameters of the LBP-operator is recommended. It would be useful to carry out experiments for several kind of neighborhoods. On this way the optimal radius and the optimal number of sampling points on the circle can be determined.

In the future, more work should be carried out for developing of advanced methods for kinship verification from videos. Also, development of novel methods for Kinship verification from gait, voice (and possibly also recording new databases if needed) and development of multimodal methods for Kinship verification from gait and voice.

Bibliography

Bibliography

[1] Julian Ashbourn, "The Biometric White Paper" [© 2005 Applied Engineering, Inc., 7999 Knue Road, Suite 300, Indianapolis, Indiana 46250], 1999. Copyright Ashbourn 1999.

[2] Anil K. Jain and UmutUludag, "Hiding Biometric Data," IEEE, Vol. 25, No. 11, November 2003 [Department of Computer Science and Engineering, Michigan State University, 3115 Engineering Building, East Lansing, MI 48824] 2003. IEEE, Published by the IEEE Computer Society, IEEE Transactions on Pattern Analysis and Machine Intelligence, Copyright © 2003.

[3] "Palm Print Recognition," Office of Science &Technology Policy (OSTP),NSTC Subcommittee on Biometrics,NationalScience&Technology Council (NSTC) Committees onTechnologyandHomeland&National Security, Washington, DC, March 27, 2006.

[4] "Palm Print Recognition," Office of Science &Technology Policy (OSTP),NSTC Subcommittee on Biometrics,NationalScience&Technology Council (NSTC) Committees onTechnologyandHomeland&National Security, Washington, DC, March 27, 2011b.

[5] Podio, F. (2011) 'Published International Biometric Standards Developed', by ISO/IEC JTC 1/SC 37 –Biometrics and Adopted by INCITS as INCITS/ISO/IEC Standards, pp.1-16.

[6] ISO (2006a) ISO/IEC 19784-1:2006 - Information technology –Biometric application programming interface -- Part 1: BioAPI specification. Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33922 (Accessed: 21 January 2015).

[7] NIST (2008) NIST/ITL Conformance Test Suite for Patron Format A Data Structures Speci-fied in ANSI INCITS , Common Biometric Exchange Formats Framework (CBEFF).

[8] NSTC (2011b) 'The National Biometrics Challenge', National Science and Technology Council Subcommittee on Biometrics and Identity Management.

[9] Clarke, (2011) Transparent user authentication: biometrics, RFID and behavioural profiling. London: Springer London. doi: 10.1007/978-0-85729-805-8.

[10] Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A. and Bondavalli, A.(2014) 'Continuous and Transparent User Identity Verification for Secure Internet

[11] Services', IEEE Transactions on Dependable and Secure Computing, pp(99), pp. 1–14.doi: 10.1109/TDSC.2013.2297709.Nanavati, S., Thieme, M. and Nanavati, R. (2002)

Biometrics Identity Verification in a Networked World. Edited by M. Eldridge and A. Obi. New York: Robert Ipsen.

[12] H. and Satyanarayana, R. (2012) ‘Biometric Authentication as a Service on Cloud: Novel Solution’, International Journal of Soft Computing and Engineering, 2(4), pp. 163–165.

[13] Biometrics Institute (2013) Biometrics Institute Industry Survey 2013, 1-6.

[14] Mokadem A .2018. Efficient person identification by Finger-Knuckle-Print based on Discrete Cosine Transform Network . Master Academic Systems Of Communications. UnivOuargla, 4-37p

[15] Woodward, J. D. J., Orlans, N. M. and Higgins, P. T. (2003) Biometrics: Identity Assurance in the Information Age. New York: McGraw Hill/Osborne.

[16] Nanavati, S., Thieme, M., Raj, N., &Nanavati, R. (2002). Biometrics: Identity Verification in a Networked World. New York, NY, USA: John Wiley & Sons, Inc.

[17] Miller, A. (2015). Current and Future Uses of Biometric Data and Technologies.

[18] Wright, D., &Kreissl, R. (2014). Surveillance in Europe. Taylor & Francis. Retrieved from https://books.google.dz/books?id=9amQBAAAQBAJ

[19] M. Georgopoulos, Y. Panagakis, and M. Pantic, \Modelling of facial aging and kinship: A survey," Image and Vision Computing, 2018.

[20] T. R. Alley, Social and applied aspects of perceiving faces. Psychology Press, 2013.

[21] J. H. Park, M. Schaller, and M. Van Vugt, \Psychology of human kin recognition: Heuristic cues, erroneous inferences, and their implications." Review of General Psychology, vol. 12, no. 3, p. 215, 2008.

[22] I. STRAVINSKY, \Rodney needham remarks on the analysis of kinship and marriage," Rethinking kinship and marriage, vol. 11, p. 1, 2004.

[23] D. Jones, \The generative psychology of kinship: Part 1. cognitive universals and evolutionary psychology," Evolution and Human Behavior, vol. 24, no. 5, pp. 303{319, 2003.

[24] L. T. Maloney and M. F. Dal Martello, \Kin recognition and the perceived facial similarity of children," Journal of Vision, vol. 6, no. 10, pp. 4{4, 2006.

[25] M. F. Dal Martello and L. T. Maloney, \Where are kin recognition signals in the human face?" Journal of Vision, vol. 6, no. 12, pp. 2{2, 2006.

[26] L. M. DeBruine, F. G. Smith, B. C. Jones, S. C. Roberts, M. Petrie, and T. D. Spector,\Kin recognition signals in adult faces," Vision research, vol. 49, no. 1, pp. 38{43, 2009.

[27] K. Finkler, C. Skrzynia, and J. P. Evans, \The new genetics and its consequences for family, kinship, medicine and medical genetics," Social Science & Medicine, vol. 57, no. 3, pp. 403{412, 2003.

[28] J. H. Relethford, \Bioassay of kinship from continuous traits," Human biology, pp. 689{700, 1980.

[29] A. Alvergne, C. Faurie, and M. Raymond, \Differential facial resemblance of young children to their parents: who do children look like more?" Evolution and Human behavior, vol. 28, no. 2, pp. 135{144, 2007.

[30] L. M. DeBruine, \Resemblance to self increases the appeal of child faces to both men and women," Evolution and Human Behavior, vol. 25, no. 3, pp. 142{154, 2004.

[31] H. Dibeklioglu, A. Ali Salah, and T. Gevers, \Like father, like son: Facial expression dynamics for kinship verification," in Proceedings of the IEEE International Conference on Computer Vision, pp. 1497{1504, 2013.

[32] G. Guo and X. Wang, \Kinship measurement on salient facial features," IEEE Transactions on Instrumentation and Measurement, vol. 61, no. 8, pp. 2322{2325, 2012.

[33] G. Somanath and C. Kambhamettu, \Can faces verify blood-relations?" in Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on. IEEE, pp. 105{112, 2012.

[34] Yan H, Jiwen L, Deng W, Zhou X (2014) Discriminative multi-metric learning for kinship verification

[35] Fang R, Tang KD, Snavely N, Chen T (2010) Towards computational models of kinship verification. In: 2010 17th IEEE international conference on image processing (ICIP). IEEE, pp 1577–1580

[36] Shao M, Xia S, Yun F (2011) Genealogical face recognition based on ubkinface database. In: 2011 IEEE computer society conference on computer vision and pattern recognition workshops (CVPRW). IEEE, pp 60–65

[37] Bottino AG, De Simone M, Laurentini A, Vieira T (2012) A new problem in face image analysis: finding kinship clues for siblings pairs 50 Vieira TF, Bottino A, Ul Islam I (2013) Automatic Verification of Parent-Child Pairs from Face Images, pp 326–333. Springer

[38] Vieira TF, Bottino A, Laurentini A, De Simone M (2013) Detecting siblings in image pairs. Vis Comput:1–13

[39] Kohli N, Singh R, VatsaM(2012) Self-similarity representation of weber faces for kinship classification. In: 2012 IEEE Fifth international conference on biometrics: theory, applications and systems (BTAS). IEEE, pp 245–250

[40] M. Georgopoulos, Y. Panagakis, and M. Pantic, \Modelling of facial aging and kinship: A survey," Image and Vision Computing, 2018.

[41] T. R. Alley, Social and applied aspects of perceiving faces. Psychology Press, 2013.

[42] J. H. Park, M. Schaller, and M. Van Vugt, \Psychology of human kin recognition: Heuristic cues, erroneous inferences, and their implications." Review of General Psychology, vol. 12, no. 3, p. 215, 2008.

[43] T. Ahonen, A. Hadid, and M. Pietikainen, \Face description with local binary patterns: Application to face recognition," IEEE transactions on pattern analysis and machine intelligence, vol. 28, no. 12, pp. 2037{2041, 2006.

[44] X. Wu, E. Boutellaa, M. B. L_opez, X. Feng, and A. Hadid, \On the usefulness of color for kinship veri_cation from face images," in Information Forensics and Security (WIFS), 2016 IEEE International Workshop on. IEEE, pp. 1{6, 2016.

[45] Szegedy, C., Liu, W., Jia, Y., et al.: 'Going deeper with convolutions'. Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition, Boston, USA, 2015, pp.1–9

[46] R. Kohavi et al., \A study of cross-validation and bootstrap for accuracy estimation and model selection," in Ijcai, vol. 14, no. 2. Montreal, Canada, pp. 1137-1145, 1995.

[47] L. Zhang, R. Chu, S. Xiang, S. Liao, and S. Z. Li, \Face detection based on multi-block lbp representation," in International conference on biometrics. Springer, pp. 11{18, 2007.

[48] S. Xia, M. Shao, and Y. Fu, \Kinship veri_cation through transfer learning," in IJCAI, pp. 2539{2544, 2011.

[49] V. Vapnik, \The nature of statistical learning theory springer new york google scholar," 1995.

[50] E. Vezzetti and F. Marcolin, Similarity measures for face recognition. Bentham Science Publishers, 2015.

[51] J. A. Hanley and B. J. McNeil, \The meaning and use of the area under a receiver operating characteristic (roc) curve." Radiology, vol. 143, no. 1, pp. 29{36, 1982.

[52] Dr.Tedjani Amina 'Automatic kinship verification' ;submitted for the degree of doctor 2018/2019

[53] B.K julsing 'face recognition with local binary patterns 'may11,2007