



People's Democratic Republic of Algeria

UNIVERSITY OF KASDI MERBAH OUARGLA



**Faculty of New Technologies of Information and
Communication**

Department of Electronics and Telecommunications

FINAL STUDY DISSERTATION

In the aim of obtaining MASTER Degree - ACADEMIC

Domain: Science and Technology

Specialty: Electronic

Option: Automatic

Presented by :

MEISSA Aymen

TRABELSI Chemseddine

Topic

Effecient algorithms For Biometric Anti-spoofing

Was Publicly Debated in: May 2017 in front of The Examining Committee

Composed From:

Dr.	A. MENNCER	MCB	President	UKM Ouargla
Dr.	D. SAMAI	MCB	Supervisor	UKM Ouargla
Mr.	A. BENLAMOUDI	Doctorant	Co- Supervisor	UKM Ouargla
Dr.	H. ELAGOUN	MCB	Examiner	UKM Ouargla

Academic year : 2016 /2017

Acknowledgments

In the Name of Allah, the Most Merciful, the Most Compassionate all praise be to Allah, the Lord of the worlds; and prayers and peace be upon Mohamed His servant and messenger.

First and foremost, we must acknowledge our limitless thanks to Allah, the Ever-Magnificent; the Ever-Thankful, for His help and bless. We are totally sure that this work would have never become truth, without His guidance.

we owe a deep debt of gratitude to our university for giving us an opportunity to complete this work.

we are grateful to some people, who worked with us from the beginning till the completion of the present research particularly our supervisor Dr. Djamel SAMAI, who has been always generous during all phases of the research, and we highly appreciate the efforts expended by Mr.Azeddine BENLAMOUDI and Mr.Khaled BENSID

Our most grateful thanks to all those who have contributed to the realization of this memory.

DEDICATION

*I dedicate this modest work to those who are the source of my inspiration
and my courage.*

*To my dear mother, who always gives me hope to live and who has never
stopped praying for me.*

*To my dear father, for his encouragement and support, And above all for
his sacrifice so that nothing will hinder The course of my studies.*

*To all the professors and teachers who have followed me throughout my
schooling and who have allowed me to succeed in my studies.*

To my dear brother

To my sisters

All my friends

Meissa Aymen

DEDICATION

*I dedicate this modest work to those who are the source of my inspiration
and my courage.*

*To my dear mother, who always gives me hope to live and who has never
stopped praying for me.*

To my dear Father, God have mercy on him.

*To my dear Brother SAID, for his encouragement and support, And above
all for his sacrifice so that nothing will hinder The course of my studies.*

*To all the professors and teachers who have followed me throughout my
schooling and who have allowed me to succeed in my studies.*

To my dear brothers

To my sisters

All my friends

TRABELSI Chemseddine

Table of Contents.....	I
List of Figures.....	II
List of Tables.....	III
Acronyms.....	IV

	General Introduction	1
	Thesis Outline.....	2
I.	Chapter I : Overview on biometrics	
<i>I.1.</i>	Introduction.....	3
<i>I.2.</i>	Overview of biometrics.....	3
<i>I.3.</i>	Technical of biometric.....	4
<i>I.3.1.</i>	Physical biometrics (Morphological).....	4
<i>I.3.2.</i>	Behavioral biometrics.....	10
<i>I.3.3.</i>	Biological biometrics.....	15
<i>I.4.</i>	Architecture of a biometric system.....	16
<i>I.5.</i>	Comparative representation between some Biometric Technical.....	18
<i>I.6.</i>	Applications of biometric systems.....	19
<i>I.7.</i>	Performance evaluation of Biometric system.....	19
<i>I.8.</i>	Conclusion.....	21
II.	Chapter II : Anti-spoofing Methods	
<i>II.1.</i>	Indroduction.....	22
<i>II.2.</i>	Overview On Biometric Anti-Spoofing.....	22
<i>II.2.1.</i>	Spoofing attacks in face recognition.....	22
	Photo Attacks.....	23
	Video Attacks.....	23
	Mask Attacks.....	24
<i>II.2.2.</i>	State of the art face anti-spoofing.....	24
<i>II.2.3.</i>	Face anti spoofing techniques.....	24
	Sensor-level techniques.....	25
	Feature-level techniques.....	26
	Score-level techniques.....	27
<i>II.3.</i>	Face Anti-Spoofing Methods.....	28
<i>II.3.1.</i>	Face anti-spoofing preprocessing.....	28
	Face detection.....	28
	Why Viola-Jones algorithm?.....	28
	Eyes localization.....	30
	Face normalization.....	30
	Face representation.....	31
<i>II.3.2.</i>	Feature extraction.....	32
	Local Binary Pattern.....	32
	Local Phase Quantization.....	33
	Binarized Statistical Image Features.....	35
<i>II.3.3.</i>	Classification.....	36
	The advantages of support vector machines are.....	38
	The disadvantages of support vector machines include.....	38
<i>II.4.</i>	Conclusion.....	38
III.	Chapter III: Experemental results and discusssion.....	
<i>III.1.</i>	Database and protocol.....	40

<i>III.2.</i>	Proposed approach.....	41
<i>III.3.</i>	The experimental results.....	42
<i>III.3.1.</i>	results obtained in the absence of the stasm.....	42
<i>III.3.1.1.</i>	Extraction features for one block.....	42
<i>III.3.1.2.</i>	Extraction features for Multi- block and multi-level	44
<i>III.3.2.</i>	Comparative study shows the role of Stasm.....	48
<i>III.3.3.</i>	Comparative analysis between MB and ML with and without fisher score	50
<i>III.4.</i>	Conclusion.....	53
<i>III.5.</i>	General conclusion and perspectives.....	54
	Bibliography.....	55

List of figures

Figure I.1	: Fingerprint.....	5
Figure I.2	: Hand geometry.....	6
Figure I.3	: Iris scans.....	7
Figure I.4	: The Face recognition.....	8
Figure I.5	: Palm print recognition.....	9
Figure I.6	: The Retina scans.....	10
Figure I.7	: The voice print recognition.....	11
Figure I.8	: Signature Dynamics.....	12
Figure I.9	: Keystroke dynamics.....	13
Figure I.10	: Gait dynamics.....	14
Figure I.11	: DNA patterns.....	15
Figure I.12	: Hand veins.....	16
Figure I.13	: Generic architecture of a biometric system.....	17
Figure I.14	: Illustration of FRR and FAR.....	20
Figure I.15	: ROC curve.....	21
Figure II.1	: Example photo attack.....	23
Figure II.2	: Example video attack.....	23
Figure II.3	: Example mask attack.....	24
Figure II.4	: General classification of anti-spoofing methods.....	25
Figure II.5	: General diagram of a biometric system.....	25
Figure II.6	: Example Face detection.....	29
Figure II.7	: Example Eyes localization.....	30
Figure II.8	: Example Face normalization.....	31
Figure II.9	: Example Multi-Blocks.....	31
Figure II.10	: Example Multi-level.....	32
Figure II.11	: The basic LBP operator.....	33
Figure II.12	: Construction of LPQ descriptor.....	35
Figure II.13	: Example of a linear classifier.....	37
Figure II.14	: Example of hyperplane.....	37
Figure II.15	: Example of SVM Classifier.....	38
Figure III.1	: The proposed approach.....	41
Figure III. 2	: Illustration the role of Stasm.....	49
Figure III. 3	: Comparison between the descriptors.....	50
Figure III. 4	: Comparison of the results (in EER %) between ML-LBP and MB-LBP approach without (Fisher) and with (Fisher).....	50
Figure III. 5	: Comparison of the results (in EER %) between ML-LPQ and MB-LPQ approach without (Fisher) and with (Fisher).....	51
Figure III. 6	: Comparison of the results (in EER %) between ML-BSIF and MB-BSIF approach without (Fisher) and with (Fisher).....	51
Figure III. 7	: ROC curve with Stasm-Fisher.....	52
Figure III. 8	: Performance (DET curve) of the proposed approach with (Fisher)	52
Figure III. 9	: FAR vs. FRR Curves.....	53

List of Tables

Table 1	: Comparison between some biometric features.....	18
Table 2	: Number of images in the training set and test set.....	40
Table 3	: Obtained EER result without Stasm.....	42
Table 4	: The different LBP results.....	43
Table 5	: The different LPQ results.....	43
Table 6	: The different BSIF results.....	44
Table 7	: The different MB-LBP results.....	45
Table 8	: The different ML-LBP results.....	45
Table 9	: The different MB-LPQ results.....	46
Table 10	: The different ML-LPQ results.....	46
Table 11	: The different MB-BSIF results.....	47
Table 12	: The different ML-BSIF results.....	47
Table 13	: Performance comparison between our proposed approach and the best results without stasm in the same database.....	48
Table 14	: Comparison between the proposed countermeasures with stasm.....	49

Acronyms

ACC	: Accuracy
BSIF	: Binarized Statistical Image Features
DB	: Data Base
DET	: Detection error tradeoff
DNA	: Deoxyribo Nucleic Acid
EER	: Equal Error Rate
FAR	: False Acceptance Rate
FRR	: False Rejection Rate
GAR	: Genuine Acceptance Rate
IBG	: International Biometric Group
LBP	: Local Binary Pattern
LPQ	: Local Phase Quantization
MB	: Multi-Block
ML	: Multi-Level
PIN	: Personal Identification Number
ROI	: Region Of Interest
ROC	: Receiver Operating Curve
SVM	: Support Vector Machine



GENERAL

INTRODUCTION



GENERAL INTRODUCTION

From time to time we hear all over the world about the crimes of credit card fraud, identity thefts by criminals, or security breaches in a company or government building. Furthermore to the international growth of communications, both in volume and diversity (physical displacement, financial transaction, access to services, etc...), so this is why we need to ensure the identity of individuals.

Nowadays we leave our biometric characteristics (finger prints, faces, voice recorded, etc...) everywhere in our day to day lives, so the chance of someone lifting them and copying them is real. As we mentioned earlier, there are various biometric traits one of the them is face, it's used in various fields for identification and authentication of the person. An important difference with other biometric modalities is that faces can be captured from some distance away, with for example surveillance cameras and can be applied without the subject knowing that he is being observed. Unfortunately, in spite of increasing use of face recognition systems, there are face spoofing attacks are also being under usage. Face spoofing techniques can be changed based on the current face recognition system. In this work we will focused on photo attacks.

In the area of anti-spoofing assessment as in other biometric related scenarios, two main types of evaluations are possible: algorithm-based (Software), this type of evaluation is therefore well suited to assess feature-level techniques. The second type is system-based (Hardware); it is suited to assess sensor-level schemes where acquisition devices are specific for each system.

This work aims at the realization of uni-modal anti-spoofing system based on the methods: LBP (and their MB, ML), LPQ (and their MB, ML), BSIF (and their MB, ML) with and without Fisher score, SVM classifier, than we will evaluate the system in term of Equal Error Rate performance criteria (EER %).

Thesis Outline:

In this dissertation thesis, we will try to achieve this objective through three chapters, several notions and concepts of biometrics and realization of an anti-spoofing face system will be addressed:

- Chapter I: overview on biometrics.
- Chapter II: Face Anti-Spoofing methods.
- Chapter III: Experimental results and discussion.

Finally, we will conclude this paper with a general conclusion in which we will discuss about obtained results and draw out perspectives and proposals with the view that this work will serve as an introduction to further research in this field.



Chapter I

OVERVIEW ON BIOMETRICS

I.1 Introduction

Human recognition has become an important topic as the need and investments for security applications grow continuously. Biometrics enable reliable and efficient identity management human characteristics's that are permanent, universal and easy to access. This is why the topic of biometrics attracts higher attention today.

In this chapter, we initially give some basic concepts and definitions related to biometrics. Then we explain how a biometric systems work and how do evaluate them.

I.2 Overview of biometrics

For thousands of years, humans have used body characteristics such as face, voice, gait, and so on to recognize each other. In the mid-19th century, ‘Alphonse Bertillon’, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using various body measurements (for example, height, length of arms, feet, and fingers) to identify criminals. In the late 19th century, just as his idea was gaining popularity, it was eclipsed by a far more significant and practical discovery: the distinctiveness of human fingerprints. Soon after this discovery, many major law enforcement departments embraced the idea of “booking” criminals’ finger prints and storing them in databases (initially, card files). Later, police gained the ability to “lift” leftover, typically fragmentary, fingerprints from crime scenes (commonly called latents) and match them with fingerprints in the database to determine criminal’s identities. Day by day biometric technology is gaining more popularity in the field of security system in recent few years ago. Today, biometric has come up as an independent field of study with precise technologies of establishing personal identities [1].

With increasing use of Information Technology in the field of medication, banking, science ...etc, there is an immense need to protect the systems and data from unauthorized users.

The term "Biometric" come from the Greek words "bio" (life) and "metric" (to measure). Biometric is technology used for measuring and analyzing a person's unique characteristics. There are various traits present in humans, which can be used as biometrics information. Each biometric informations that can discriminate individuals is considered as a biometric modality.

The biometric modalities fall under three types:

- ✚ *Behavioral characteristics* such as voice and accent of speech, signature dynamic, or the way of typing keys of computer keyboard (keystroke dynamic)...etc.
- ✚ *Physical characteristics* such as finger prints, color of iris, hand geometry, face and retina ...etc.
- ✚ *Biological characteristics* such as DNA, hand veins...etc.

Ideal biometric information should respect the following properties:

- ✓ **Universality:** all individuals must be characterized by this information.
- ✓ **Uniqueness:** this information must be as dissimilar as possible for two different individuals.
- ✓ **Permanency:** it should be present during the whole life of an individual.
- ✓ **Collectability:** it can be measured in an easy manner.
- ✓ **Acceptability:** it concerns the possibility of a real use by users. [2]

I.3 Technical of biometric

There are several biometric modalities used in various sectors, one can distinguish three categories:

I.3.1 Physical biometrics (Morphological)

The first question that needs to be asked is what Physical biometrics is. Physical biometrics deals with the human features that we were born with. They usually are dictated by our genetics. The feature data are gathered from our body characteristics.

a) Fingerprint

Fingerprint is one of the oldest and most popular recognition techniques. Every person has a unique fingerprint which is composed of ridges, grooves, and direction of the lines. There are three basic patterns of ridges namely, **arch**, **loop**, and **whorl**. The uniqueness of a fingerprint is determined by these features as well as **minutiae features** such as bifurcation and spots ridge endings. That modality is largely regarded as an accurate biometric recognition method. Today, fingerprint scanners are available at low cost and increasingly integrated in laptops and other portable ICT devices. This type of system is used by financial institutions for their employees and customers. It is also found in hospitals, schools, airports, identity cards, passports, driving licenses and many other applications. [3]

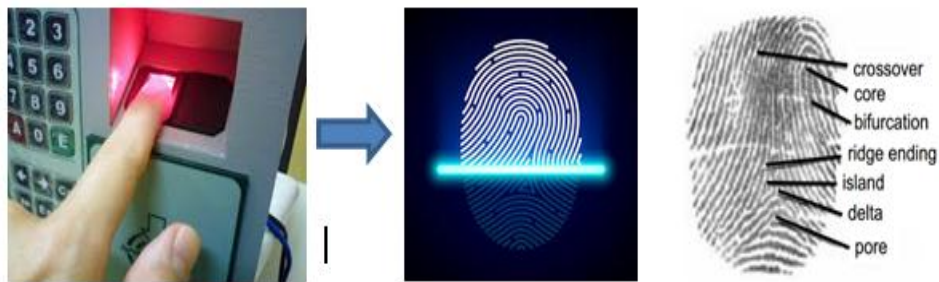


Figure I.1 : Fingerprint.

Merits of Finger Recognition System

- It is the most contemporary method.
- It is the most economical method.
- It is highly reliable and secure.
- It works on a small template size, which speeds up the verifying process.
- It consumes less memory space.

Demerits of Finger Recognition System

- Scars, cuts or absence of finger can hinder the recognition process.
- The systems can be fooled by using artificial fingers made of wax.
- It involves physical contact with the system.
- They leave the pattern of the finger behind at the time of entering the sample.

Applications of Finger Recognition System

- Verification of driver-license authenticity.
- Checking validity of driving license.
- Border Control/Visa Issuance.
- Access control in organizations.

b) Hand geometry

It includes measuring length and width of palm, surface area, length and position of fingers, and overall bone structure of the hand. A person's hand is unique and can be used to identify a person from others.

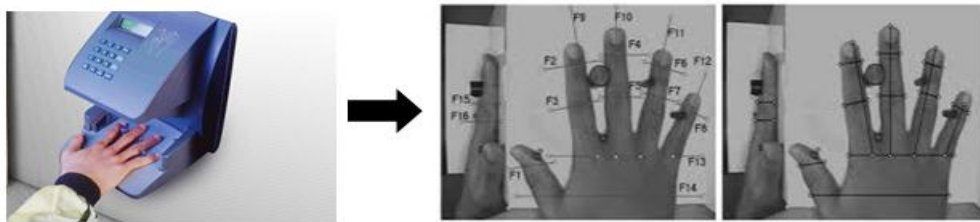


Figure I.2: Hand geometry.

Merits of Hand Geometry Recognition System

- It is sturdy and user friendly.
- The changes in skin moisture or texture do not affect the result.

Demerits of Hand Geometry Recognition System

- Since the hand geometry is not unique, it is not very reliable.
- It is effective in case of adults and not for the growing children.
- If candidate's hand is with jewelry, plaster, or arthritis, it is likely to introduce a problem.

Applications of Hand Geometry Recognition System

- Nuclear power plants and military use Hand Geometry Recognition for access control.

c) Iris patterns

The iris is a part of the eyeball. The iris is recognizable by its circular shape. It is he who determines what is commonly called the color of the eyes. The iris is inseparable from the pupil. Iris scanning biometrics measures the unique patterns in the colored circle of your eye to verify and authenticate your identity. The acquisition of the iris is carried out by means of a camera to compensate for the inevitable movements of the pupil.

The acquisition of the iris is carried out by means of a camera to compensate for the inevitable movements of the pupil. It is very sensitive (precision, reflection ...) and relatively unpleasant for use because the eye must remain wide open and it is illuminated by a light source to ensure a correct contrast. [4]

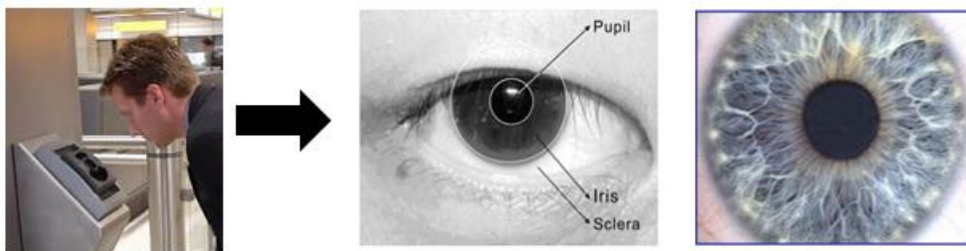


Figure I.3: *Iris scans.*

Merits of Iris Recognition System

- It is highly accurate as the chance of matching two irises is 1 in 10 billion people.
- It is highly scalable as the iris pattern remains same throughout a person's lifetime.
- The candidate need not remove glasses or contact lenses; they do not hamper the accuracy of the system.
- It involves no physical contact with the system.
- It provides instant verification *2to5seconds* because of its small template size.

Demerits of Iris Recognition System

- Iris scanners are expensive.

- High quality images can fool the scanner.
- A person is required to keep his/her head very still for accurate scanning.

Applications of Iris Recognition System

- National security and Identity cards such as Adhaar card in India.
- Google uses iris recognition for accessing their datacenters.

d) Face recognition

The face is certainly the biometric characteristic that humans use most naturally to identify with each other, which may explain why it is generally very well accepted by users. The acquisition system is either a camera or a digital camera.

The difficulty of face recognition varies greatly depending on whether the acquisition is in a controlled environment or not. In a controlled environment, parameters such as the background, direction and intensity of the light sources, the angle of the shooting, the distance from the camera to the subject are parameters controlled by the system. In an uncontrolled environment, a series of pre-treatments are often necessary before making the actual recognition. The presence or absence of faces must first be detected in the image (detection face). The face must then be segmented (face segmentation). [5]

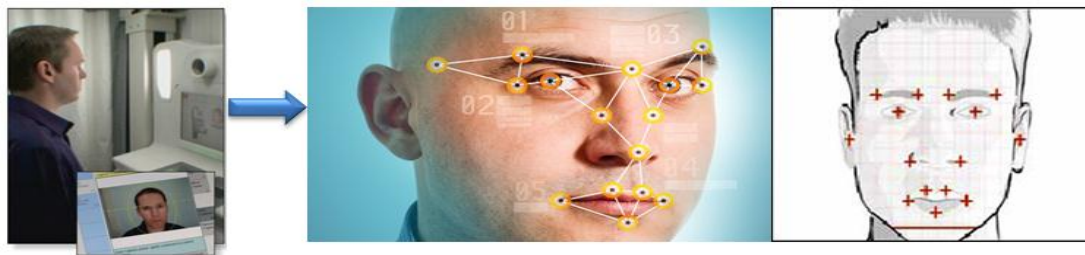


Figure I.4: The Face recognition.

Merits of Facial Recognition System

- It offers easy storage of templates in database.
- It reduces the statistic complexities to recognize face image.
- It involves no physical contact with the system.

Demerits of Facial Recognition System

- Facial traits change over time.
- Uniqueness is not guaranteed, for example, in case of identical twins.
- If a candidate face shows different expressions such as light smile, then it can affect the result.
- It requires adequate lighting to get correct input.

Applications of Facial Recognition System

- General Identity Verification.
- Verification for access control.
- Human-Computer Interaction.
- Criminal Identification.
- Surveillance.

e) Palmprint

The palm of the hand is the inner part of the hand (part not visible when the hand is closed) from the wrist to the roots of the fingers. Thus, the palmar impression is none other than the impression (image) of the palm of the hand made by the pressure of the latter on a given surface. In other words, it can be defined as the model of the palm of the hand illustrating the physical characteristics of the pattern of the skin such as the lines (main and wrinkles), points, minuteness and texture.

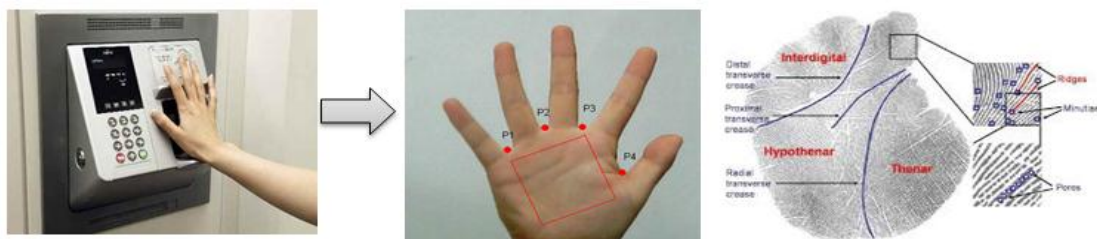


Figure I.5: *Palm print recognition.*

f) Retina scans

Retina is the lining layer at the back of the eyeball that covers 65% of the eyeball's inner surface. It contains photosensitive cells. Each person's retina is unique

due to the complex network of blood vessels that supply blood. It is a reliable biometric as the retina pattern remains unchanged throughout the person's life, barring the patterns of persons having diabetes, glaucoma, or some degenerative disorders.

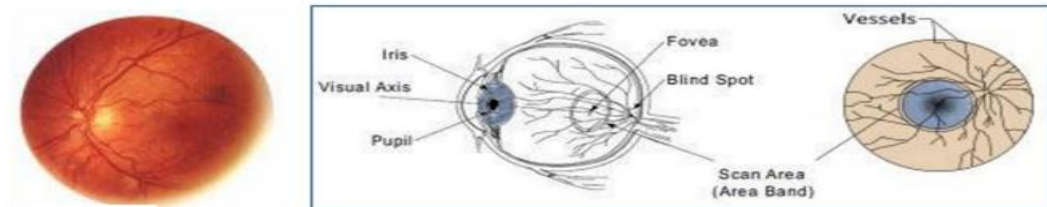


Figure I.6: The Retina scans

Merits of Retinal Scanning System

- It cannot be forged.
- It is highly reliable as the error rate is 1 out of a crore samples which is almost 0.

Demerits of Retinal Scanning System

- It is not very user friendly as the user needs to maintain steadiness that can cause discomfort.
- It tends to reveal some poor health conditions such as hypertension or diabetes, which causes privacy issues.
- Accuracy of the results is prone to diseases such as cataracts, glaucoma, diabetes, etc.

Applications of Retinal Scanning System

- It is practiced by some government bodies such as CID, FBI, etc.
- Apart from security applications, it is also used for ophthalmological diagnostics.

I.3.2 Behavioral biometrics

This group consists of methods measuring human features indirectly. Behavioral biometrics measures the repeated activities we make in our daily life.

Every human takes actions in his own way, differing from the manner in which others perform them.

a) Voice print

The human voice is influenced by the physiological characteristics of lungs, tongue, throat ...etc. and its behavioral features evolve and change over time. They can be influenced by factors such as age, illnesses, mood, conversational partner or surrounding noise.



Figure I.7: The voice print recognition.

Merits of Voice Recognition

- It is easy to implement.

Demerits of Voice Recognition

- It is susceptible to quality of microphone and noise.
- The inability to control the factors affecting the input system can significantly decrease performance.
- Some speaker verification systems are also susceptible to spoofing attacks through recorded voice.

Applications of Voice Recognition

- Performing telephone and internet transactions.
- Working with Interactive Voice Response *IRV*-based banking and health systems.
- Applying audio signatures for digital documents.
- In entertainment and emergency services.
- In online education systems.

b) Signature dynamics

Signature verification works by considering a variety of factors, including both features of the signature itself (the static product) and details on how the signature is generated (the dynamic process). The signature itself provides geometry, curvature, and shape information of individual characters and complete words. How a signature is generated provides additional information on stroke direction, speed, pen up and pen down events, and pressure metrics. Hand written signatures are electronically captured with a digitizing tablet and stylus.

Many signing tablets are commercially available today. They come in a variety of sizes, options, and performance characteristics, as some are intended for graphics applications beyond just electronic signature capture. [6]

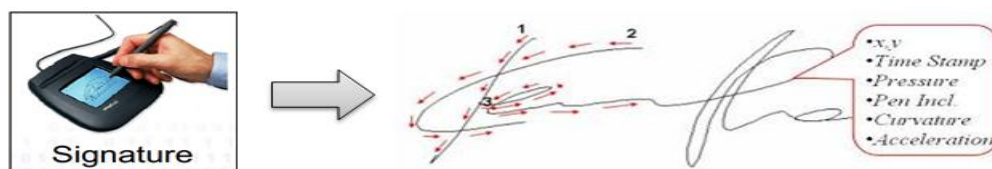


Figure I.8: Signature Dynamics

Merits of Signature Recognition System

- Signature recognition process has a high resistance to imposters as it is very difficult to imitate the behavior patterns associated with the signature.
- It works very well in high amount business transactions. For example, Signature recognition could be used to positively verify the business representatives involved in the transaction before any classified documents are opened and signed.
- It is a non-invasive tool.
- We all use our signature in some sort of commerce, and thus there are virtually no privacy rights issues involved.
- Even if the system is hacked and the template is stolen, it is easy to restore the template.

Demerits of Signature Recognition System

- The live sample template is prone to change with respect to the changes in behavior while signing. For example, signing with a hand held in plaster.
- User need to get accustomed of using signing tablet. Error rate is high till it happens.

Applications of Signature Recognition System

- It is used in document verification and authorization.
- The Chase Manhattan Bank, Chicago is known as the first bank to adopt Signature Recognition technology.

c) Keystroke dynamics

Monitoring keystroke dynamics is considered to be an effortless behavioral based method for authenticating users which employs the person's typing patterns for validating his/her identity. Keystroke dynamics is “not what you type, but how you type.” In this approach, the user types in text, as usual, without any kind of extra work to be done for authentication. [7]

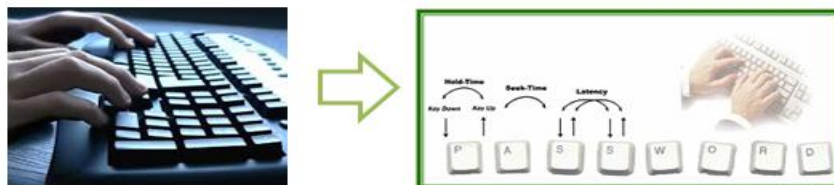


Figure I.9: Keystroke dynamics.

Merits of Keystroke Recognition System

- It needs no special hardware to track this biometric.
- It is a quick and secure way of identification.
- A person typing does not have to worry about being watched.
- Users need no training for enrollment or entering their live samples.

Demerits of Keystroke Recognition System

- The candidate's typing rhythm can change between a number of days or within a day itself because of tiredness, sickness, influence of medicines or alcohol, change of keyboard, etc.
- There are no known features dedicated solely to carry out discriminating information.

Application of Keystroke Dynamics

- Keystroke Recognition is used for identification/verification.
- It is used with user ID/password as a form of **multifactor authentication**.
- It is used for surveillance. Some software solutions track keystroke behavior for each user account without end-user's knowledge.
- This tracking is used to analyze if the account was being shared or used by anyone else than the genuine account owner.
- It is used to verify if some software license is being shared.

d) Gait dynamics

A fairly recent active biometric modality is gait recognition. Here, the goal is to find specific characteristics in movement of subjects from video streams. This discipline has been motivated by experimental observations, where

Individuals were able to identify other people known to them only by looking at the projection of silhouettes of their body movements. Besides movement characteristics, the proportions of human limbs appear to be of significance to human in this natural recognition experiment.

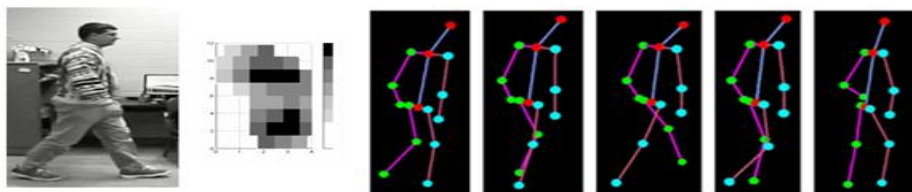


Figure I.10: Gait dynamics.

Merits of Gait Recognition System

- It is non-invasive.
- It does not need the candidate's cooperation as it can be used from a distance.
- It can be used for determining medical disorders by spotting changes in walking pattern of a person in case of Parkinson's disease.

Demerits of Gait Recognition System

- For this biometric technique, no model is developed with complete accuracy till now.
- It may not be as reliable as other established biometric techniques.

Application of Gait Recognition System

- It is well-suited for identifying criminals in the crime scenario.[8]

I.3.3 Biological biometrics

a) DNA

Deoxyribo Nucleic Acid (DNA) is the one- dimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns.

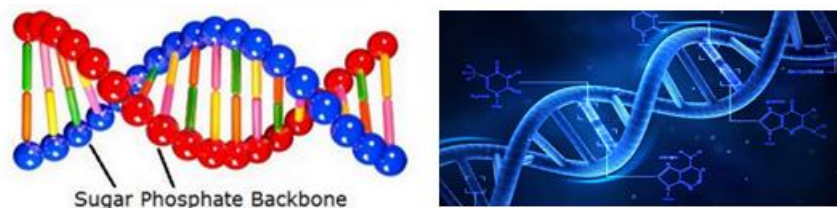


Figure I.11: DNA patterns.

Merit of DNA Recognition System

- It provides the highest accuracy.

Demerits of DNA Recognition System

- Length of procedure from sample acquisition to result is large.
- Being more informative, it brings privacy issues.

- It needs more storage space.
- Sampling contamination or degradation of sample may affect the result.

Applications of DNA Recognition System

- It is mainly used to prove guilt or innocence.
- It is used in physical and network security.

b) Hand veins

It has long been considered that the vein model in human anatomy may be unique to individuals. As a result, there have been various achievements of vein sweeping over the years, from hand sweeping, to wrist sweeping, and more recently to finger sweeping. This technique uses a "scanner of the palmar venous network", to be identified it must place the surface concerned above the reader. The aim here is to analyze the Drawing formed by the network of the veins to keep some characteristic points [9].

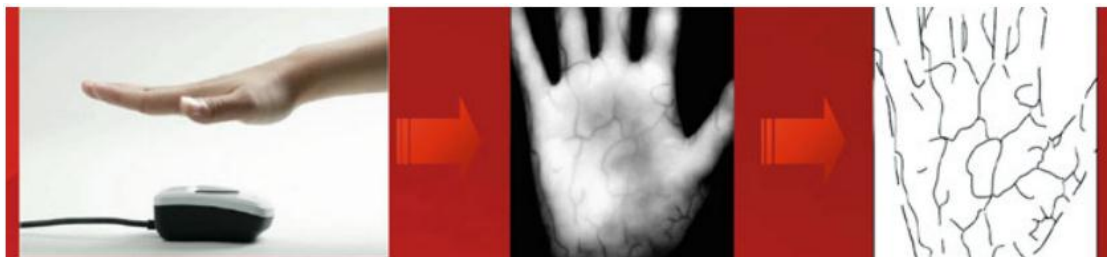


Figure I.12: Hand veins.

I.4 Architecture of a biometric system

The generic architecture of a biometric system consists of five main modules as illustrated in next Figure:

- ❖ *Capture module*: It consists of capturing the biometric raw data in order to extract a numerical representation. This representation is then used for enrollment, verification or identification.
- ❖ *Signal processing module*: It allows the reduction of the extracted numerical representation in order to optimize the quantity of data to store during the enrollment phase, or to facilitate the processing time during the verification and

identification phases. This module can have a quality test to control the captured biometric data.

- ❖ *Storage module*: It is used to store biometric individuals' templates.
- ❖ *Matching module*: It is used to compare the extracted biometric raw data to one or more previously stored biometric templates. The module therefore determines the degree of similarity (or of divergence) between two biometric vectors.
- ❖ *Decision module*: It is used to determine if the returned index of similarity is sufficient to determine the identity of an individual.

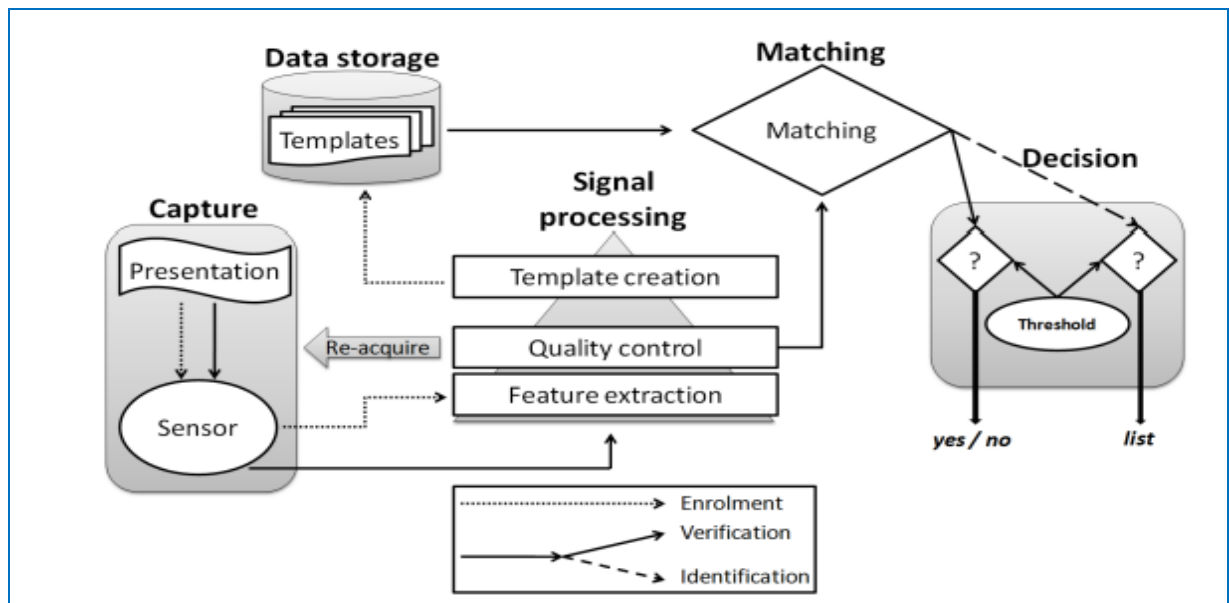


Figure I.13: Generic architecture of a biometric system. [10]

In biometric system there are two modes, which are enrollment mode (apprenticeship) and authentication mode (test). Furthermore; authentication is achieved either in verification mode or identification mode.

- ❖ *Enrolment mode*: It constitutes the initial process of collecting biometric data samples from a person and subsequently creates a reference template representing a user's identity to be used for later comparison. Enrollment is generally performed in a well-controlled environment.
- ❖ *Authentication mode*: Biometric data of user is acquired and used by the system either for verification or identification purposes. The biometric data captured for recognition is a probe sample. In *verification mode*, the probe sample is matched

with the claimed template for validation, and it either accepts or rejects the identity, claim. Verification is one-to-one matching. On the other hand, in *identification mode*, all biometric references in the gallery are examined and the one with the best match-score denotes the class of the input. Identification is one-to-many matching.

In verification mode, if the match score is above some threshold, the identity claim is accepted. Otherwise, it is rejected. There are four outcomes of this setting which are:

- ❖ True accept: The person is genuine and the claim is verified.
- ❖ True reject: The person is impostor and the claim is not verified.
- ❖ False accept: The person is impostor and the claim is verified.
- ❖ False reject: The person is genuine and the claim is not verified [5].

I.5 Comparative representation between some Biometric Technical

There are several biometric technical that are used in various Applications. Each biometric technique has its strengths and weaknesses, so the choice depends on the application. No biometric technique can meet the requirements of all applications. In other words, no biometric technique is optimal. The correspondence between a biometric technique and an application depends on the operational mode of the application and the properties of the biometric characteristic.

The following table shows the comparison between some biometric modalities:

Table 1: *Comparison between some biometric features.*

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	Low
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	Medium	Medium	Medium
Signature	Medium	Medium	High
Face	Low	High	High

I.6 Applications of biometric systems

Biometric applications fall into three main groups:

- ❖ *Commercial applications*, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning.
- ❖ *Government applications* such as national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement.
- ❖ *Forensic applications* such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

Traditionally, commercial applications have used knowledge-based systems employing PINs and passwords, government applications have utilized systems based on tokens such as ID cards and badges, and forensic applications have relied on human experts to match biometric features.

I.7 Performance evaluation of Biometric system

First, in order to understand how to determine the performance of a biometric system, we need to clearly define three main criteria.

- (A) **The first criterion** is called the False Reject Rate (FRR). This rate represents the percentage of people deemed to be recognized but rejected by the system.

$$FRR = \frac{\text{Number of clients rejected (FR)}}{\text{Total number of customers}} \quad (1)$$

- (B) **Second criterion** is the False Accept Rate (FAR). This rate represents the percentage of people who are not recognized but who are still accepted by the system.

$$FAR = \frac{\text{Number of imposters accepted (FA)}}{\text{Total number of impostor accesses}} \quad (2)$$

(C) **Third criterion** is known as Equal Error Rate (EER). This rate is calculated from the first two criteria and is a current performance measurement point. This point corresponds to the place where $FRR = FAR$, that is to say the best compromise between false rejections and false acceptances.

$$EER = \frac{\text{Number of false acceptances} + \text{number of false rejections}}{\text{number of tottel access}} \quad (3)$$

Figure 14 illustrates the FRR and FAR from distributions of genuine and Impostors scores while the EER is shown in Figure 15.

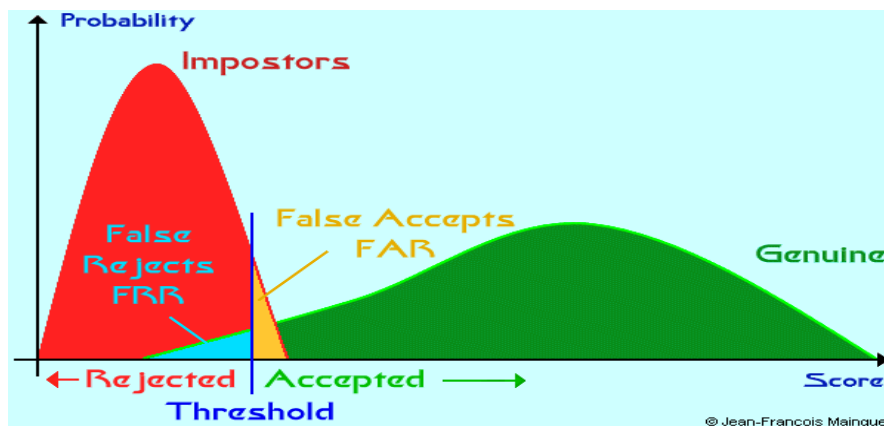


Figure I.14: Illustration of FRR and FAR.

Depending on the nature (authentication or identification) of the biometric system, there are two ways of measuring its performance:

When the system operates in authentication mode, we use what we call a ROC curve (Receiver Operating Characteristic). The ROC curve (Figure 16) traces the rate of false rejection according to the rate of false acceptance. The more this curve tends

to conform to the shape of the mark, the more efficient the system, That is to say having a high overall recognition rate.

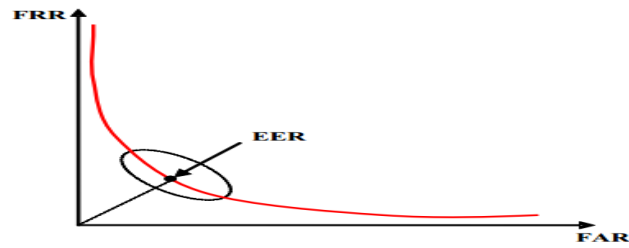


Figure I.15: ROC curve.

(D) Fourth criterion Genuine Acceptance Rate (GAR) is the probability that an authorized person is successfully accepted. It is calculated as a ratio of the number of genuine attempts successfully accepted by the system to the total number of genuine trials. It is equal to 1-FRR.

$$GAR = \frac{\text{Number of genuine attempts accepted}}{\text{Total number of genuine trials}} \quad (4)$$

I.8 Conclusion

In this chapter we had some basic notions related to biometric and its various technologies, the main modules of biometric system and how to measure their performance.

Based on what we reported from biometric modalities also through the comparative study, we decide to study the face recognition because it is more acceptable tm the users, it does not require a time as well as the sensing process has not directly contact with customers like fingerprint or DNA. But this type of recognition has an important weaknesses represented in spoofing by video or photo from unauthorized users.

From this point we will take care of the Methods used in anti-spoofing biometrics in the next chapter.



Chapter II

Face Anti-Spoofing Methods

II.1 Introduction

In recent years, facial biometric systems have received increased deployment in various applications such as surveillance, access control and forensic investigations.

Nowadays one of the limitations of face recognition system is the high possibility of the system being deceived or spoofed by non-real faces, so it need to cope with additional problem: spoofing attacks, like presenting a photo of a person (client) to camera.

We study in this chapter an anti-spoofing solution for distinguishing between 'live' and 'fake' faces.

II.2 Overview on Biometric Anti-Spoofing

Biometric spoofing is a method of fooling a biometric identification management system, where an artificial object is presented to the sensor that imitates the unique face properties of a person which the system is designed to measure, so that the system will not be able to distinguish the fake one from the live, this is the major security issue for face recognition system.

Facial biometrics spoofing techniques involve placing genuine photographs or dummies, playing video recording etc., in front of the camera. A human photograph represents planar objects with only one static facial expression. However, it lacks the three dimensional (3D) information and provides less physiological clues than videos³. These limitations of still photographs are often exploited in liveness detection for facial biometrics. However, the challenges in facial detection increase for spoofing attacks that involve the use of video cameras.

II.2.1 Spoofing Attacks In Face Recognition

The attacks can be classified in two groups depending on whether the artefacts used are: 2D surfaces (e.g., photo, video) which are successful against 2D face recognition systems or 3D volumes (e.g., masks). Such artefacts have been used to carry out three main types of attacks [11] which present an increasing level of spoofing potential:

a) Photo Attacks

These fraudulent access attempts are carried out presenting to the recognition system a photograph of the genuine user. The photograph may have been taken by the attacker using a digital camera, or even retrieved from the internet after the user himself uploaded it to one of the very popular online social networks available today. The image can then be printed on a paper (i.e. print attacks, which were the first to be systematically studied in the literature) or may be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital-photo attacks) .A slightly more advanced type of photo-attack that has also been studied is the use of photographic masks. These masks are high resolution printed photographs where eyes and mouth have been cut out. At the time of the attack the impostor is placed behind so that certain face movements such as eye blinking are reproduced.



Figure II.1: Example photo attack

b) Video Attacks

In this case, the attacker does not use a still image, but replays a video of the genuine client using a digital device (e.g., mobile phone, tablet or laptop). Such attacks appeared as a further step in the evolution of face spoofing and are more difficult to detect, as not only the face 2D texture is copied but also its dynamics.



Figure II.2: Example video attack

c) Mask Attacks

In these cases the spoofing artefacts is a 3D mask of the genuine client's face, increasing the difficulty to find accurate countermeasures against them. Since the complete 3D structure of the face is imitated, the use of depth cues which could be a solution to prevent the previous two types of attacks (carried out with flat surfaces), becomes inefficient against this particular threat. [11]



Figure II.3: Example mask attack.

II.2.2 State Of The Art Face Anti-Spoofing:

It cannot be argued that since biometrics can now affect whole populations, anti-spoofing needs determined study. Biometrics experts both in academia and industry have been working on methods to deal with the spoofing threat. Referred as anti-spoofing, spoof detection or presentation attack detection, this task consists of differentiating between a real biometric reading from a live person and a fake one forged by the attacker.

II.2.3 Face Anti Spoofing Techniques

In order to guard against such spoofing, a secure system needs anti-spoofing techniques. In our work we interest to feature level-technique. These techniques are showing in the following figure:

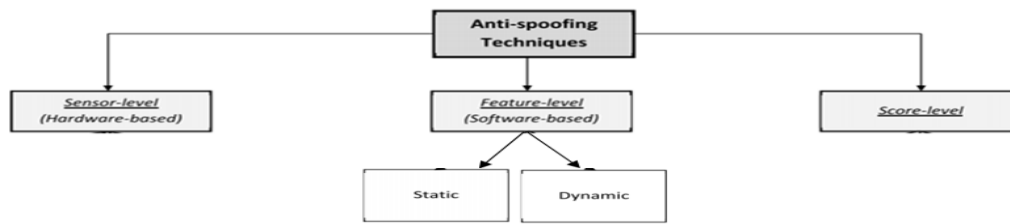


Figure II.4: General classification of anti-spoofing methods.

In the following figure there are more illustrations of different anti spoofing techniques:

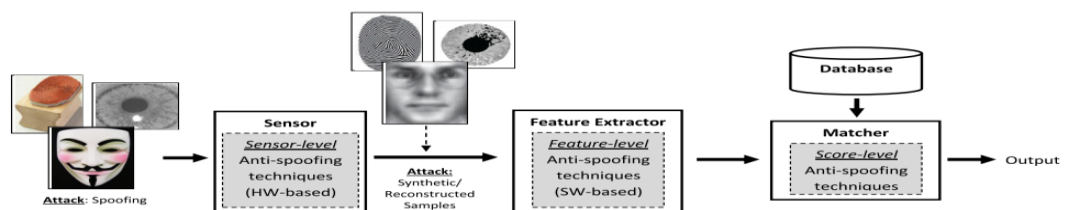


Figure II.5: General diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated. Also displayed are the two different types of attacks for which anti-spoofing. [12]

a) Sensor-level techniques

Usually referred to in the literature by the term hardware-based techniques. These methods add some specific device to the sensor in order to detect particular properties of a living trait. In general, hardware-based approaches measure one of three characteristics, namely: (i) intrinsic properties of a living body, including physical properties (e.g., density or elasticity), electrical properties (e.g., capacitance, resistance or permittivity), spectral properties (e.g., reflectance and absorbance at given wavelengths) or even visual properties (e.g., colour and opacity); (ii) involuntary signals of a living body which can be attributed to the nervous system. Good examples are the pulse, blood pressure, perspiration, pupillary unrest (hippus), brain wave signals (EEG) or electric heart signals; (iii) responses to external stimuli, also known as challenge-response methods, which require the user cooperation as they are based on detecting voluntary or involuntary (reflex reactions) responses to an external signal. Examples of such methods can be the pupil contraction after a lighting

event (reflex), or the head movement following a random path determined by the system.

b) Feature-level techniques:

Usually referred to in the literature by the term software-based techniques. In this case the fake trait is detected once the sample has been acquired with a standard sensor. As such, features used to distinguish between real and fake traits are extracted from the biometric sample, and not directly from the human body as in the case of sensor-level techniques. These methods are integrated after the sensor, usually functioning as part of the feature extractor module. They can be further classified into static and dynamic anti-spoofing methods, depending on whether they work with only one instance of the biometric trait, or with a sequence of samples captured over time.

[13] – [15]

Although they may present some degradation in performance, in general, static features are preferable over dynamic techniques as they usually require less cooperation from the user, which makes them faster and less intrusive. Such a subdivision into static and dynamic approaches is of special interest in face recognition, where there exist systems working on single facial images (e.g., passport picture) and on video sequences (e.g., surveillance camera).

There are three liveness indicators for extraction the features:

- ❖ Motion analysis: the analysis is based on the fact that there is significant difference between motions of planar objects and real human faces (3D). Algorithms of spoofing detection based on motion analysis are usually associated with optical flow. The assumption is that different patterns of optical flow fields reveal the difference between movements of 3D face (real face) and 2D face (spoofing face).
- ❖ Texture analysis: it is assumed that printed/LED faces contain outstanding texture patterns that do not exist in real faces. The other common observation is that images/videos with spoofing faces (printed or replayed) are usually noisier than those of real faces. In this case, noise variance may be used as a distinction feature for the detection.

- ❖ **Liveness detection:** Life signs may include eye blinking, lips movements, etc. This requires analysis of local movement against global movement. Developed algorithms under this approach focus on the movement of a certain identified part of a face.

Among the three categories, texture analysis dominates approaches to distinction of live and spoofing faces. In the recent competition on counter measures to 2D face spoofing attacks, eight teams took part in the competition, and seven of them made use of image textures in their algorithms. These texture features include local binary code (LBP), gray-level co-occurrence matrix (GLCM), and Gabor features. LBP has shown its effectiveness as image features in face spoofing detection. Statistical features, such as first and second moments are also used as descriptors in the feature space. For motion analysis, optical flows are popularly adapted in algorithm development; and live signs are connected to both eye blinking and lip moving. With regards to classifiers, a variety of Support Vector Machines (SVMs) have seen their applications in face spoofing detection.

Finally texture analysis has advantages of simple implementation, possible decision from a single frame, and no user collaboration needed. However it requires data covering all possible attacks, and may fail with low textural attacks. Algorithms based on motion and life sign detection are independent to textures and very hard to spoof by 2D images, but it needs a video sequence, and may also need user-cooperation. The new developing trend of 2D face anti-spoofing algorithms is fusion of different categories of cues, either in the feature level (a single classifier) or in the score level (multiple classifiers). Such an approach is effective in tackling a diverse set of face spoofing attacks.

c) Score-Level Techniques

Recently, a third group of protection methods which fall out of the traditional two-type classification (software- and hardware-based). These protection techniques, much less common than the previous two categories, are focused on the study of biometric systems at score-level in order to propose fusion strategies that increase their resistance against spoofing attempts. Due to their limited performance, they are designed as supplementary measures to the sensor-level and feature-level techniques

presented above, and are usually integrated in the matcher. The scores to be combined may come from: i) two or more unimodal biometric modules; ii) unimodal biometric modules and anti-spoofing techniques; or iii) only results from anti-spoofing modules.

[13]

II.3 Face anti-spoofing methods

Various approaches have been developed to detect photograph spoofing. The existing techniques mainly concentrate on texture analysis. There are also several countermeasure techniques based on liveness detection and motion analysis, in case analyses are not restricted to a single image. [16]

II.3.1 Face anti-spoofing preprocessing

We must pre-process face images to improve the face recognition rate, then we extract the features. The next steps explain how we use preprocessing step by step which are: face detection, eyes localization and face normalization.

a) Face detection

In this part, we will address to face detection, we will use the Viola-Jones algorithm to detect the region of interest (face).

❖ Why Viola-Jones algorithm?

We use Viola-Jones in our approach to detect the face. The question here is why we didn't use other algorithms, because viola getting really good in face detection with any pictures has faces.

The Viola - Jones algorithm is a method for detecting an object in a digital image, proposed by Paul Viola and Michael Jones in 2001. Originally invented to detect faces, it may also be used to detect other types of objects such as cars or aircraft. [17]

The characteristics of Viola-Jones algorithm which make it a good detection algorithm are:

- ❖ Robust – very high detection rate (true-positive rate) and very low false-positive rate always.
- ❖ Real time – For practical applications at least 2 frames per second must be processed.
- ❖ Face detection only (not recognition) - The goal is to distinguish faces from non faces (detection is the first step in the recognition process).

❖ Steps

The algorithm has four stages:

- ❖ Haar Feature Selection.
- ❖ Creating an Integral Image.
- ❖ Adaboost Training.
- ❖ Cascading Classifiers.

❖ Advantages of Viola–Jones algorithm

- ✓ Efficient feature selection.
- ✓ Scale and location invariant detector.
- ✓ Instead of scaling the image itself (e.g. pyramid-filters), we scale the features.

Such a generic detection scheme can be trained for detection of other types of objects (e.g. cars, hands). [18]

An example of face detection is showing in the figure below:

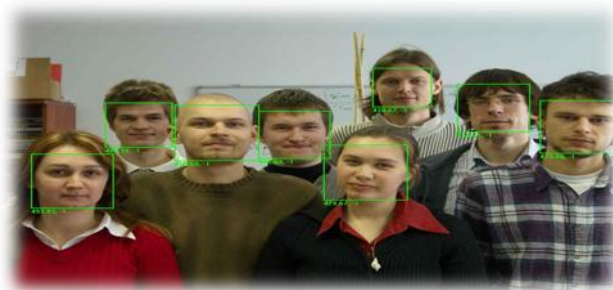


Figure II.6: Example Face detection.

b) Eyes localization

We present a method of eye localization which can be used in face anti spoofing application. It is based on the Pictorial Structure (PS) algorithm, to make this algorithm work it has to be resize the face after we detect it into (64,64) this is the reason why we use viola jones algorithm.



Figure II.7: Example Eyes localization.

c) Face normalization

After face detection and eye localization we must normalize the face. In face normalization we rotate and crop the face depending on coordinate of eyes.

The previous paragraph is summarized by the next algorithm:

Steps

Step 1: Check image is human face or not.

Step 2: Find the face boundary.

Step 3: Find the eye region

Step 4: Find the horizontal nose position

Step 5: Find the position of iris

Step 6: Find the vertical mouth position

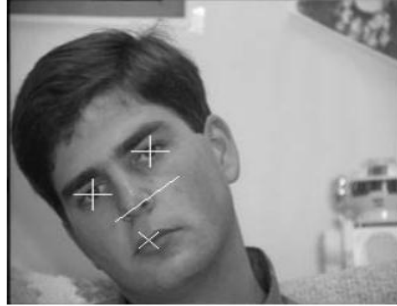


Figure II.8: Example Face normalization.

d) Face representation

Face representation is a technique divide ROI (Region of Interest) face in blocks; the ROI is the process of highlighting key and interesting features as a smaller region before moving into the feature extraction stage.[19] After that we apply our descriptors in each block which is divided.

To expand the experiments, we adopt two face representation techniques Multi-Block (MB) and Multi-Level (ML). In below we explain those techniques:

a) Multi-Blocks

Multi Blocks is technique divided the ROI into $(n \times n)$ sub-blocks which have the same size. In each block we apply one of our descriptors to give us as much as possible features of the ROI.

The figure below illustrates Multi-block technique:

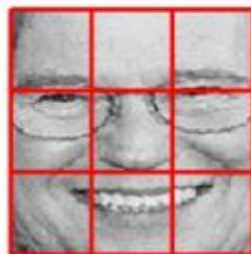


Figure II.9: Example Multi-Blocks.

b) Multi-Levels

ML face representation is a spatial pyramid representation which constructed by sorted series of MB representations. In other term, take the whole face ROI than divided the ROI to sub-blocks, like this equation $1^2 + 2^2 + 2^3 + \dots + 2^n$ and until we reach the intended n level. The figure below illustrates Multi-level technique:

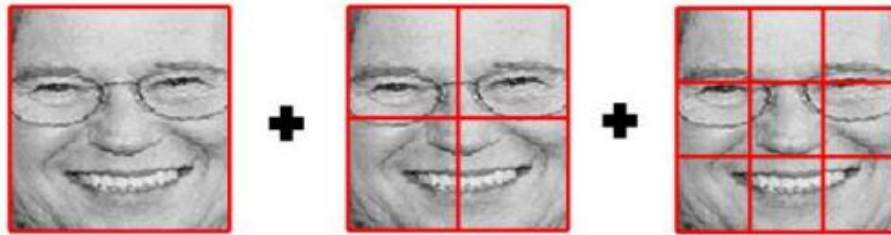


Figure II.10 : Example Multi-level.

II.3.2 Feature Extraction

Feature extraction is a very important stage in the identification process of biometric systems. It involves the simplification of the amount of resources which describes a large set of data. Feature extraction is mainly used to minimize the original dataset by getting some properties that can be used to classify and get patterns that are present in the input images. [16]

a) Local Binary Pattern (LBP)

The LBP is an image operator which transforms an image into an array or image with more detail. The basic LBP, introduced by Ojala et al. [20] was based on the assumption that texture has locally two complementary aspects, a pattern and its strength.

The original LBP works in a 3x3 pixel block of image. The pixels in this block are thresholded by its center pixel value, multiplied by powers of two and then summed to obtain a label for the center pixel. As the neighborhood consists of 8 pixels, a total of $2^8=256$ different labels can be obtained depending on the relative gray values of the center and its neighborhood. [21]

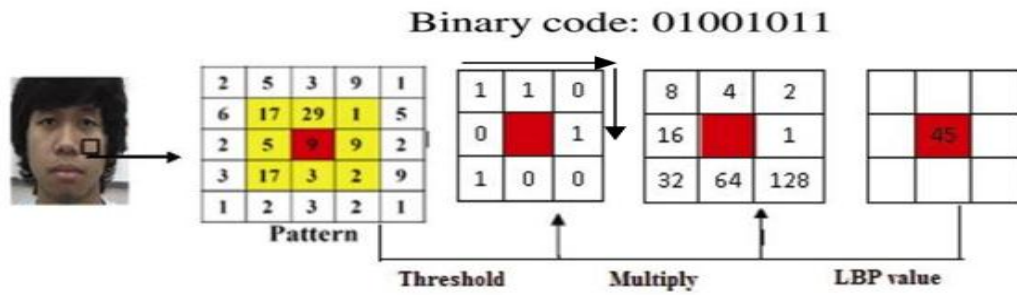


Figure II.11 : The basic LBP operator.

There is another extension of original LBP called Local Binary Pattern uniform which defined by equation in below:

$$LBP_{P,R}^{u_2} = \sum_{p=0}^{P-1} S(g_p - g_c) 2^p \quad (5)$$

Where the notation (P, R) is generally used for pixel neighborhoods to refer to sampling points (P) and circle of radius(R), U_2 refers to the LBP uniform. Moreover g_c corresponds to the gray value of the center pixel (x_c, y_c), g_p refers to gray values of P equally spaced pixels on a circle of radius R , and S defines a thresholding function as follows:

$$S(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

The LBP uniform called with this name uniform if only has at least two transitions from 0 to 1 or vice versa. We give example for explain the uniform pattern, like 00000000 or 11111111 have zero transition, although 00111000 two transition and 00001111 one transition which all those examples are uniform. In another hand when is more than three transition patterns are non-uniform like 00110011 have three transition, 01010101 seven transition, 00110101 five transition and 10101111 four transition.

b) Local Phase Quantization (LPQ)

Spatial blurring is represented by a convolution between the image intensity and a point spread function (PSF). In the frequency domain, this results in a

multiplication $\mathbf{G} = \mathbf{F} \cdot \mathbf{H}$, where \mathbf{G} , \mathbf{F} and \mathbf{H} are the discrete Fourier transforms (DFT) of the blurred image, original image, and the PSF respectively. Further considering only the phase of the spectrum the relation turns into a sum $\angle \mathbf{G} = \angle \mathbf{F} + \angle \mathbf{H}$. When the PSF of the blur is centrally symmetric its Fourier transform H is always real valued i.e. $\angle \mathbf{H} \in \{0, \pi\}$. Furthermore, the shape of H for a regular PSF is close to a Gaussian or a **sinc** function ensuring that at least the low frequency values of H are positive. At these frequencies, $\angle \mathbf{H} = 0$ causing $\angle \mathbf{F}$ to be a blur invariant property. Because LPQ uses finite size 2-D discrete STFT computed locally, this invariance is in part disturbed but is still pertinent.[22]

In LPQ, the phase is examined in local neighborhoods N_x at each pixel position $\mathbf{x} = [x_1, x_2]^T$ of the image $f(\mathbf{x})$.

These local spectra are computed using a discrete STFT defined by

$$\mathbf{F}(\mathbf{u}, \mathbf{x}) = \sum_{\mathbf{y}} f(\mathbf{y}) w_R(\mathbf{y} - \mathbf{x}) e^{-j2\pi \mathbf{u}^T \mathbf{y}} \quad (6)$$

Where \mathbf{u} is the frequency and $w(\mathbf{x})$ is a window function defining the neighborhood N_x . In the case of regular LPQ, w_R is a N_R -by- N_R rectangle given as $w_R(\mathbf{x}) = 1$ if $|x_1|, |x_2| < N_R/2$ and 0 otherwise.

The local Fourier coefficients are computed at four frequency points $\mathbf{u}_1 = [a, 0]^T$, $\mathbf{u}_2 = [0, a]^T$, $\mathbf{u}_3 = [a, a]^T$ and $\mathbf{u}_4 = [a, -a]^T$, where a is a sufficiently small scalar to satisfy $H(\mathbf{u}_i) > 0$. For each pixel position this results in a vector

$$\mathbf{F}(\mathbf{x}) = [\mathbf{F}(\mathbf{u}_1, \mathbf{x}), \mathbf{F}(\mathbf{u}_2, \mathbf{x}), \mathbf{F}(\mathbf{u}_3, \mathbf{x}), \mathbf{F}(\mathbf{u}_4, \mathbf{x})]$$

The phase information in the Fourier coefficients is recorded by observing the signs of the real and imaginary parts of each component in $\mathbf{F}(\mathbf{x})$. This is done by using a simple scalar quantization.

$$q_j = \begin{cases} 1 & \text{if } \mathbf{q}_j \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

Where g_j is the j -th component of the vector $G(x) = [\text{Re}\{F(x)\}, \text{Im}\{F(x)\}]$.
 The resulting eight binary coefficients q_j are represented as integer values between 0-255 using coding:

$$F_{\text{LPQ}(x)} = \sum_{j=1}^8 q_j 2^{j-1} \quad (8)$$

Finally, a histogram of these values from all positions is composed, and used as a 256-dimensional feature vector in classification.

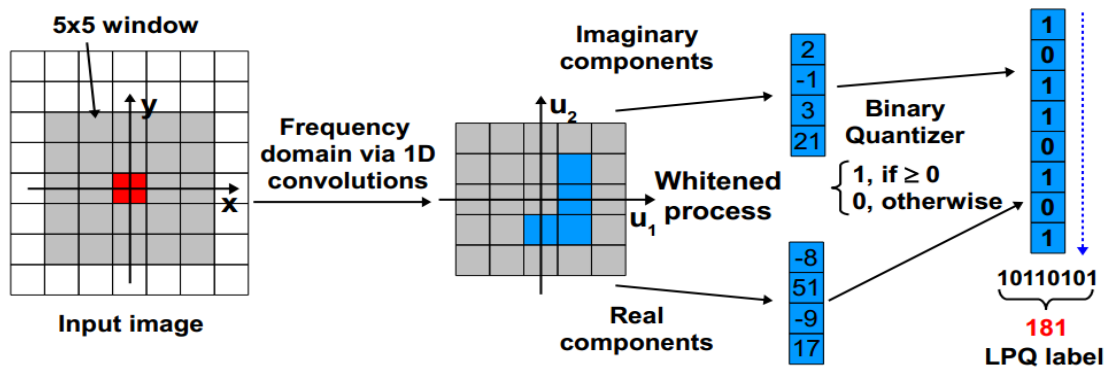


Figure II.12: Construction of LPQ descriptor.

c) Binarized Statistical Image Features (BSIF)

This method used for constructing local image descriptors which efficiently encode texture information and are suitable for histogram based representation of image regions. BSIF method computes a binary code string for the pixels of a given image.

The code value of a pixel is considered as a local descriptor of the image intensity pattern in the pixel's surroundings. This descriptor can be used in texture recognition tasks in a similar manner as local binary patterns [23].

Given an image patch X of size 1×1 pixels and a linear filter W_i of the same size, the filter response S_i is obtained by:

$$S_i = \sum_{u,v} W_i(u,v)X(u,v) = W_i^T X \quad (9)$$

Where vector notation is introduced in the latter stage, i.e., vectors w and x contain the pixels of W_i and X .

The binarized feature b_i is obtained by setting $b_i = 1$ if $S_i > 0$ and $b_i = 0$ otherwise. Given n linear filters W_i , we may stack them to a matrix W of size $n \times l^2$ and compute all responses at once:

$$\mathbf{s} = \mathbf{W}\mathbf{x}$$

The binary code string b , which corresponds to image patch x , is obtained by binarizing each element S_i of S as follows:

$$b_i = \begin{cases} 1 & \text{if } s \geq 0 \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

Whereas b_i is the i^{th} element of b .

II.3.3 Classification

Classification refers to assigning an object physically into one of a set of predefined categories. The main idea behind the use of a classification algorithm is to divide the database into groups where each group has homogenous characteristics. The important step is to design a classifier based on texture (case of our work) or some soft biometric attribute. [24]

Support vector machines (SVM) have become a widely studied and applied classification technique, especially used in face recognition. A Support Vector Machine (SVM) is a supervised machine learning algorithm that can be employed for both classification and regression purposes. SVMs are more commonly used in classification problems and as such, this is what we will focus on in this section.

SVMs are based on the concept of decision planes that define decision boundaries. A decision plane is one that separates between a set of objects having different class memberships. The figure below is a classic example of a linear classifier, i.e., a classifier that separates a set of objects into their respective groups (GREEN and RED in this case) with a center line.

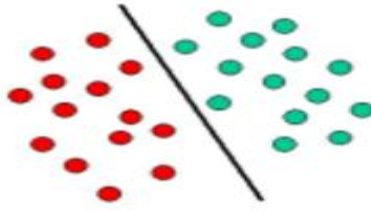


Figure II.13: example of a linear classifier.

Most classification tasks, however, are not that simple, and often more complex structures are needed in order to make an optimal separation, i.e., correctly classify new objects (test cases) on the basis of the examples that are available (train cases). This situation is depicted in the illustration below. Compared to the previous schematic, it is clear that a full separation of the GREEN and RED objects would require a curve (which is more complex than a line). Classification tasks based on drawing separating lines to distinguish between objects of different class memberships are known as hyperplane classifiers. Support Vector Machines are particularly suited to handle such tasks.

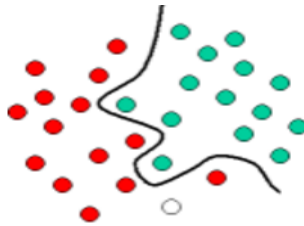


Figure II.14: Example of hyperplane.

The illustration below shows the basic idea behind Support Vector Machines. Here we see the original objects (left side of the schematic) mapped, i.e., rearranged, using a set of mathematical functions, known as kernels. The process of rearranging the objects is known as mapping (transformation). Note that in this new setting, the mapped objects (right side of the schematic) is linearly separable and, thus, instead of constructing the complex curve (left schematic), all we have to do is to find an optimal line that can separate the GREEN and the RED Objects.[25]

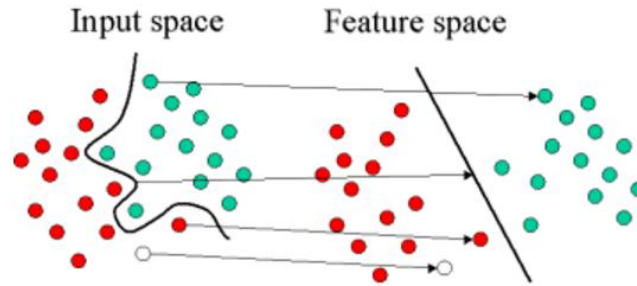


Figure II.15: Example of SVM Classifier.

a) The advantages of Support Vector Machine are

- Prediction accuracy is generally high.
- Robust works when training examples contain errors.
- Fast evaluation of the learned target function.

b) The disadvantages of support vector machine includes

- Long training time.
- Difficult to understand the learned function (weights).
- Not easy to incorporate domain knowledge.

II.4.Conclusion

We proposed in this work, an approach for anti-spoofing detection based on LBP and support vector machine that discriminate live faces from fake ones.

There are different anti-spoofing methods that have been developed to raise the difficulty level for photo, video and synthesis attacks. Even though the outcome of research efforts on anti-spoofing appears to be making a significant progress, but the quest continues towards a more reliable and secure system. Although a great amount of work has been done in the field of spoofing detection, attacking methodologies are also becoming more and more sophisticated. As a consequence, there are still big challenges to be faced in the protection against direct attacks that will hopefully lead in the coming years to a new generation of more secure biometric systems. For blinking and movement of eyes based Finally, after all we have seen, we hope to

apply these selected methods of anti-spoofing in the next chapter and analysis the results we will get liveness.



Chapter III

Experemantal results and discussion

Experimental Results

and Discussion

III.1 Database and protocol

In our work, we used the publicly available NUAA Photograph Imposter Database. The NUAA database comprises images extracted from videos of 15 subjects captured in three sections and contains attempts of attack based on hand-held printed photos. This dataset is divided into training and test sets. The former has 1743 live images and 1748 non-live, and the latter consists of 3362 live and 5761 non-live samples. [26]

Table 2: Number of images in the training set and test set

NUAA dataset		Session1	Session2	Session3	Total
Training Set	Client	889	854		1743
	Imposter	855	893		1748
Test Set	Client	0	0	3362	3362
	Imposter	0	0	5761	3362
Total		1744	1747	9123	12614

During the development of this application, we used Matlab 2016b.

We applied our approach using face detection without Stasm using the same image normalization in NUAA data bases in one hand. In other hand, we calculated the results using the Viola Jones algorithm and Active Shape Model with Stasm.

III.2 Proposed approach

- Our face anti spoofing approach consists in three steps which are: face detection, features extraction, classification or decision.
- First in the face detection step, we used Viola-Jones algorithm to locate all components of the face images and Stasm (software package) for locating landmarks using Active Shape Models (ASMs) to localizing the eyes. The coordinates of the eyes are used to rotate and to crop the face, after that we normalize all faces using the center of the eyes points.
- In this way, we use an approach to extract features from different Multi-Block and Multi-Level divisions [27-29] which are inspired by Local Binary Pattern **LBP**, Local Phase Quantization **LPQ** and Binarized Statistical Image Features **BSIF** methodologies [30- 32]. These methods describe each pixel's neighborhood by a binary code which is obtained by first convolving the image with a set of linear filters and then binarizing the filter responses. After that we reduce the Histograms by fisher score.
- Finally, we use our classifier Support Vector Machine (**SVM**), to be able differentiate between the fake face and the real one.

The figure below illustrates the used proposed approach.

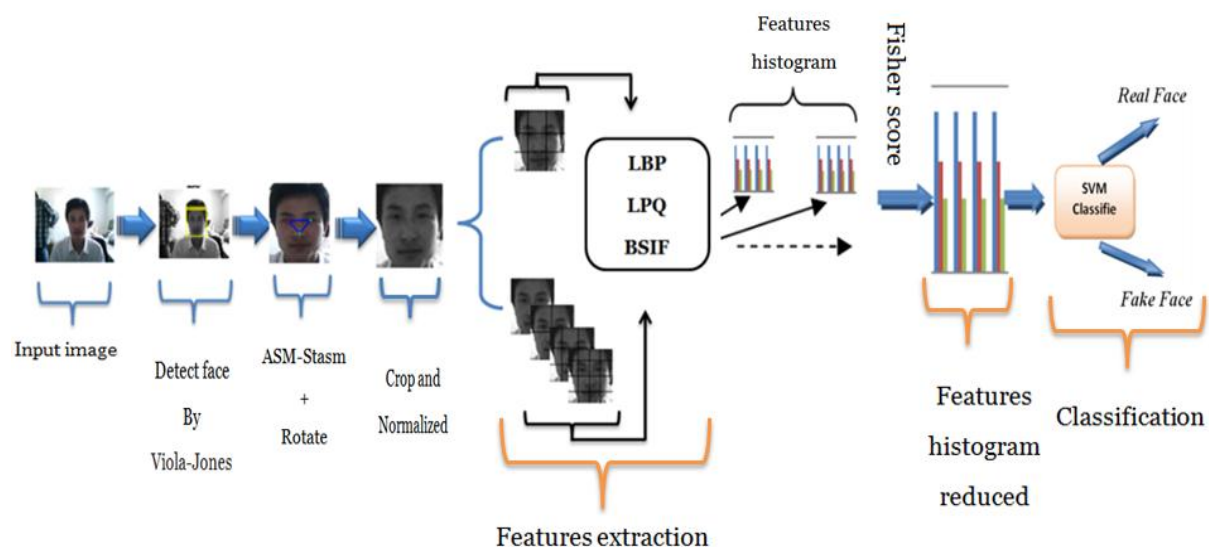


Figure III. 1: The proposed approach.

III.3 The experimental Results

In this section, we give results of our approach compared with the state of the art. The performance evaluations of the studied anti-spoofing algorithm are measured in terms of the Equal Error Rate (EER).

III.3.1 Results obtained in the absence of the stasm

In this part we applied our approach using face detection without Stasm i.e. using the crop image in NUAA database. Here a table of obtained results (EER %):

Table 3: Obtained EER result without Stasm.

<i>Methods</i>	EER %
LBP	15.93
MB-LBP	4.25
ML-LBP	2.84
LPQ	17.08
MB-LPQ	10.11
ML-LPQ	11.89

Here we observe that the ML-LBP gives an EER value better compared with LPQ methods.

In this part we apply each descriptor separately.

a) Extraction features for one block:

By LBP, LPQ and BSIF we extract the features with one block which means taking the whole image. The results obtained as showing in below:

- **LBP descriptor:**

Table 4: The different LBP results.

Parameters	EER %	Acc %
8_1	11.4737	74.0217
8_2	13.1574	77.5622
16_2	21.9215	74.7671

Through this table we note that the first parameter $LBP_{8,1}^{u2}$ with, $P = 8$ and $R = 1$ (8 surrounding pixels) give us a good value of EER compared with the other parameters. Because whenever the window is smaller the EER value becomes less.

Due to the large number of LPQ, BSIF parameters, we consider who have the best result among them.

- **LPQ descriptor:**

Table 5: The different LPQ results.

Parameters	EER %	Acc %
LPQ_block_1_3_0_2	26.0559	75.1836
LPQ_block_1_3_1_2	6.5735	90.8035
LPQ_block_1_5_1_2	47.5091	71.9391
LPQ_block_1_7_1_1	53.7754	67.0942
LPQ_block_1_7_1_2	51.1898	71.8842
LPQ_block_1_9_1_2	49.2267	69.6372
LPQ_block_1_13_1_3	43.5158	72.8488
LPQ_block_1_15_1_2	35.4253	70.7552
LPQ_block_1_15_1_3	38.1184	74.1532
LPQ_block_1_17_1_2	30.7555	72.52

We note from these results that the fifth parameter compared to LPQ **block_1_3_1_2** with 3x3 (default size) uniform window and using STFT (Short-Term Fourier Transform) with estimation frequency = 1 give us a good EER value compared with the other parameters.

- **BSIF descriptor:**

Table 6: The different BSIF results.

Parameters	EER %	Acc %
BSIF_block_1_5_5_5	5.6514	82.4838
BSIF_block_1_5_5_6	12.4284	86.2436
BSIF_block_1_5_5_9	39.0244	72.5638
BSIF_block_1_9_9_5	23.7061	72.6187
BSIF_block_1_9_9_8	40.2736	74.3834
BSIF_block_1_11_11_5	38.4135	59.4322
BSIF_block_1_11_11_8	37.4067	70.4374
BSIF_block_1_15_15_8	36.8233	66.3488
BSIF_block_1_15_15_9	6.3772	64.7375
BSIF_block_1_17_17_9	33.1053	71.6869

We note from the previous table that the first BSIF parameter which is **block_1_5_5_5** gives us a good EER value compared with the other parameters.

All the previous local descriptors have gained attention due to their robustness to challenges such as pose and illumination changes in images. Among these descriptors, BSIF has shown to perform better than others.

b) Extraction features for Multi- block and multi-level

To better perform extraction features task, we must increase the characteristics vector. When dividing the face image into blocks and levels, we consider the better operators (**LBP8_1**, **LPQ_block_1_3_1_2** and **BSIF_block_1_5_5_5**) on each region (ROI).

So we integrate the notion of multi-block and multi-level, results showing in below:

MB-LBP_{8,1}:

Table 7: The different MB-LBP results.

Parameters\ Performance criteria	EER %	Acc %
LBP_block_1_1_8_1	11.4737	74.0217
LBP_block_2_1_8_1	2.8467	96.2622
LBP_block_3_1_8_1	5.8299	93.0067
LBP_block_4_1_8_1	2.9149	97.0953
LBP_block_5_1_8_1	51.1898	96.7555
LBP_block_6_1_8_1	3.7775	95.9334
LBP_block_7_1_8_1	5.2647	94.2015
LBP_block_8_1_8_1	4.6401	92.338

When dividing with the best LBP parameter into 8 block. EER value becomes 2.84 %.

- **ML-LBP_{8,1}**

Table 8: The different ML-LBP results.

Parameters\ Performance criteria	EER %	Acc %
LBP_level_1_1_8_1	11.4737	74.0217%
LBP_level_2_1_8_1	3.2633	94.1576%
LBP_level_3_1_8_1	4.0444	95.5936%
LBP_level_4_1_8_1	2.6384	97.3912%
LBP_level_5_1_8_1	2.4301	97.6543%
LBP_level_6_1_8_1	2.7947	96.9966
LBP_level_7_1_8_1	3.7775	95.9443
LBP_level_8_1_8_1	3.8535	95.2866

When we did the same procedure but with ML-LBP dividing, we got a smaller EER (%) value (2.43%). then MB.

- **MB-LPQ:**

For this proposed method we used the local phase quantization (LPQ) as descriptor of features extraction. Depending on LPQ, we compared Multi-level Local Phase Quantization (ML-LPQ) and Multi-Blocks Local Phase Quantization (MB-LPQ).

Table 9: The different MB-LPQ results.

Parameters	EER %	Acc %
LPQ_block_1_3_1_2	5.4729	90.4637
LPQ_block_2_3_1_2	9.9809	86.4957
LPQ_block_3_3_1_2	2.5877	97.3693
LPQ_block_4_3_1_2	4.2527	92.0859
LPQ_block_5_3_1_2	2.8814	96.2512
LPQ_block_6_3_1_2	6.4545	90.2664
LPQ_block_7_3_1_2	3.837	96.0868
LPQ_block_8_3_1_2	3.8667	96.1307

- **ML-LPQ:**

Table 10: The different ML-LPQ results.

Parameters\ Performance criteria	EER %	Acc %
LPQ_level_1_3_1_2	5.47	90.4637
LPQ_level_2_3_1_2	11.12	86.2545
LPQ_level_3_3_1_2,	4.40	94.048
LPQ_level_4_3_1_2	3.74	92.7655
LPQ_level_5_3_1_2	2.18	95.6045
LPQ_level_6_3_1_2	2.95	94.2015
LPQ_level_7_3_1_2	2.67	95.9772
LPQ_level_8_3_1_2	2.41	96.7226

The table 9 and 10 showing that the increasing of features vector sorted by LPQ descriptor resulting decrease of EER. In ML-LPQ (2.18 %) better then MB.

- **MB-BSIF:**

Table 11: The different MB-BSIF results.

Parameters\ Performance criteria	EER %	Acc %
BSIF_block_1_5_5_5	5.6514	82.4838
BSIF_block_2_5_5_5	9.0125	91.6694
BSIF_block_3_5_5_5	3.8965	96.9747
BSIF_block_4_5_5_5	3.3314	96.613
BSIF_block_5_5_5_5	3.1939	97.1829
BSIF_block_6_5_5_5	3.599	96.8103
BSIF_block_7_5_5_5	2.6472	97.731
BSIF_block_8_5_5_5	2.7067	97.457

- **ML-BSIF**

Table 12: The different ML-BSIF results.

Parameters	EER %	Acc %
BSIF_level_1_5_5_5	5.6514	82.4838
BSIF_level_2_5_5_5	9.2504	91.5159
BSIF_level_3_5_5_5	4.7591	96.1855
BSIF_level_4_5_5_5	3.6288	96.9308
BSIF_level_5_5_5_5	2.7365	97.7639
BSIF_level_6_5_5_5	2.9744	97.731
BSIF_level_7_5_5_5	2.6175	97.7529
BSIF_level_8_5_5_5	2.6211	97.6543

The table 11 and 12 showing that the increasing of features vector sorted by BSIF descriptor resulting decrease of EER. In ML-BSIF (2.64 %) better then MB.

III.3.2 Comparative study shows the role of Stasm :

In this part we explore the most important property of stasm and its effectiveness in improving the recognition rate:

Table 13: Performance comparison between our proposed approach and the best results without stasm in the same database.

<i>Methods</i>	EER %
LBP	15.93
LBP (with stasm)	11.4737
MB-LBP	4.25
MB-LBP (with stasm)	2.8467
ML-LBP	4.07
ML-LBP (with stasm)	2.4301
LPQ	17.08
LPQ (with stasm)	6.5735
MB-LPQ	10.11
MB-LPQ (with stasm)	2.5877
ML-LPQ	11.89
ML-LPQ (with stasm)	2.1871

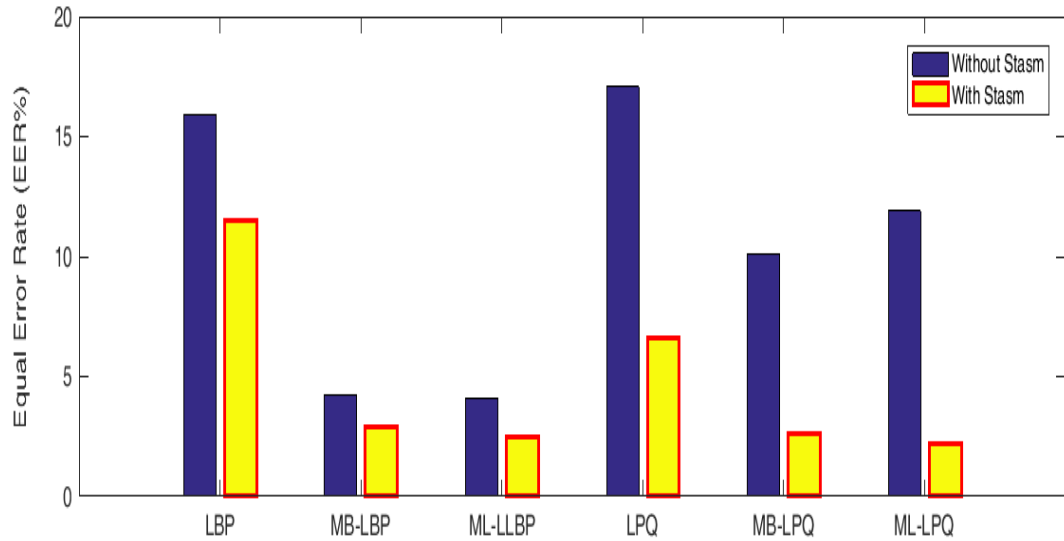


Figure III. 2: Illustration the role of Stasm.

Table 14: Comparison between the proposed countermeasures with stasm.

Methods	EER %
LBP	11.4737
MB-LBP	2.8467
ML-LBP	2.4301
LPQ	6.5735
MB-LPQ	2.5877
ML-LPQ	2.1871
BSIF	5.6514
MB-BSIF	2.6472
ML-BSIF	2.6175

The table above provides a comparison with the descriptors of face spoofing detection techniques proposed in the literature, which show that ML always gives better results than MB when using the same descriptors. However, the descriptor LPQ also gives good results close to LBP and BSIF.

The figure below describes all of them:

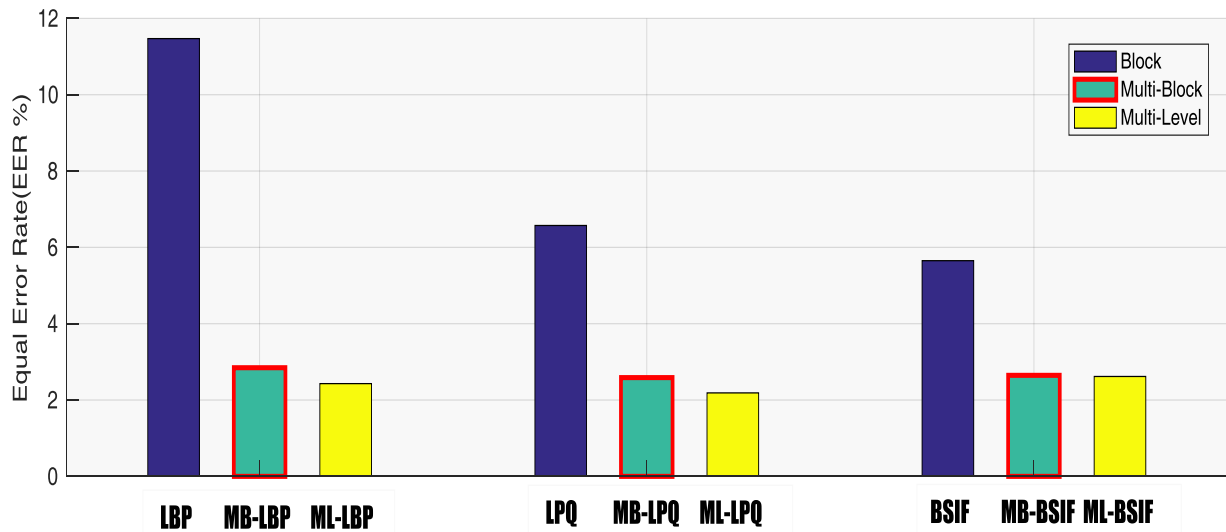


Figure III.3: Comparison between the descriptors.

For the purpose of improvement the EER and after what we see that the ML, MB increasing the characteristic vectors. However the EER value, execution time, memory space still not slightly improved. *Fisher score* one of the most algorithms who will improve it while preserving the most discriminant images features.

III.3.3 Comparative analysis between MB and ML with and without fisher score :

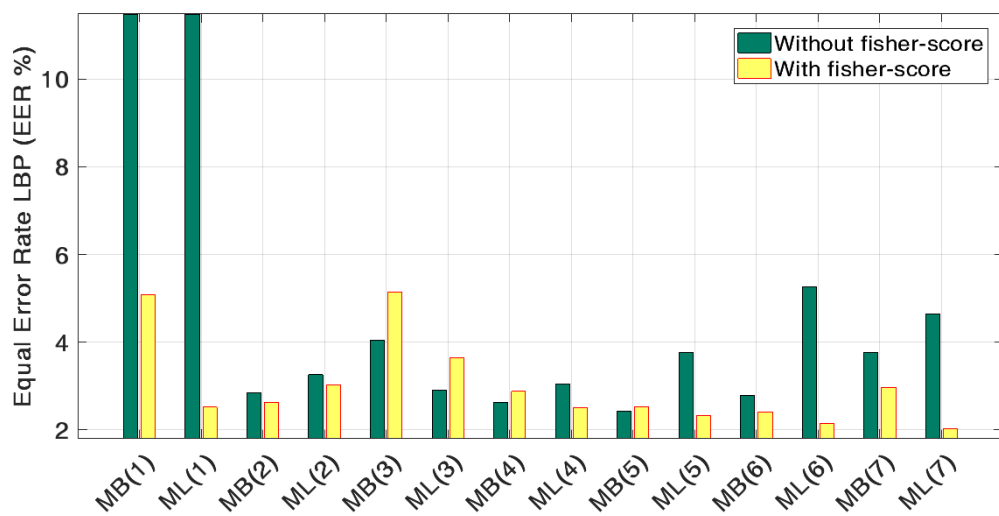


Figure III.4: Comparison of the results (in EER %) between ML-LBP and MB-LBP approach without (Fisher) and with (Fisher).

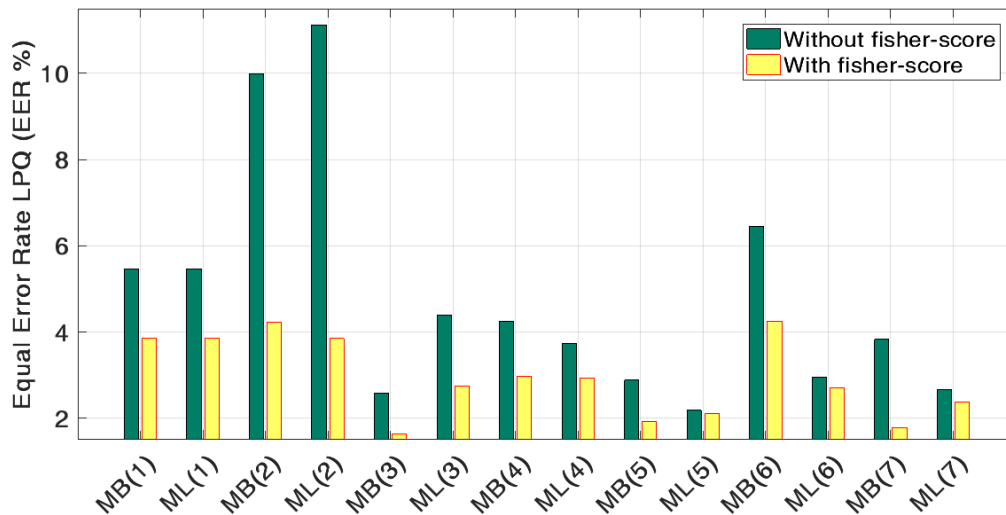


Figure III.5: Comparison of the results (in EER %) between ML-LPQ and MB-LPQ approach without (Fisher) and with (Fisher).

MB(3) of LPQ give good result.

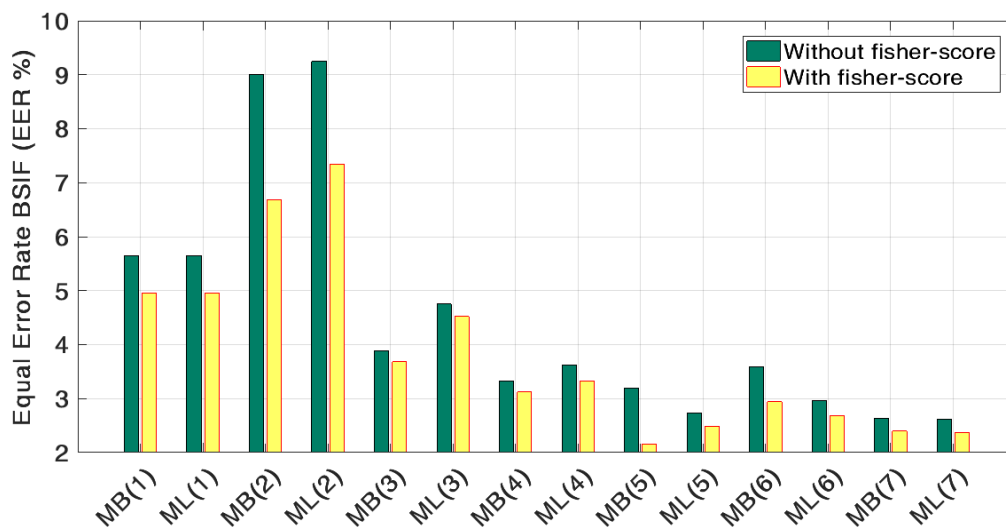


Figure III.6: Comparison of the results (in EER %) between ML-BSIF and MB-BSIF approach without (Fisher) and with (Fisher).

We note that the fisher score decreases the value of EER.

Figure 23 shows the ROC curve and the figure 24 shows the DET curve in NUAA database.

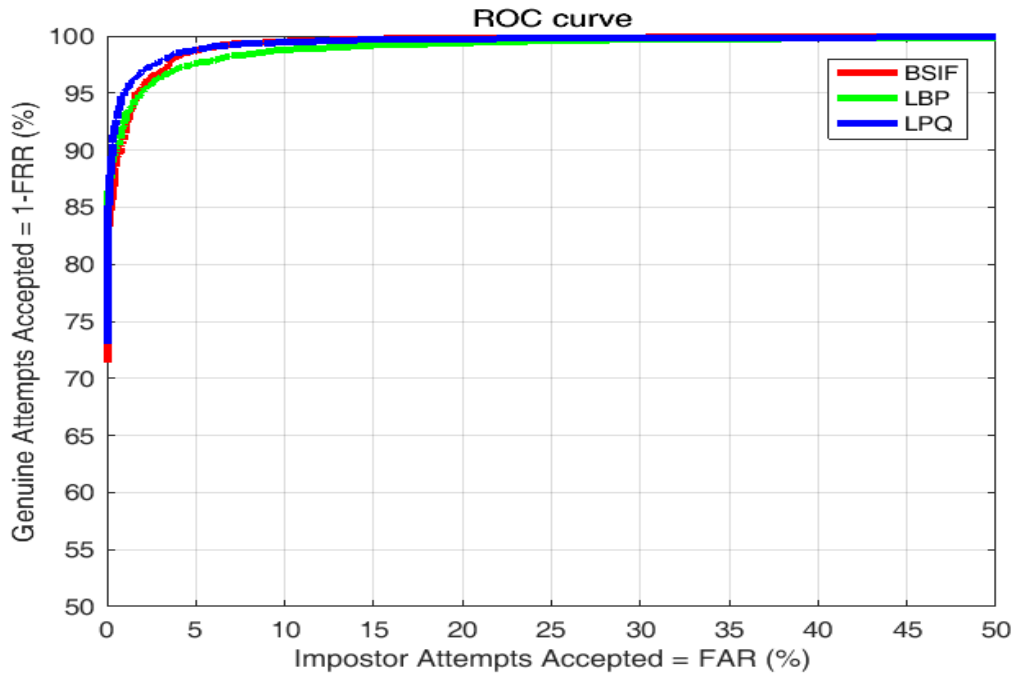


Figure III.7: ROC curve with Stasm-Fisher.

The ROC curve showing the best result of LPQ with fisher score compared to LBP, and BSIF because the LPQ descriptor is the better operator used to extracting features of blurring image.

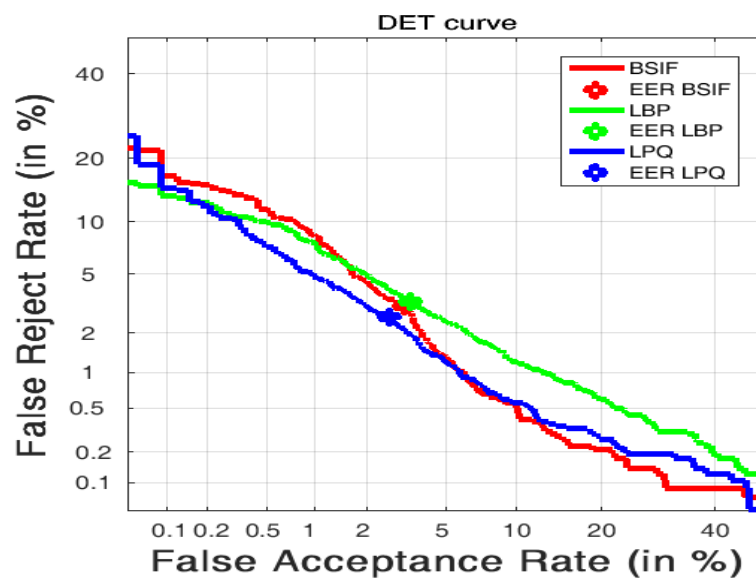


Figure III.8: Performance (DET curve) of the proposed approach with (Fisher).

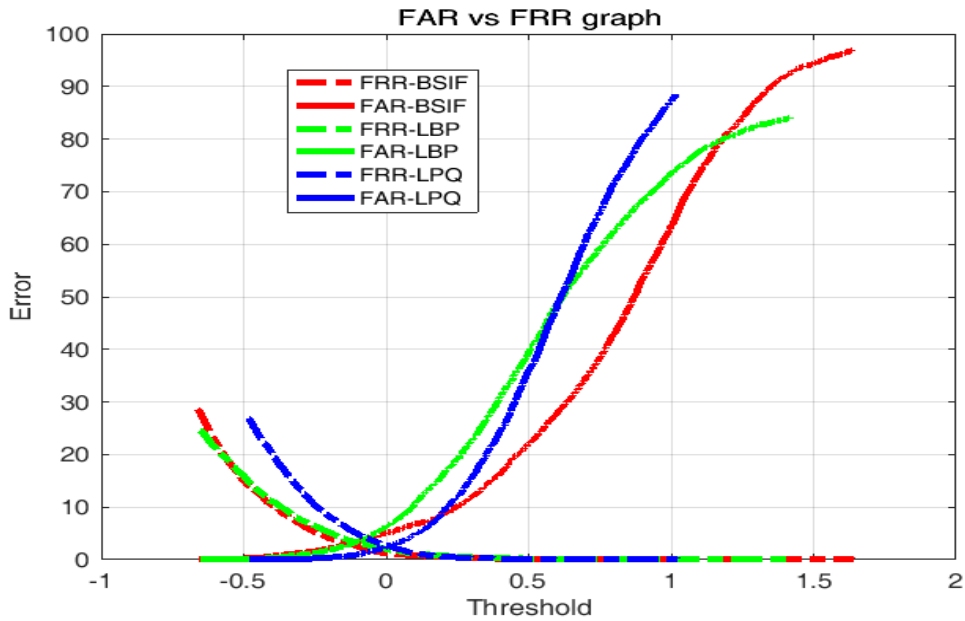


Figure III.9: FAR vs. FRR Curves.

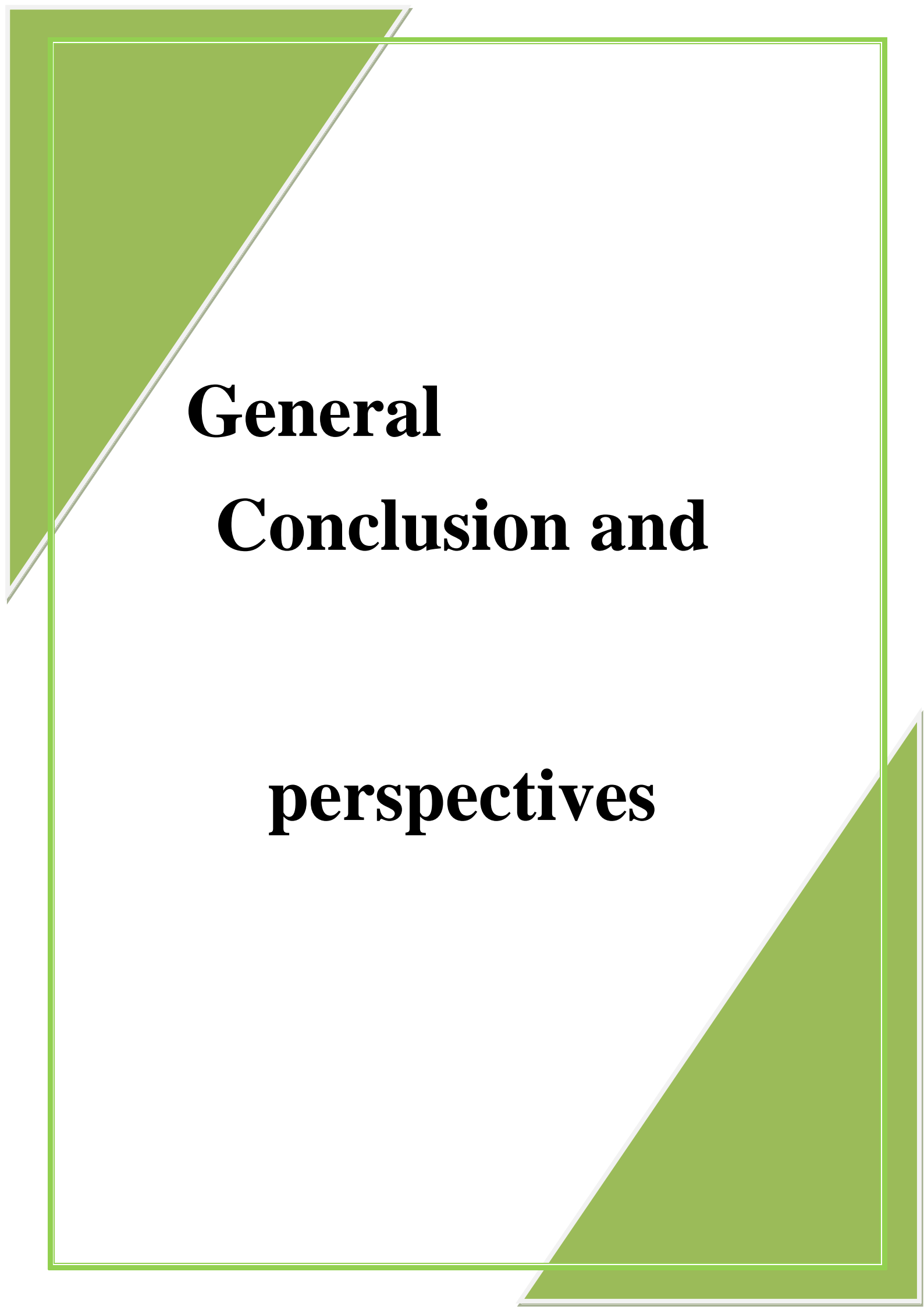
The observation of three figures shows us that the LPQ based method gives an optimum recognition rate open set 2.18%.

III.4 Conclusion

In this chapter we have presented applications on face anti-spoofing system based on LBP, LPQ and BSIF features extraction with MB, ML. The experimental results showed that the ML-LPQ features provide a better performance than the others, so the results obtained justify the effectiveness of our proposed approach system.

Our approach tested on NUAA Photograph Imposter Database which contains several real and fake faces showed excellent results.

We have seen how fisher score reducing the characteristic vectors with preservation of the discriminating values, as well as we used SVM classifier to train different spoof attacks then we can test if the person is real or not. We also found that the performance of biometric systems depends on several factors and that they vary from one system to another. Among the criteria for evaluating the quality of the biometric system, we presented all performance rate (FAR, FRR and ERR) as well as the ROC curves.



**General
Conclusion and
perspectives**

General

Conclusion and perspectives

Face recognition systems have been shown to be vulnerable to attacks with photography, mask and video. For this reason, countermeasure techniques are needed to mitigate the impact of identity theft on facial recognition.

In chapter 2, we proposed an anti spoofing technique, based on texture analysis for the detection of attacks with photography.

Different anti-spoofing methods have been developed and implemented that may significantly raise the difficulty level for attacks.

Finally, no matter what security measures are in place, no system is spoof-proof. Anti-spoofing measures simply make it more difficult for intruders to attack face biometric systems.

Our future suggestion is try to test our approach on other videos databases like Replay Attack and CASIA Face Anti-spoofing (CASIA-FA) database which is contains video recordings of real and fake faces.

Bibliography

- [1] Nidhi Saxena, Vipul Saxena, Neelesh Dubey, Pragya Mishra, "HAND GEOMETRY: A New Method For Biometric Recognition" ISSN: 2231-2307, Volume-2, Issue-6, January 2013.
- [2] Mohamad El-Abed, Christophe Charrier. Evaluation of Biometric Systems. New Trends and Developments in Biometrics, pp. 149 - 169, 2012.
- [3] PJames_L._Wayman,_Anil_K._Jain,_Davide_Maltoni,_Da_Biometric Systems, © Springer-Verlag London Limited 2011.
- [4] " Biometricsystème-IDTECK", Document available at:
<http://www.idteck.com/technology/biometrics.jsp>.
- [5] Florent PERRONNIN, Jean-Luc DUGELAY., "Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo", Traitement du Signal 2002 – Volume 19 – n°4.
- [6] John D, Woodward, Jr., "Christopher Horn, Julius Gatune, and Arynthomas,"Biometrics Alookat Facial Recognition",documented briefing by RAND public safety and Justice for the Virginia state crime commission, 2003.
- [7] F. Monrose and A. Rubin, "Authentication via Keystroke Dynamics", in the Fourth ACM Conference on Computer and Communication Security, 1997.
- [8] https://www.tutorialspoint.com/biometrics/behavioral_modalities.htm
- [9] P [Claus_Vielhauer]_Biometric_User_Authentication_for_IT_SECURITY Networked Society.
- [10] ISO/IEC 19795-1. Information technology – biometric performance testing and reporting – part 1: Principles and framework, 2006.
- [11] Rinu Anna Varghese, July Susan Mathew, " Face Anti spoofing methods "; IJSTE - International Journal of Science Technology & Engineering | Volume 2 | Issue 4 | October 2015 ISSN (online): 2349-784X
- [12] JAVIER GALBALLY, SÉBASTIEN MARCEL, and JULIAN FIERREZ "A Survey in Face Recognition"; IEEE VOLUME 2, pp.1532, 2014
- [13] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
- [14] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in

Proc. IEEE Int. Conf. Image Process. (ICIP), Oct. 2006, pp. 317–320.

[15] J. Galbally, R. Plamondon, J. Fierrez, and J. Ortega-Garcia, “Synthetic on-line signature generation. Part I: Methodology and algorithms,” *Pattern Recognit.*, vol. 45, no. 7, pp. 2610–2621, 2012.

[16] kose-neslihan, “spoofing-and-disguise-variations-in-face-recognition”, Phd Thesis 14/4/20014

[17] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” in *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, vol. 1. IEEE, 2001, pp. I–511.

[18] https://en.wikipedia.org/wiki/Viola%E2%80%93Jones_object_detection_framework

[19] F. G. Barbosa and W. L. S. Silva, “Automatic voice recognition system based on multiple Support Vector Machines and mel-frequency cepstral coefficients,” in *Proc. 11th Int. Conf. Natural Comput. (ICNC)*, Aug. 2015, pp. 665–670

[20] T. Ojala, M. Pietikainen, and T. Maenpaa, “Multiresolution gray-scale and rotation invariant texture classification with local binary patterns,” *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 24, no. 7, pp. 971–987, 2002.

[21] Azeddine Benlamoudi*, Djamel Samai*, Abdelkrim Ouafi†, Salah Eddine Bekhouche†, Abdelmalik Taleb-Ahmed‡, and Abdenour Hadid§; “Face spoofing detection using Local binary patterns and Fisher Score” IEEE CONFERENCE PAPER · MAY 2015 DOI: 10.1109/CEIT.2015.7233145.

[22] V. Ojansivu and J. Heikkilä. Blur insensitive texture classification using local phase quantization. In *Proc. Int. Conf. on Image and Signal Processing (ICISP'08)*, pages 236–243, 2008.

[23] T. Ojala et al. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *TPAMI*, 7(24):971–987, 2002.].

[24] <http://what-when-how.com/information-science-and-technology/biometric-identification-techniques-information-science/>

[25] <https://support.quest.com/technicaldocuments/statistics/current/textbook/support-vector-machines-svm>

[26] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” in *Computer Vision—ECCV 2010*. Springer, 2010, pp. 504–517.

[27] Bekhouche, Salah Eddine, et al. "Facial age estimation and gender classification using multi level local phase quantization." *Control, Engineering & Information Technology (CEIT), 2015 3rd International Conference on*. IEEE, 2015.

[28] Bekhouche, S. E., et al. "AUTOMATIC AGE ESTIMATION AND GENDER CLASSIFICATION IN THE WILD." (2015).

[29] Benlamoudi, A., et al. "Face spoofing detection using Multi-Level Local Phase Quantization (ML-LPQ)." (2015).

[30] Benlamoudi, Azeddine, et al. "Face spoofing detection from single images using active shape models with stasm and lbp." Proceeding of the Troisième CONFERENCE INTERNATIONALE SUR LA VISION ARTIFICIELLE CVA 2015. 2015.

[31] Benlamoudi, A., M. E. Zighem, and F. Bougourzi. "Face Anti-Spoofing combining MLLBP and MLBSIF."

[32] Bekhouche, Salah Eddine, et al. "Facial age estimation using bsif and lbp." arXiv preprint arXiv:1601.01876 (2016).

Abstract

In recent years, automatic personal identification is becoming an important requirement in variety applications such as access control, surveillance systems and physical buildings. Biometrics, which deals with identification of individuals based on their physical or behavioral features, has been emerging as an effective automatic identification technology, which offers more properties and several advantages over the traditional security. Face is one important biometric feature. Which provides uniqueness, stability and high distinguish ability.

Today's biometric systems are vulnerable to spoof attacks made by non-real faces. The problem is when a person shows in front of camera a print photo or a picture from cell phone. We study in this dissertation an anti-spoofing solution for distinguishing between 'live' and 'fake' faces. In our approach we focused in face detection using Viola-Jones algorithm and Active Shape Models with Stasm for locating landmarks. Then, we apply LBP, LPQ and BSIF operators to extract the features in each region of the image. Finally, we used a Support Vector Machine (SVM) classifier for determining whether the input image corresponds to a live face or not.

key words: Biometrics, Spoofing, Anti-Spoofing, STASM, LBP, LPQ, BSIF, SVM, NUAA.

ملخص:

أصبح التعرف الشخصي الآلي في السنوات الأخيرة مطلبا هاما في تطبيقات متنوعة مثل: التحكم في الدخول، أنظمة المراقبة، والمباني.

فظهرت القياسات الحيوية التي تعتمد على تعريف الأفراد على أساس الميزات البدنية ومظاهر السلوك باعتبارها تقنية فعالة للتعرف الآلي. توفر المزيد من الخصائص، والعديد من المزايا مقارنة بتقنيات الأمن التقليدية. الوجه هو إحدى الميزات الحيوية، والتي توفر التفرد وتضمن الاستقرار والقدرة الفائقة على التمييز.

حاليا نظم التحقق من الهوية عرضة لمحاولات الخداع بوجوه ليست حقيقية. المشكلة هي عندما يظهر شخص على الكاميرا صورة مطبوعة أو صورة من الهاتف المحمول. ندرس في هذه الأطروحة حل لمكافحة الغش لتمييز الوجوه الحقيقية من الكاذبة. في نهجنا، ركزنا على كشف الوجه باستخدام خوارزمية فيولا جونز ونماذج الشكل النشطة مع Stasm لتحديد الخصائص المميزة للوجه. ثم نطبق مشغلي LBP، LPQ و BSIF لاستخراج الخصائص الموجودة في كل منطقة من الصورة. وأخيرا، استخدمنا المصنف (SVM) لتحديد مدى توافق الصورة المعروضة مع الصورة الحقيقية. لقد كان لدينا تحليل تجريبي على قاعدة بيانات متاحة والتي هي NUAA Database.

الكلمات المفتاحية: بيومتري، تزوير، ضد التزوير، STASM، LBP، LPQ، BSIF، SVM، NUAA.

Resumé :

Au cours des dernières années, l'identification personnelle automatique devient une exigence importante dans les applications variées telles que le contrôle d'accès, les systèmes de surveillance et les bâtiments physiques. La biométrie, qui traite de l'identification des individus en fonction de leurs caractéristiques physiques ou comportementales, a émergé comme une technologie d'identification automatique efficace, qui offre plus de propriétés et de nombreux avantages par rapport à la sécurité traditionnelle. Le visage est une caractéristique biométrique importante. Ce qui offre l'unicité, la stabilité et la capacité de distinction élevée.

Les systèmes biométriques d'aujourd'hui sont vulnérables aux attaques par spoof effectuées par des visages non réels. Le problème est quand une personne montre devant une caméra une photo imprimée ou une photo du téléphone portable. Nous étudions dans cette thèse une solution anti-spoofing pour distinguer les visages réel et faux. Dans notre approche, nous nous sommes concentrés sur la détection des visages en utilisant l'algorithme Viola-Jones et les modèles Active Shape avec Stasm pour localiser les repères. Ensuite, nous appliquons les opérateurs LBP, LPQ et BSIF pour extraire les fonctionnalités dans chaque région de l'image. Enfin, nous avons utilisé un classificateur de machine de vecteur de support (SVM) pour déterminer si l'image d'entrée correspond ou non à une image en direct. Notre analyse expérimentale sur une base de données NUAA.

Mots clé: Biométrie, Falcification, Anti-Falcification, STASM, LBP, LPQ, BSIF, SVM, NUAA.