UNIVERSITY KASDI MERBAH OUARGLA

Faculty of New Information and Communication Technologies

Department of Electronics and Communications

Dissertation

In order to obtain the Diplôme de Master Academic

Domain: Science Industry: Electronics

Specialty: Industrial control

Presented by :

ASSAL MEGHNIA **MOULAY OMAR MAHMOUD**

Theme:

RECURSIVE LEARNING FUZZY LOGIC MODEL FOR BUILDING FEATURE EXTRACTOR IN IDENTIFICATION BIOMETRIC SYSTEM

Supported publicly

On: 25 / May / 2017

Before the jury:

Mr SMAHI MOKHTAR	**MA (A) Supervisor UKM Ouargla**
Mr KADRI FARID	**MC (B) President UKM Ouargla**
Mr NASRI	**MA (A) Examiner UKM Ouargla**

Academic year 2016/2017

Dedication

To my parents

To my brother and sisters

TO MY WIFE

To my children (Zinou, Ahmed)

To all my friends

To all my masters and teachers

Mahmoud

Dedication

RECURSIVE LEARNING FUZZY LOGIC MODEL FOR BUILDING FEATURE EXTRACTOR IN IDENTIFICATION BIOMETRIC SYSTEM

Acknowledgments

We would like to express our sincere thanks to:

- *Our promoters Mr SMAHI Mokhtar and Mr BENSID Khaled, who throughout this work have given us their valuable advice, their remarks and who have placed their trust in us*

- *We would like to thank all our teachers throughout our school and university life.*

- *We thank the president of the jury: Mr. and thus the members of this honorable jury: Mr. and Mr..*

- *Finally, we express our thanks to all those who helped from near or far.*

Summary

List of tables

List of figures

ملخص

الهدف من هذه المذكرة التي بين أيدينا هو تطبيق المنطق الضبابي في أنظمة التعرف البيومترية، وذلك باستعماله في بناء مستخرج الخصائص الشخصية من الصور والتي هي مرحلة مهمة في أي نظام بيومتري. تم اختيار النموذج الضبابي المناسب لهذه العملية وذلك باستعمال دوال انتماء غوصية لاحداثيات بكسل الصور و دوال انتماء نقطية للقيمة الرمادية للبكسل. هذا النموذج يخضع لعملية تدريب لتتناسب مخرجاته مع صورة الشخص المقدمة لتُعتبر في الأخير عناصر هذا النموذج الممرن كشعاع خصائص معرف للشخص. يتم في الأخير استعمال الحاسوب المجهز بنظام الماطلاب وكذا قاعدة معلومات مشكلة من خمسمائة شخص باثني عشر صورة لكل أحد، وذلك لاختبار النظام البيومتري الجديد حيث تم الحصول على نتائج جيدة حسب البيانات الموضحة.

الكلمات الدلالية: النظام البيومتري، المنطق الضبابي، مستخرج الخصائص،

Résumé

L'objectif de cette mémoire est d'appliquer la logique floue dans les systèmes biométrique d'identification. Cette logique est utilisée exactement pour construire un extracteur de caractéristiques qu'est une étape essentielle dans le système biométrique. Pour cela, un modèle flou est choisi par ces fonctions d'appartenance des coordonnées de pixels d'image de type gaussien et celles de niveau de gri de type constants. Ce modèle est subi à une opération d'apprentissage afin de l'approcher à l'image en cours d'utilisation. Les paramètres de modèle apprenti sont les éléments du vecteur de caractéristique. Les tests de ce système biométrique sont fait à l'aide du logiciel Matlab et une base de données de 500 personnes de 12 images chacun. Les résultats obtenus justifient ce choix.

Mots clés: Système biométrique, logique floue, image palmaire, apprentissage, vecteur de caractéristiques

Abstract

The objective of this dissertation is the integration of fuzzy logic to biometric systems for person identification. Fuzzy logic is used exactly to build the feature extractor of the biometric system. For this propose a fuzzy model for the image is chosen by selecting Gaussian membership functions for pixel coordinates and constants functions for gray level of pixels. The fuzzy model will be learned by an iterative procedure to extract the vector of characteristics. This biometric system is tested using Matlab software and a database of 500 persons with 12 images for each person. The results of simulation give good results with the FRR, FAR and EER values.

Key words: biometric system, fuzzy logic, learning, palm modality, feature vector

General introduction

General introduction

In all security and access control domains, passwords or keys are used that consist of numbers or letters. But, in recent times with the advancement of technology these passwords have become easily forgeable and crossable. This is why researchers from different fields have focused their work on keys that are impossible to falsify, safe and above all effective. Biometrics has become fashionable in areas that require a high level of security and control and of all the biometric technologies that exist.

In a biometric recognition system, the extraction of the characteristics, or the extraction of the vector of observations is an important step. A feature vector (observation vector) is used to represent the discriminating characteristics of the image of the person's modality with generally a reduced size with respect to the image.

Several techniques are used to generate feature vector. Fuzzy logic is a widely used technique in the field of control of industrial systems and processes; our contribution is to use this technique for generating the vector of biometric characteristics. In this case, fuzzy feature vector is the set of fuzzy model parameters that are adjusted to meet the characteristics of the person's image.

For this, our brief entitled "Recursive learning fuzzy logic model for building feature extractor in identification biometric system" is the tool to achieve the objective of this contribution, which is organized as following:

In the first chapter, we introduce some definitions of biometrics and different biometric modalities, and then we detail the palm modality for the identification of a person.

The theoretical concepts of fuzzy logic, fuzzy system and the learning approach are discussed in the second chapter.

After this, and by the third chapter, we give the essential steps helping us establishing, the fuzzy model for palm image and the fuzzy feature extractor for the entire biometric system.

In the last chapter, we have studied our biometric system using a RIO database of 500 person's palms where we have made different tests of biometric identification and we have given all the results of treatment in this process.

Chapter I

Biometric system

Chapter I : Biometric system

I.1 Introduction to Biometrics

Nowadays, biometrics is an emerging technique that allows us to verify the identity of an individual busing one or more of his or her personal characteristics. Its advantage is to increase the level of security by using as an identifier data that cannot be lost, stolen, or tampered with unlike passwords or personal identification number (PIN) codes, since they are directly related to the body or the behavior of the individual. A resurgence of interest in these techniques has been observed sincethe2000s, a period when security policies were implemented in the G8 countries following the attacks of 9/11, among others. Recently several big deployments of biometrics systems have taken place. Let us quote the biometric passport, national identity cards and the new census of the

I.2 Definition of biometric

Biometrics is the science of establishing the identity of a person based on 'Who you are' refers to his physiological characteristics such as fingerprints, iris, or face. And 'What you produce' refers to his behavioral patterns that characterize your identity such as the voice or the signature. These physiological or behavioral characteristics are called biometric modalities. Biometrics such as we wants to use it today in the security systems aims to make an automatic recognition.[1]

The importance of biometrics in our society has been reinforced by the need for large-scale identity management systems whose functionality relies on the reliable determination of an individual's identity in the context of several different applications. Examples of these applications include:

- Sharing networked computer resources.
- Granting access to nuclear facilities.
- Performing remote financial transactions.
- Boarding a commercial flight.
- Web-based services (e.g., online banking).
- Customer service centers (e.g., credit cards).

I.3 Biometric characteristics

The choice of a biometric trait for a particular application depends on a variety of issues besides its matching performance and accuracy. In theory, any human characteristic (physiological or behavioral) can be used as a biometric identifier as long as it satisfies these requirements:

- Universality: Every person in the population should posse the biometric modality.

- Distinctiveness: The given modality should be sufficiently different across individuals comprising the population, it's also known as uniqueness.

- Permanence: The biometric trait should be sufficiently invariant over a period of time with respect to the matching algorithm.

- Collectability: The ability to measure the biometric quantitatively, in other words, it should be possible to acquire and digitize the biometric traits using suitable devices that do not cause undue troubles to the individual.

The biometric modalities do not have all these properties, or at least have them with different degrees. No biometrics is thus perfect or ideal, but is more or less adapted to applications. The compromise between presence or absence of some of these properties is done according to each application requirements, in the choice of the biometric method.[1]

I.4 Biometric Modalities

Different biometric modalities have been proposed and used in various applications. Physiological biometrics includes the ear, face, hand geometry, iris, retina, palm print and fingerprint. Behavioral biometrics includes voice, signature, gait or key stroking. Examples of these traits are shown in the following sections:

I.4.1 Physiological

I.4.1.1 Definition of palm print

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, as shown in Figure III.1. 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 its skin such as the lines (main and wrinkles), points, minuteness and texture.

Figure I-1: The palm of the hand

A palmar identification can be seen as the ability to identify one person among others in a unique way through an appropriate algorithm exploiting the Characteristics of the palmar footprint.

I.4.1.2 Fingerprint

Humans have used fingerprints for personal identification for many decades. Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations.

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of fetal development. It has been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person. One main shortcoming for fingerprint identification systems is that small injuries and burns highly affect the fingerprint. [3]

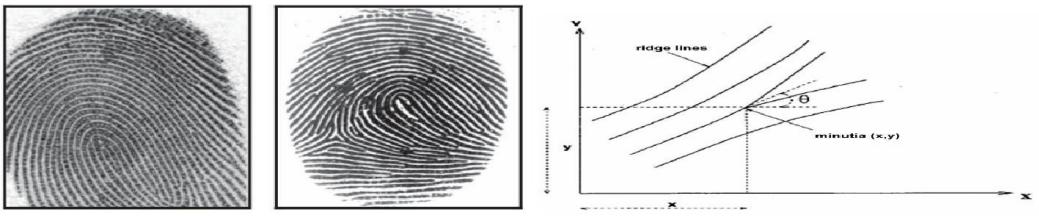


Figure I-2 :Fingerprint (a)(b) Examples (c) Minutiae Representation

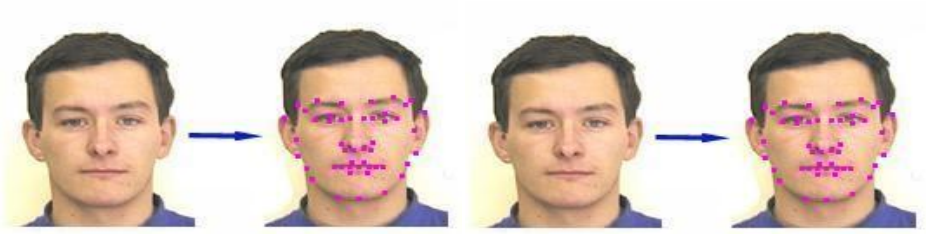
I.4.1.3 Face

Face recognition is an active area of research with many applications. It consists of the analysis of facial features or patterns for the authentication or recognition of an individual's identity. During the past 25 years, a substantial amount of research effort has

been devoted to face recognition. A number of face-recognition techniques are widely popular, including:

- Principle Component Analysis (PCA)
- Linear Discriminant Analysis (LDA)
- Singular Value Decomposition(SVD)
- A variety of Neural Network-based technique
-

The performance of these approaches is quite impressive and is sufficiently mature that they can be ported to real-time experimental/demonstration systems. Generally, there are two major tasks in face recognition:



a -Locating faces in input images ***b*- Recognizing the located faces**

Figure I-3: Face Modality

I.4.2 Behavioral traits

I.4.2.1 Keystroke dynamics

The recognition of keystroke dynamics is the process of analyzing the way an individual types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to recognize the individual based on habitual typing rhythm patterns. Keystroke dynamics are described by speed (the time a key is pressed, the time between keys pressed), rhythm, precision, keys used (e.g., left Shift key or right Shift key, Caps Lock), and other typing characteristics.

Similar to other active traits, an individual's keystroke rhythm evolves over time, for instance by switching from two finger typing to touch typing. Subjects can become tired or distracted during the course of a work day, which in turn affects the typing rhythm. Recognition accuracy would be very limited if only a small number of variables were considered. The longer the text entered the more characteristics revealed and the more accurate recognition can be. The ultimate aim is to be able to continually check the identity of an individual typing on a keyboard. [3]

The equipment requirements are minimal (keyboard) and give information about the huge field of possible applications. For instance, Psylock, a keystroke recognition system developed at University of Regensburg (Germany), uses a JavaScript function to capture the user's keystroke dynamics on the client side (using a web browser), transmits the data on an encrypted connection (SSL) to an authentication server, which replies to authentication requests. The university successfully used the system to authenticate users for service desk tasks (password reset); it was also proposed as an alternative to transaction authentication numbers (TAN) in home-banking applications.

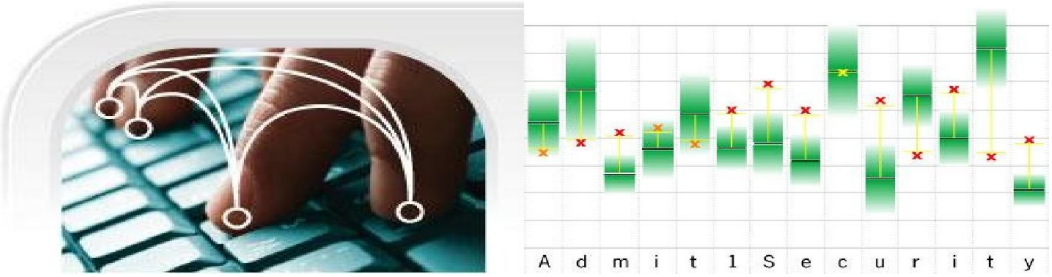


Figure I-4: Keystroke Dynam

I.4.3 Chemical

To this point, modalities have been presented and categorized on whether their recognition depends on the physical aspect or the behavior of individuals. This last part deals with a modality that is of the chemical nature: the DNA.

I.4.3.1 DNA

The cells that contain DNA share genetic information through chromosomes. Humans have 23 chromosomes pairs that house a person's DNA and their genes. 0.3% of an individual's DNA is variable repetitive coding unique to an individual. This repetitive coding is the basis of DNA biometrics. DNA recognition uses genetic profiling, also called genetic fingerprinting, to isolate and identify these repetitive DNA regions that are unique to each individual to either identify or verify a person's identity.[3]

The basic steps of DNA profiling include:

a. Isolate the DNA (sample can originate from blood, saliva, hair, semen, or tissue)
b. Section the DNA sample into shorter segments containing known variable number tandem repeats (VNTRs)identical repeat sequences of DNA
c. Organize the DNA segments baize

d. Compare the DNA segments from various samples

The more repeats of sequences there are for a given sample, the more accurate the DNA comparison will be, thus decreasing the likelihood of the sample matching multiple individuals. A few drawbacks of this technique are the depth of the procedure, the physical invasiveness of obtaining the DNA sample, and the time required to perform a DNA comparison. Also contamination of the sample renders the comparison impossible.

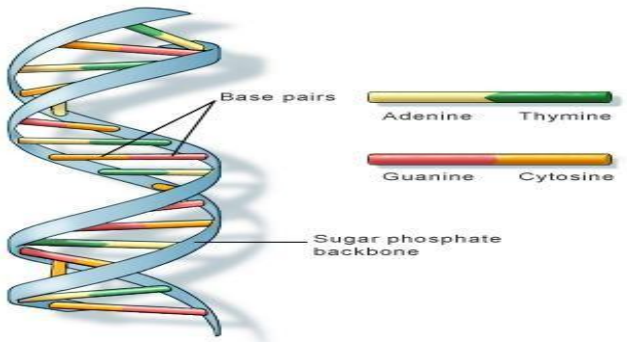


Figure I-5: DNA Code

I.5 The structure of a biometric system

A biometric system is a pattern recognition system, which acquires the 'individual biometric data , extracts some features from this data , compares it against one or the whole stored in the database, and it take a decision based on the comparison results, so, a biometric system function according to the following stages :

- **Enrollment**: In order to access to the biometric system, the user has to be registered. In this stage, we assign an ID, and capture an image of the specific biometric trait. This image is then converted to a template (after the feature extraction process).
- **Storage**: In this stage, the biometric template is stored on a database, an individual workstation or portables devices for the future comparison (authentication).

Matching: When the user (already enrolled in the database) tries to access the System for the verification or identification task, he will introduce another biometric sample, which is converted into a template and is then compared to the stored template. Then, according to the final decision taken by the biometric system, the user is then accepted as client, or rejected as an impostor. [2]

Every biometric system is composed of two phases, the first called enrollment and the second Called recognition, these two phases require a main step called extraction

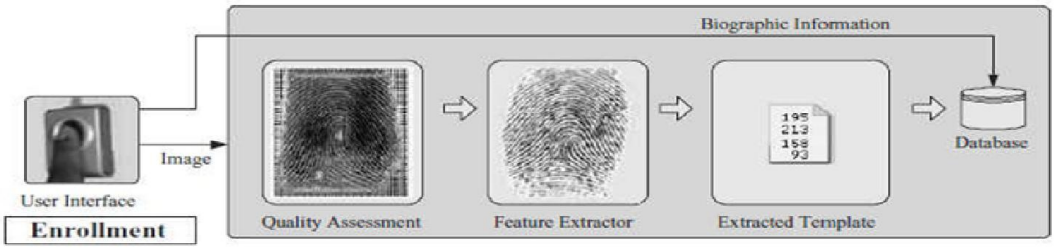


Figure I-6: Biometric Enrollment[3]

I.6 Verification versus identification

There are several types of application which require the user's authentication. Depending on the application context, these applications can be separated into two categories which are the identity verification or identification. [3]

I.6.1 Verification

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. Generally , it is usually associated with the means of traditional identification such as a smart card, a badge or a key, and is used as an additional security to ensure that the card or the badge was not stolen or is not used by a not authorized person. The verification is a YES or NO decision type with the question: "the individual is he well that which he claims to be? The system conducts a one-to-one comparison to determine whether the claim is true or not. Verification is typically used for positive recognition, to prevent multiple people from using the same identity.[3]

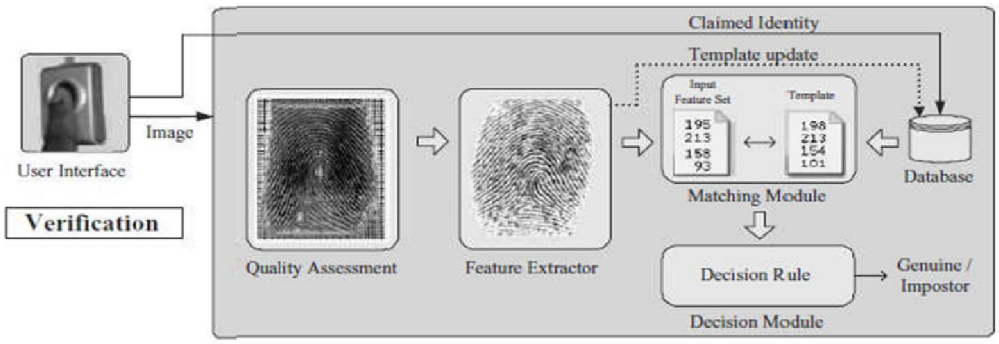


Figure I-7: Biometric Verification.

I.6.2 Identification

In the identification mode, to recognize an individual the biometric system searches in the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity ("Whose biometric data is this?"). Identification can be used for the negative recognition to prevent a single person from using multiple identities. The identification can be used to authorize the use of the services, such as controlling the access to a protected zone for which only a restricted number of people (saved in a database) have the access authorization.[3]

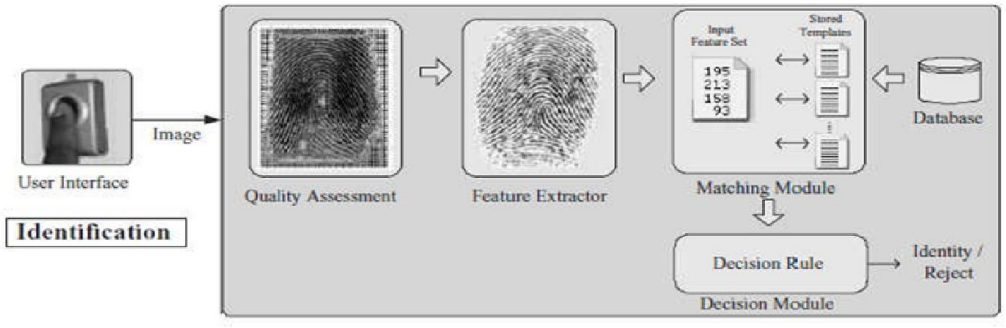


Figure I-8: Biometric Identification

I.7 Multimodal biometric systems

Biometric authentication systems that used only one biometric trait may not accomplish the requirements of demanding applications in terms of the characteristics described before, and the limitations of a unmoral biometric system can be addressed by designing a system that integrates (fuse) biometric information from multiple sources, for example, multiple traits of the same individual, such systems, known as multimodal biometric systems.

Multimodal biometric system is expected to be more robust to noise, address the problem of non-universality, improve the matching accuracy, and provide reasonable protection against spoof attacks.[4]

I.8 Different levels of fusion

Biometric system has four important modules. The sensor module acquires the biometric data from a user via sensors; the feature extraction module processes the acquired biometric data and extracts a feature set to represent it; the matching module compares the extracted feature set with the stored templates using a classifier or matching

algorithm in order to generate matching scores; in the decision module the matching scores are used either to identify an enrolled user or verify a user's identity.

In a multibiometric system, fusion can be accomplished by utilizing the information available in any of these modules. Thus, four different levels of fusion are possible: the sensor level, the features extraction level, the matching score level, and the decision level. Sanderson et al. have classified information fusion in biometric systems into two broad categories: pre-classification fusion and post-classification fusion. The sensor level and the features extraction level are referred to as pre-classification fusion while the matching score level and the decision level are referred to as post-classification fusion.[3]

I.8.1 Pre-Classification fusion

Pre-classification fusion refers to combining information prior to the application of any classifier or matching algorithm. This integration can take place either at the sensor level or at the feature level.

- ***Sensor Level***

The raw data, acquired from sensing the same biometric characteristic with two or more sensors, is combined. Sensor level fusion is applicable only if the multiple sources represent samples of the same biometric trait obtained either using a single sensor or different compatible sensors [10].

- ***Feature Extraction Level***

This level refers to combining different feature sets extracted from multiple biometric sources. When the feature sets are homogeneous (e.g., multiple measurements of a person's hand geometry), a single resultant feature vector can be calculated as a weighted average of the individual feature vectors. When the feature sets are non-homogeneous (e.g., features of different biometric modalities like face and hand geometry), we can concatenate them to form a single feature vector. Concatenation is not possible when the feature sets are incompatible (e.g., fingerprint minutiae and Eigen-face coefficients) [10].

I.8.2 Post-Classification fusion

In the post-classification fusion the information is combined after the decisions of the classifiers have been obtained. This integration can take place either at the matching score level or at the decision level.

- ***Matching Score Level***

When each biometric system outputs a match score indicating the proximity of the input data to a template, integration can be done at the match score level. This is also known as fusion at the measurement level or confidence level.

The match scores output by biometric matchers contain the richest information about the input pattern. Also, it is relatively easy to access and combine the scores generated by the different matchers. Consequently, integration of information at the match score level is the most common approach in multimodal biometric systems [04].

- ***Decision Level***

Integration of information at the abstract or decision level can take place when each biometric system independently makes a decision about the identity of the user (in an identification system) or determines if the claimed identity is true or not (in a verification system)

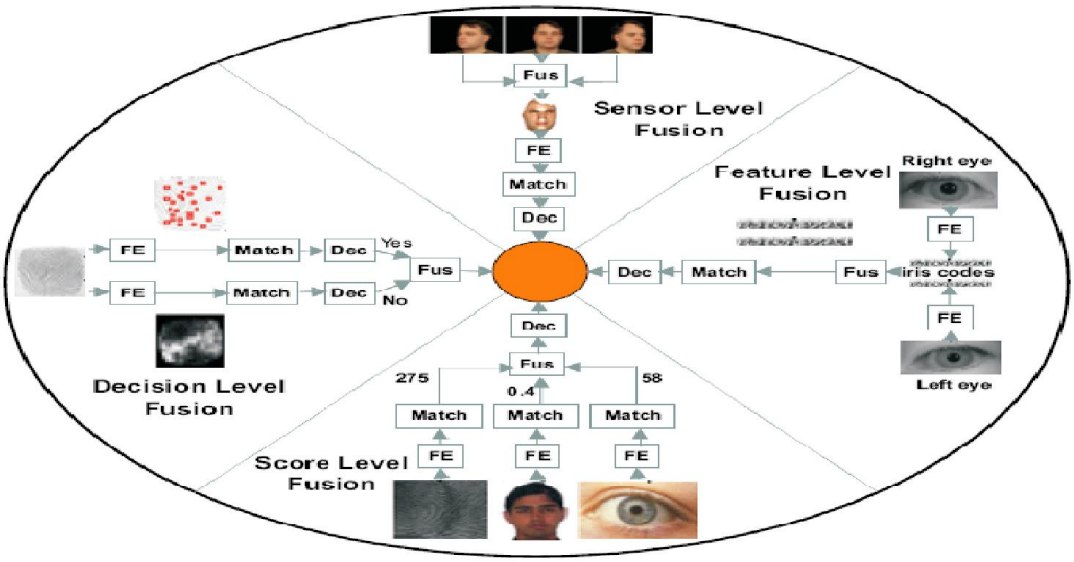


Figure I-9: Fusion levels in multimodal biometrics.

It is difficult to combine information at the feature level because the feature sets used by different biometric modalities may either be inaccessible or incompatible. Fusion at the decision level is too rigid since limited amount of information is presented at this level. Therefore, integration at the matching score level is generally preferred due to the ease in accessing and combining the scores generated by different matchers, also fusing information at this level is interesting because it reduces the complexity by allowing different classifiers to be used independently of each other .[04]

I.9 Evaluation of different modalities

As mentioned before, there are three different types of performance evaluation, but in our study we will concentrate on the most common one which is known as "technological" evaluation of the biometric and multimodal biometric systems, i.e., an evaluation of their error rates for the identity verification. There are some of the biometric systems errors that cannot be treated because they depend on the acquisition module. These errors are impossibilities of acquisition "failure to enroll" or "failure to acquire" by the sensor of the biometric data [4]

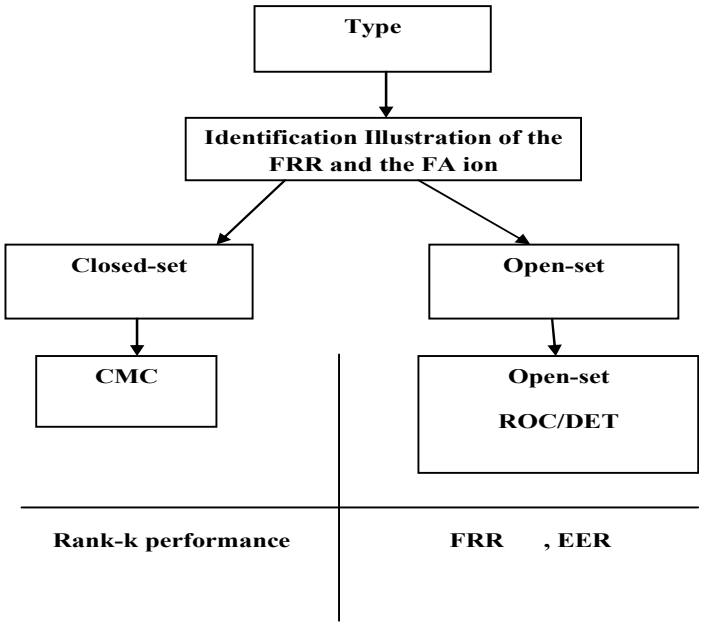


Figure I-10: Classification of different biometrics performance charts

I.9.1 Evaluation criterion

• **False Rejection Rate (FRR):** The number of false rejection accesses divided by total number of clients (NC) in the lest database

The decision error rates of the multimodal biometric verification system (FAR and FRR) are dependent on the decision threshold (η*)* and are given according to the threshold by:$FAR(\eta) = \frac{FA(\eta)}{NI}$ **(1.1)**

• **False Acceptance Rate (FAR):** and False Rejection Rate (FRR): FAR and FMR are often used interchangeably in the literature, so as FNMR and FRR. However, their subtle difference is that FAR and FRR are system-level errors which include samples failed to be acquired or compared

• **Equal Error Rate (EER):** The rate at which FMR is equal to FNMR.

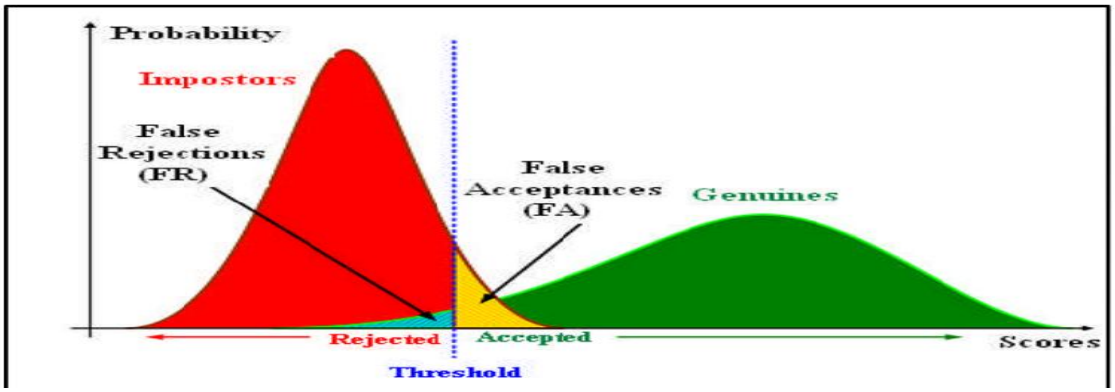


Figure I-11:Illustration of the FRR and the FAR

Evaluation carve

• **Receiver Operating Characteristic (ROC):** An ROC curve plots FRR (in the Y-axis) versus FMR (in the X-axis), or FRR versus FAR. Alternatively, a ROC curve also plots TAR versus FAR.

I.9.2 CMC

For closed-set identification, the Cumulative Match Characteristic (CMC) curve is commonly used. It is a plot of the identification rate at rank-k. A probe (or test sample) is given rank-k when the actual subject is ranked in position k by an identification system. Thus, a rank-1 outcome is considered a correct identification. The identification rate is an estimate of the probability that a subject is identified correctly at least at rank-k. Hence, identification rate is necessarily an increasing function of k.

I.10 Conclusion

The field of study that this work focuses on, biometrics and multibiometric systems has been introduced in this chapter. To have a grasp on the concept of biometrics, an overview of the characteristics of a biometric system as well as some of the widely used modalities was given. We also got acquainted with the two modes of a biometric authentication system: identification and verification.

Our investigations led to the conclusion that the unimodal systems have various limitations. We offered the multibiometric systems as a solution to elevate some of said limitations

Chapter II

Fuzzy logic

Chapter II : Fuzzy logic

II.1 History

The term “fuzzy set” first appeared in 1965 when professor Lotfi A. Zadeh from the university of Berkeley, USA, published a paper entitled “Fuzzy sets”. Since then he has achieved many major theoretical breakthroughs in this field and has been quickly joined by numerous research workers developing theoretical works.[05]

II.2 Fuzzy Set Theory

II.2.1 Definition of Fuzzy set

A fuzzy set A, defined in the universal space X, is a function defined in X which assumes values in the range [0, 1].

A fuzzy set A is written as a set of pairs $\{x, \mu_A(x)\}$ as

$$A = \{\{x, \mu_A(x)\}\}, \text{ x in the set X}$$

Where x is an element of the universal space X, and the value $\mu_A(x)$ is the membership grade of the element x in a fuzzy set A.

Example 1:

Assume that X is the universal space of ages in natural numbers, and SMALL is a fuzzy set of X consisting of ages less than 12 (12 included).

Assume: Small(1)=1, Small(2)=1, Small(3)=0.9,Small(4)=0.6, Small(5) = 0.4, Small(6) = 0.3, Small(7) = 0.2, Small(8) = 0.1, Small(u) = 0 for $9 \leq u \leq 12$.

Then, following the notations described in the definition above:

The SmallSet= {{1, 1 }, {2, 1 }, {3, 0.9}, {4, 0.6}, {5, 0.4}, {6, 0.3}, {7, 0.2}, {8, 0.1}, {9, 0 }, {10, 0 }, {11, 0}, {12, 0}}

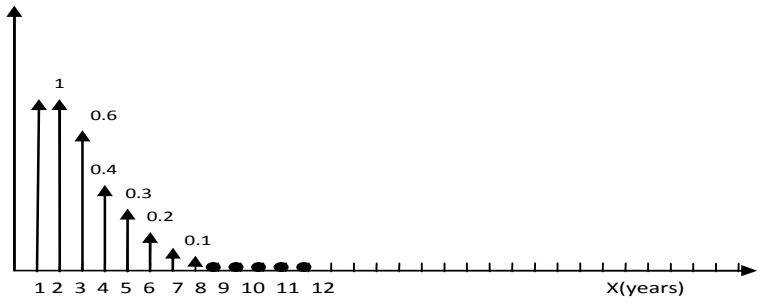


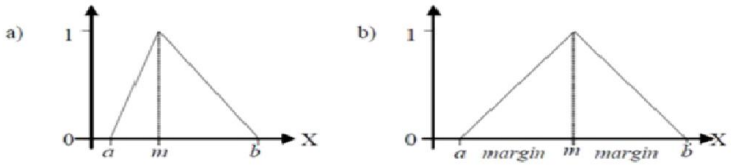
Figure II-1 :Fuzzy set

II.2.2 Fuzzy Set Representation

The fuzzy sets can be represented by several forms; between those forms we give the most known and used:

II.2.2.1 Triangular

Defined by its lower limit a, its upper limit b, and the modal value m, so that a < m < b. We call the value b-m margin when it is equal to the value m – a.



Triangular fuzzy sets: a) general and b) symmetrical.

$$A(x)=\begin{cases}0 & \text{if } x\le a\\ (x-a)/(m-a) & \text{if } x\in(a,m]\\ (b-x)/(b-m) & \text{if } x\in(m,b)\\ 0 & \text{if } x\ge b\end{cases}$$

Figure II-2: Representation triangular.

II.2.2.2 Trapezoid Function

Defined by its lower limit ***a*** and its upper limit ***d***, and the lower and upper limits of its nucleus, b and c respectively.

$$T(x)=\begin{cases}0 & \text{if } (x\le a) \text{ o } (x\ge d)\\ (x-a)/(b-a) & \text{if } x\in(a,b]\\ 1 & \text{if } x\in(b,c)\\ (d-x)/(d-c) & \text{if } x\in(b,d)\end{cases}$$

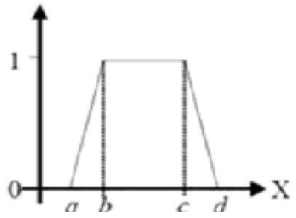


Figure II-3: Representation Function

II.2.2.3 Gaussian Function

This is the typical Gauss bell, defined by its Mid-value m and the value of σ > 0. The smaller σ is, the narrower the bell.

$$G(x) = \exp\left[\frac{-(x-\mathbf{m})^2}{2\sigma^2}\right]$$

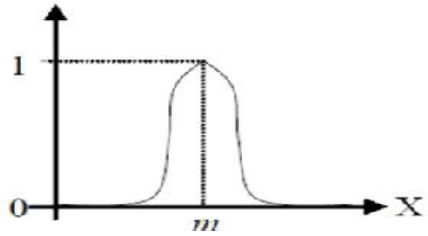


Figure II-4: Representation Gaussian

II.2.3 Fuzzy Set Operations

To clarify the most famous fuzzy operations we suppose that A and B are two fuzzy sets of the universal space X defined by their membership functions $\mu_A(x)$and μB(x) respectively.

II.2.3.1 Intersection

The intersection between A and B is a fuzzy set A∩B of X that can be defined by its membership function $\mu_{A\cap B}(x)$ equals to the minimum of $\mu_A(x)$) and μB(x):

$$\mu_{A\cap B}(x) = \text{MIN}(\mu_A(x), \mu_B(x))$$

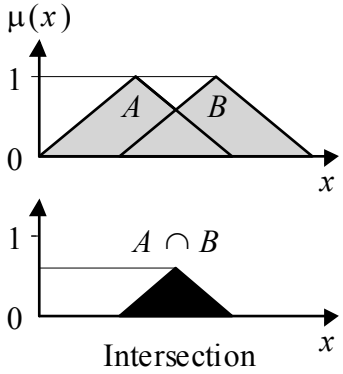


Figure II-5: Intersection

II.2.3.2 Union

The union between A and B can be defined by the maximum of $\mu_A(x)$and $\mu_B(x)$:

$\mu_{A\,U\,B}(x) = \text{MAX}(\mu_A(x), \mu_B(x))$

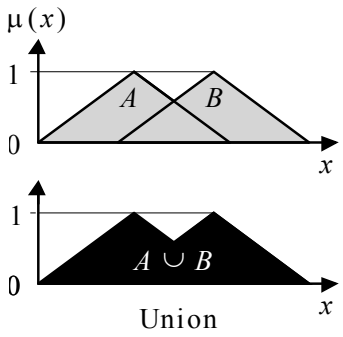


Figure II-6: Union

II.2.3.3 Complement

The complement of A is a fuzzy set $\bar{A}$ of X that can be defined by its membership function $\mu_{\bar{A}}(x)$equals to one minus$\mu_A(x)$:

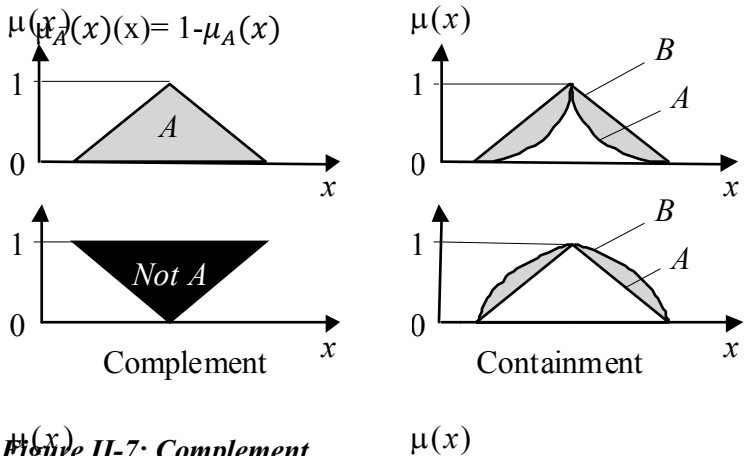


Figure II-7: Complement

II.2.4 Fuzzy Logic Reasoning

II.2.4.1 Linguistic variables, values and hedges

The basic concept in fuzzy reasoning is the *linguistic variable* that is a variable having values like words or expressions in a natural language, in example b, "Age" is a linguistic variable.

The range of possible values of a linguistic variable represents the universe of discourse of that variable. For example, the universe of discourse of the linguistic variable "Age «might be the range between 0 and 150year and may include such linguistic values as Very Small, Small, Young and old and Very Old. Those values are considered as fuzzy subsets.[05]

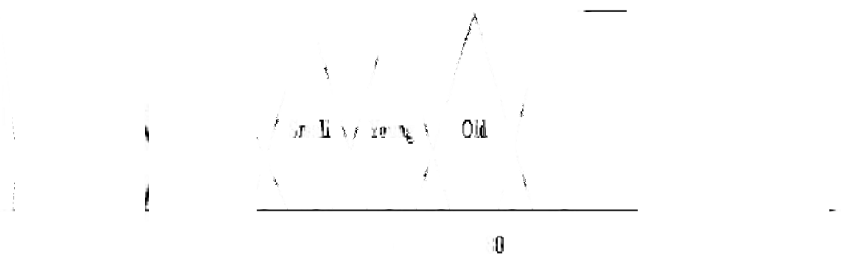


Figure II-8: Representation linguistic variable

A linguistic variable carries with it the concept of fuzzy set qualifiers, called hedges. Hedges are terms that modify the shape of fuzzy sets. They include adverbs such as very, somewhat, quite, more or less and slightly.

II.2.5 Fuzzy Proposition

A fuzzy proposition is a rate between the linguistic variable and its value in the range [0, 1].The fuzzy proposition is given in a natural language by the following form:

Xis A

In this case, *x* is a linguistic variable and A is a linguistic value.

Example: Ali is 15 years old, so for John "Age is Small" is a fuzzy proposition that has a value of 0.4. Also "Age is Young" is another fuzzy proposition that has another value of 0.2.

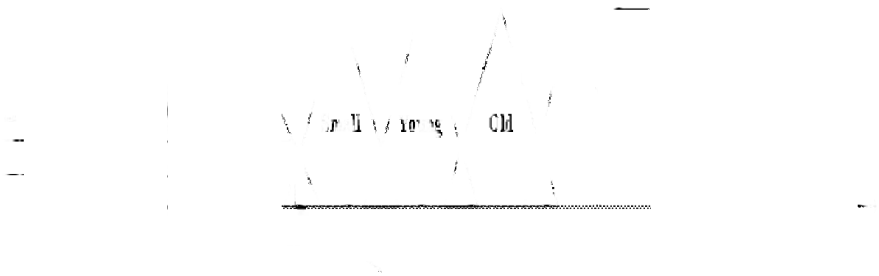


Figure II-9: Fuzzy proposition

II.2.6 Fuzzy rule

Zadeh [1973] was the first who gave a notion for the fuzzy rule in the form:

IF x is ATHEN y is B

Where x and y are linguistic variables; A and B are linguistic values determined by fuzzy sets on the universe of discourse X and Y, respectively.

Rule : IF x is A THEN y is B

Premise : x is A

Conclusion : y is B

Example:

If Age is Small THEN Clothe-Size is S

II.3 Fuzzy Systems

A fuzzy logic model with its fundamental input-output relationship consists of three components namely; the fuzzifier, the inference engine and the defuzzifier.

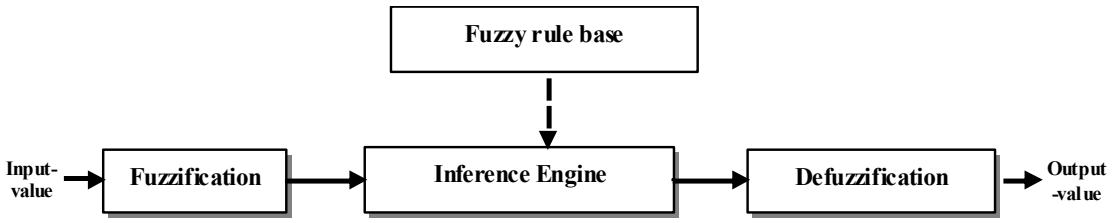


Figure II-10: Structure of a Fuzzy Logic Model

II.3.1 Fuzzification

Fuzzification determines the fuzzy subset to which the data value belongs as well as its degree of belongingness. The degree of belongingness is the value of the membership function for that particular data.

II.3.2 Inference Engine

Once all input values have been fuzzified into their respective linguistic values, the inference engine will access the fuzzy rule base of the fuzzy expert system to derive linguistic values for the intermediate as well as the output linguistic variables.

The two main steps in the inference process are aggregation and composition. Aggregation is the process of computing for the values of the IF (antecedent) part of the rules while composition is the process of computing for the values of the THEN (consequent) part of the rules.[06]

During aggregation, each condition in the IF part of a rule is assigned a degree of truth based on the degree of membership of the corresponding linguistic term. From here, either the minimum (MIN) or product (PROD) of the degrees of truth of the conditions is usually computed to clip the degree of truth of the IF part. This is assigned as the degree of truth of the THEN part.

II.3.3 Rule Base

The Fuzzy Rule Base is characterized by construction of a set of linguistic rules based on expert's knowledge. The expert knowledge is usually in the form of IF-THEN rules, which can be easily implemented by fuzzy conditional statements.

Example

If Age is small and Weight is High THEN Clothe-Size is L

OR

If Age is small andWeight is medium THEN Clothe-Size is M

OR

If Age is Small and Weight is Low THEN Clothe-Size is S

II.3.4 Defuzzification

Without defuzzification, the final output from the inference stage would remain a fuzzy set. In most process applications, there is a requirement for a numbered output value. In this step a fuzzy set is reduced to a single numbered output. There are a number of defuzzification techniques available for this operation, some of which are described below

II.3.4.1 Centre of Gravity (CoG) Method

The CoG, also known as the centre of area, method is a technique for finding a crisp value (u) from the mid-point of the output fuzzy set using a weighted average of the membership grades. Suppose, there exists a fuzzy set within a discrete universe, and μ (xi) is its membership value in the membership function. the following expression can be used to represent the weighted average of the elements in the support set :

$$u = \frac{\sum_i \mu(x_i)\, x_i}{\sum_i \mu\,(x_i)} \quad (2.1)$$

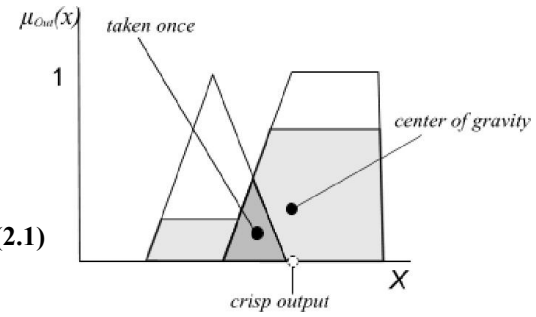


Figure II-11:Centre of Gravity (CoG) Method

II.3.4.2 Mean of Maximum (MoM) Method

This is the algorithm that we use in the experiment. The output is easily calculated by locating the "highest points" of the resulting output fuzzy set and finding their "middle point".

$$B = f(A) = \sum_i \frac{\mu_A(x_i)}{f(x_i)}$$

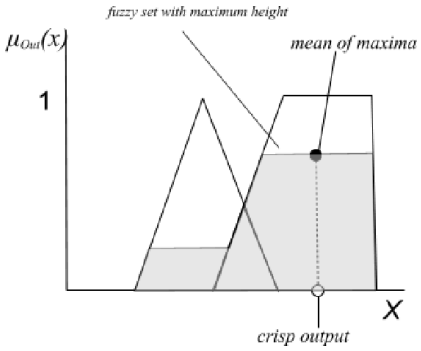


Figure II-12:Mean of Maximum (MoM) Method

II.3.4.3 Weighted average method

Among the various defuzzification methods the weighted average method is the most frequently used since it is one of the more computationally efficient method. But the main drawback of this method is restricted to symmetrical output membership functions. It is given by the algebraic expression

$$x^* = \frac{\sum_{i=1}^{n} w_i . x_i^*}{\sum_{i=1}^{n} w_i} \qquad \textbf{(2.2)}$$

Where

∑represents the algebraic sum and

wi :Represents the factor of appertenance of the conditions in the rule Ri.

xi: The center of gravity of the fuzzy subset of the output variable associated with the rule Ri

The weighted average method can be shown graphically as in Figure

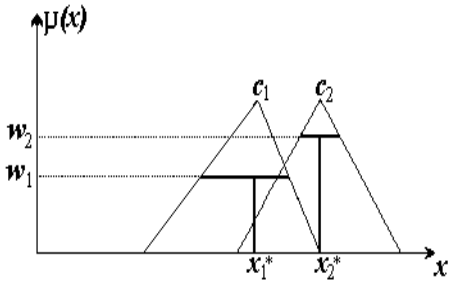


Figure II-13 :weighted average method

The weighted average method is formed by weighting each membership function in the output by its respective maximum membership value. In the proposed Fuzzy Logic based controller, weighted average method is used to defuzzify the output variables.

II.4 Conclusion

Fuzzy systems are obviously better than linear systems from when they generate results that are close enough to human reasoning, subject to have previously defined well the three parts that structure operate, namely: the modeling of input data in linguistic variables by means of functions the definition of a list of rules of inferences which represent the knowledge of the system and finally, the choice of the logical operator used and the typeof defuzzification chosen.

Chapter III

Fuzzy feature extractor

Chapter III : Fuzzy feature extractor

III.1 Introduction

In biometric systems, several methods are used to establish the feature extractor.fuzzy logic method has been used for last decades in the control systems. It is a new approach to use fuzzy logic to make a feature extractorofour biometric system; it's called fuzzy feature extractor. In this case, the treated image considered as a matrix is entered to the fuzzy extractor to be transformed to a less dimension vector guarding the distinguishing characteristics of the image. The following figure represents this idea.

Figure III-1: fuzzy feature extractor

III.2 Digital Image Form

A digital image i[c,r] described in a 2D discrete space is derived from an analog image i(x,y) in a 2D continuous space through a sampling process that is frequently referred to as digitization. For now we will look at the form of digital image.

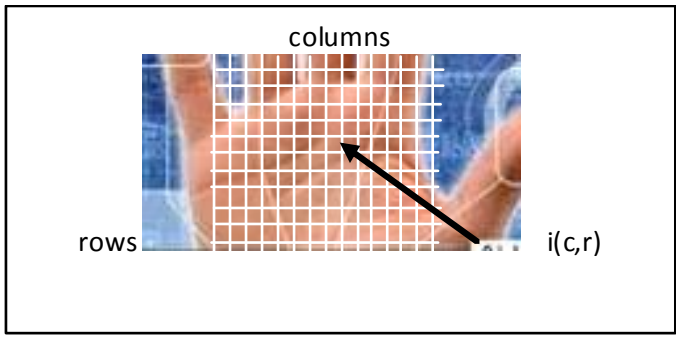


Figure III-2: Digitization of a continuous image

The effect of digitization is shown in Figure 1. The 2D continuous image i(x,y) is divided into R rows and C columns. The intersection of a row and a column is termed a

pixel.The value assigned to the integer coordinates [c, r] with {c=0,1,2,…,C–1} and {r=0,1,2,…,R–1} is

The pixel at coordinates [c=10, r=3] has the integer brightness value 110.

The image shown in Fig III-1 has been divided into N = 16 rows and M = 16 columns. The value assigned to every pixel is the average brightness in the pixel rounded to the nearest integer value. The process of representing the amplitude of the 2D signal at a given coordinate as an integer value with L different gray levels is usually referred to as amplitude quantization or simply quantization.

The used data base in our work is a collection of palm print images considered as 2D matrix where N =128, M=128 and i[m, n] takes values between 0 and 255; 0 is totally black color and 255 is totally white color; values between 0 and 255 take colors between black and white.[8]

III.3 Image Fuzzy model

III.3.1 Fuzzy sets of coordinates c and r

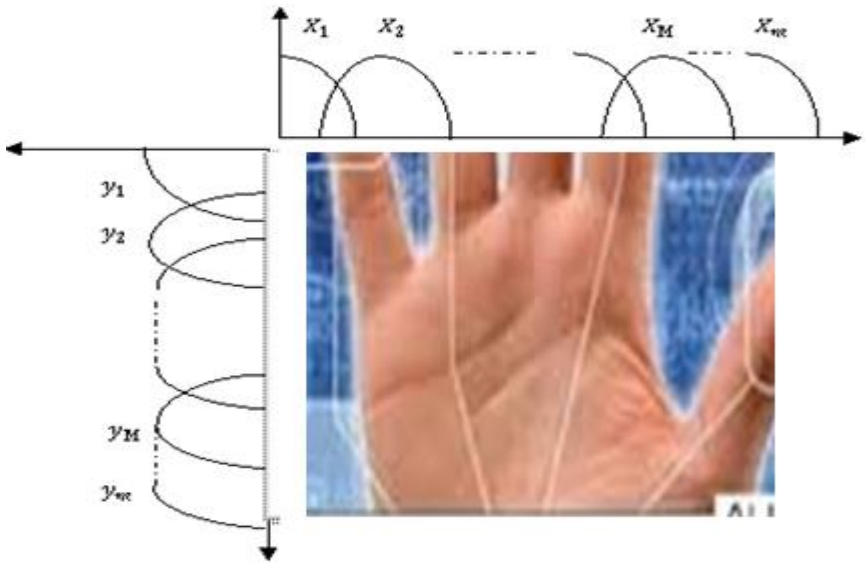


Figure III-3: Fuzzification of coordinates

We fuzzy the image by dividing the X-axes to M Fuzzy sets from X_1 to X_M and dividing the Y-axes to N fuzzy set from Y_1 to Y_N. In a special case M=N.

III.3.2 Fuzzy sets of gray level i

The gray level i(c, r) of the image takes values from 0 to 255 can be fuzzified as follows

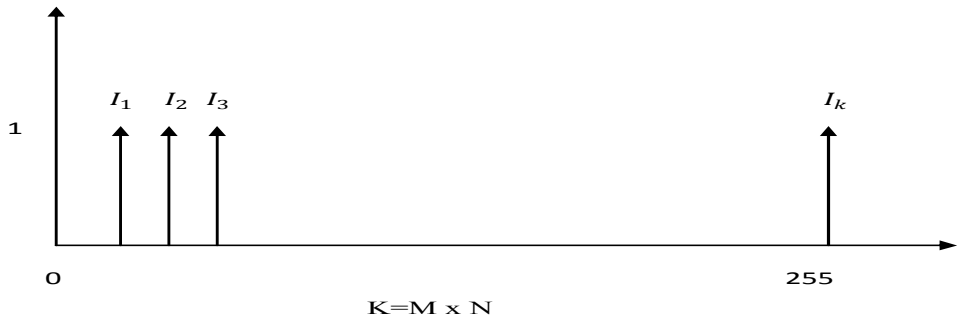


Figure III-4: Fuzzyfication of rule outputs

III.3.3 Inference engine

Depending of the above fuzzification, we build a fuzzy inference engine of MxN rules as follows:

R_k : IF c is X_m AND r is Y_n THEN i is I_k

Example:

For M=N=5

$\boldsymbol{R_1}$: If cis X_1AND r isY_1THEN i isI_1

$\boldsymbol{R_2}$: If cisX_1AND r is Y_2 THEN i is I_2

$\boldsymbol{R_3}$: If cisX_1AND r is Y_3 THEN i is I_3

……..

……..

$\boldsymbol{R_6}$: If c is X_2AND r is Y_1 THEN i is I_6

……..

……..

……..

$\boldsymbol{R_{25}}$: If cXisX_5AND r is Y_5 THEN I is I_{25}

III.3.4 Defuzzification method

By interring two coordinates c and r to our fuzzy model, they will be fuzzified on all fuzzy set of the k-rules. The result of each rule is the value w_k. using the weighted average method, the gray level corresponds to the coordinate's c and r is given by the flowed equation:

$$i=\frac{\sum w_k I_k}{\sum w_k}$$

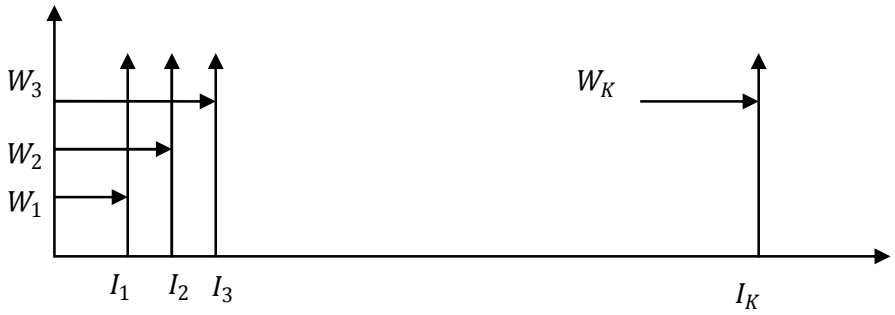


Figure III-5: deduzzifiction

III.3.5 Resume

As a result of the above work, we transform each image to a fuzzy model as follows:

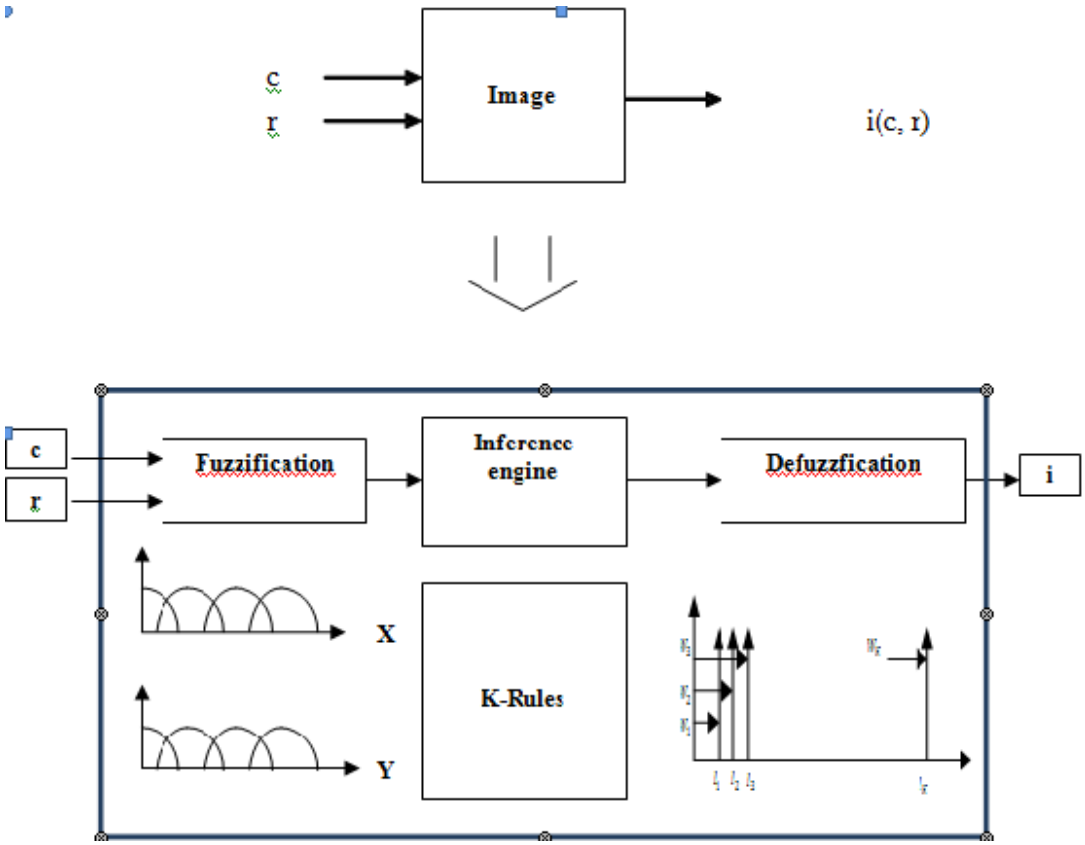
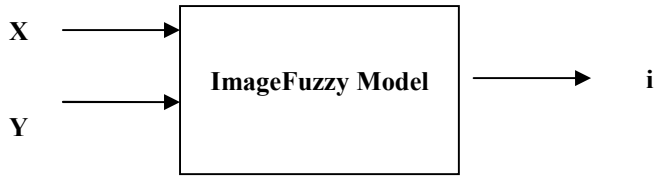


Figure III-6: Image Fuzzy Model

III.4 Fuzzy Model learning



The image fuzzy model is not necessarily similar to the image. in this case a learning method is required to adjust the image fuzzy model by estimating its parameters.

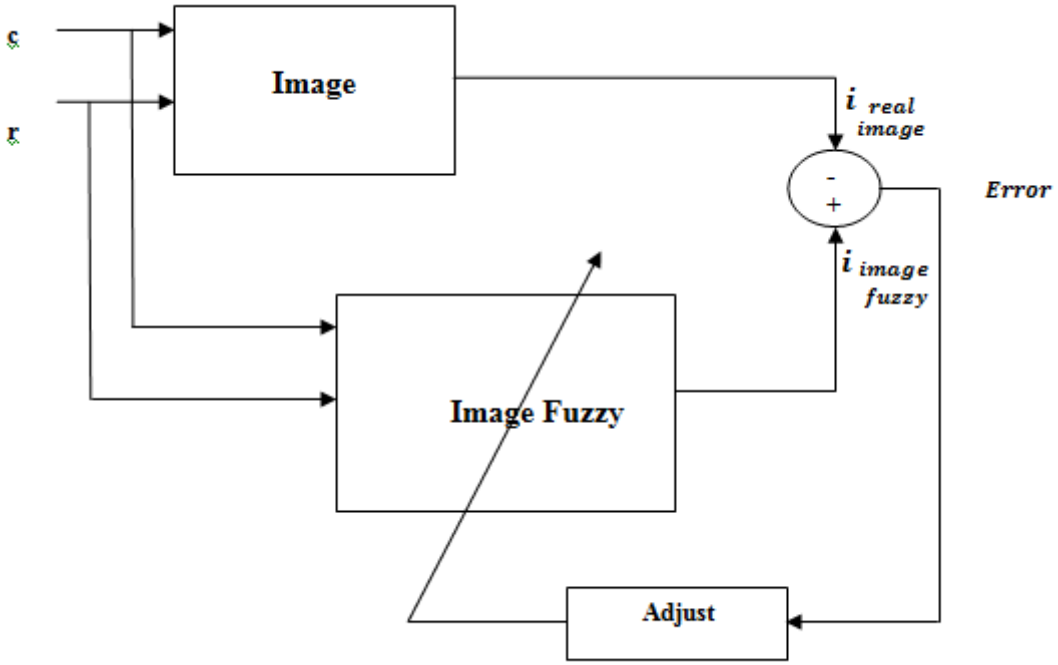


Figure III-7: Fuzzy Model learning

e (c, r): $i_{\text{real image}} - i_{\text{image fuzzy model}}$

III.4.1 Learning Algorithm

The problem of estimating the parameters consists in minimizing the criterion V.

$$V(t) = (E(t))^2 \quad (3.1)$$

E(t): The learning error metric.

The estimate of V is:

$$= \frac{1}{2}\left[i_{\text{real image}} - i_{\text{image fuzzy model}} \right]^T \left[i_{\text{real image}} - i_{\text{image fuzzy model}} \right]$$

The minimization of criterion V can be obtained by the resolution of:

$$-\nabla_z V = \left[-\frac{\partial \nabla}{\partial z_1}, \ldots, -\frac{\partial \nabla}{\partial z_k} \right] = 0, \quad \textbf{(3.2)}$$

Or $-\nabla_z V$ is the notion of the *gradient* of V.

P is the number of parameters to be adapted.

Robin and Monro [1951] proposed the following formula to solve equation (3.9):

$$z_k(t+1) = z_k(t) - \Gamma_k \nabla_z V\left[z_k(t)\right], \quad \textbf{(3.3)}$$

Γ : (*learning rate).*

III.4.2 Adaptation des paramètres :

The image fuzzy model has three types of parameters to adapt:

- The centers of c and r fuzzy sets,
- The widths…..
- consequences values $I = (I_1, \ldots I_{nk}, I_K)^T$,

Then:

$$\vec{Z} = (I_1, \ldots I_n, \ldots, I_K)^T.$$

Le nombre de paramètres à adapter est Le vecteur qui minimise le critère est donnée par :

The number of parameters to be adapted is P=K. The vector that minimizes the criterion is given by:

$$\left(\frac{-\partial V}{\partial I_1}, \ldots, \frac{-\partial V}{\partial I_k} \right) = 0. \quad \textbf{(3.4)}$$

Recursive adjustment of rules:

$$I_k(t+1) = c_k(t) - \Gamma \frac{\partial V(Z)}{\partial I_k}. \quad \textbf{(3.5)}$$

Si les fonctions d'appartenance du contrôleur sont gaussiennes, donc les dérivées partielles du critère V sont :

$$\frac{\partial V}{\partial I_k} = \left(i_{\text{real image}} - i_{\text{image fuzzy model}} \right) \frac{w_k}{\sum_{n=1}^{k} w_k}$$

Then: **(3.6)**

$$I_k(t+1) = I_k(t) - \Gamma_c \frac{w_k}{\sum_{n=1}^{k} w_k} \left(i_{\text{real image}} - i_{\text{image fuzzy model}} \right).$$

(3.7)

III.4.3 Iterative procedure:

The iterative procedure of parameter adaptation and minimization of the criterion is summarized as follows:

- **Step 1**: Initialize the parameters,

  - The consequence values I_k are random numbers.
  - Choice of parameters Anm and Bnm.

- **Step 2**: : Vector input c= $(c_1, c_2, \ldots, cn)T$.
- **Step 3**: Input of the desired output vector $i = (i_{\text{real image1}}, i_{\text{real image2}}, \ldots, i_{\text{real imagek}})T$.
- **Step 4**: Calculating the output vector of the controller

  $i = (i_{\text{image fuzzy model1}}, i_{\text{image fuzzy mode2}}, \ldots, i_{\text{image fuzzy model.k}}\ k)T$.
- **Step 5**: Adaptation of parameters I_{nk}.
- **Step 6** : Evaluation of criterion V.
- **Step 7** : Repeat steps 2 through 7 until V is less than a predefined value.

Chapter IV

Experimental results

Chapter IV Experimental results

IV.1 System biometrics

Every biometric system is composed of two phases, the first called enrollment and the second called recognition; these two phases require a main step called feature extractor

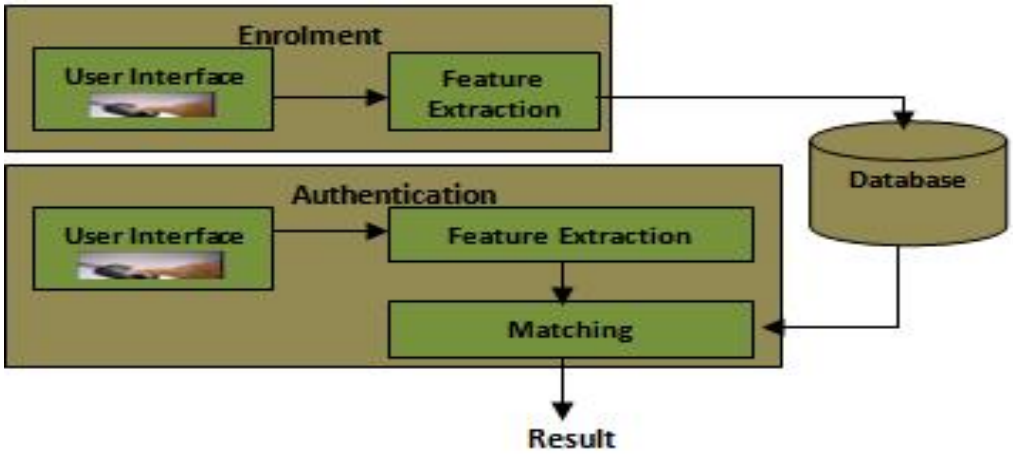


Figure IV-1:Architecture of biometrics system

IV.2 Feature extractor

Feature extraction is a type of dimensionality reduction that efficiently represents interesting parts of an image as a compact feature vector. This approach is useful when image sizes are large and a reduced feature representation is required to quickly complete tasks such as image matching and retrieval.

In our work we inserted the fuzzy logic in the extraction step to reduce the size of the image of 128x128 by a vector of 25 elements.

Extraction by fuzzy logic:

We are going to go through the next steps, like what we mentioned in chapter 2

- *1 step fuzzification*
- *2 step inference of enrage*
- *3 stepdefuzification*

IV.3 Data base

In the thesis, we use a database of 500 persons identified where each person has 12 images of which 3 used in enrollment and 9 in test.

- **Learning image**

The first, fifth and ninth images of each person serve for phase Learning.

- **Test image**

The remaining 9 images of each individual were used for the realization of the different Tests.

IV.3.1 Used Image

In this work we will use an image of palm print type

IV.3.1.1 Definition of palm print

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, as shown in Figure III.1. 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 its skin such as the lines (main and wrinkles), dots, minuteness and texture

Figure IV-2: The palm of the hand

A palmar identification can be seen as the ability to identify one person among others in a unique way through an appropriate algorithm exploiting the Characteristics of the palmar footprint.

IV.3.1.2 Advantages of the palm print

- Palmar impressions contain more information than fingerprints
- They are more discriminating

- The sources of the fingerprinting sensor are much cheaper than those of iris capture.
- The palm prints contain additional distinctive features such as lines and fine lines.
- By combining all the characteristics of a palm, it is possible to establish a robust system of biometrics.

IV.4 The physical environment

To develop this application I used a machine, configured as follows::

- Toshiba notebook
  - Memory(RAM): 8;00 GO
  - Hard disk:
  - Processor: Intel (R) Core (TM) I 5-5200 CPU @ 2.20 GHz.

IV.5 Environnement Logiciel

Millions of engineers and scientists worldwide use MATLAB® to analyze and design the systems and products transforming our world. MATLAB is in automobile active safety systems, interplanetary spacecraft, and health monitoring devices, smart power grids, and LTE cellular networks. It is used for machine learning, signal processing, image processing, computer vision, communications, computational finance, control design, robotics, and much more.

IV.6 System evaluation:

To study the performance of our system knowing that each step requires a dedicated approach that already desires to make the first chapter

IV.6.1 The curve FAR vs. FRR:

This curve, sometimes called the FAR vs. FRR curve, is the most often used by researchers trying to understand the performance of their recognition system. It shows the evolution of both error rates (FAR and FRR) at all thresholds (Fig.IV-3)

The EER value will pinpoint the score at which the threshold is optimal, in the sense of the best trade-off between the FAR and FRR.

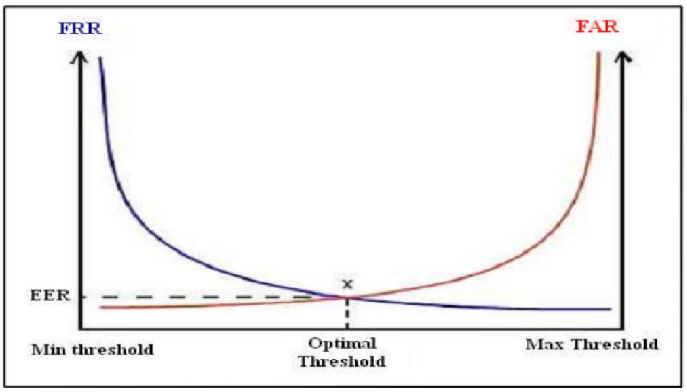


Figure IV-3:the curve FAR vs. FRR

Minimizing the area under the Crossover of the two plots is generally the goal of the researcher. The user of an authentication system uses this curve to calculate where to set their operating threshold. The graph will show the expected FAR and FRR at any chosen threshold.

We will follow the following values (EER and Optimal Threshold)

IV.6.2 The CMC curve

The Cumulative Match Curve (CMC) is used as a mea- sure of 1: m identification system performance. It judges the ranking capabilities of an identification system.

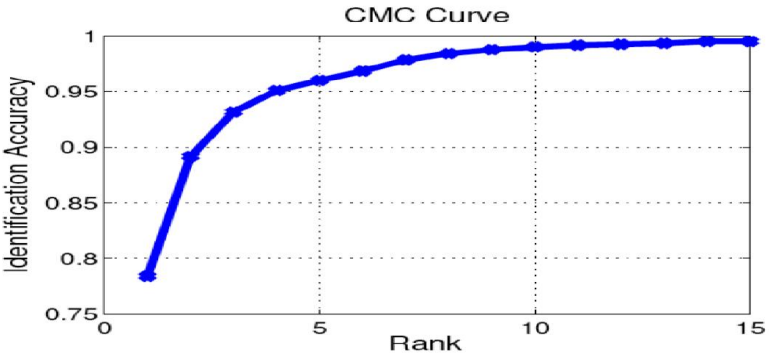


Figure IV-4: the CMC curve

We will follow the following values (ROR and RPR)

IV.7 Experimental Evaluation

Adaption parameter

In this system, we apply the image fuzzy model method, this method of learning, which is applied in the enrollment phase, is recognition phase.

We will use three parameter two fix

a :The horizontal and vertical centers;

b: The horizontal and vertical widths

For third parameter (Tc: The center of output): we will do a tuning

Therefore, we make an empirical method for the application of different values of Tc on our system and we take the following results:

IV.8 Result

The following table shows the results of EER For the band NIR to different Tc

Band NIR				
Tc	***ERR***	***TSH***	***ROR***	***RPR***
0.01	0.0667	0.1315	99.33	50
0.05	0.1551	0.113	98	85
0.1	0.1811	0.1041	98	80
0.5	0.5051	0.1132	96	130

Tableau IV-1: EER For the band NIR to different Tc

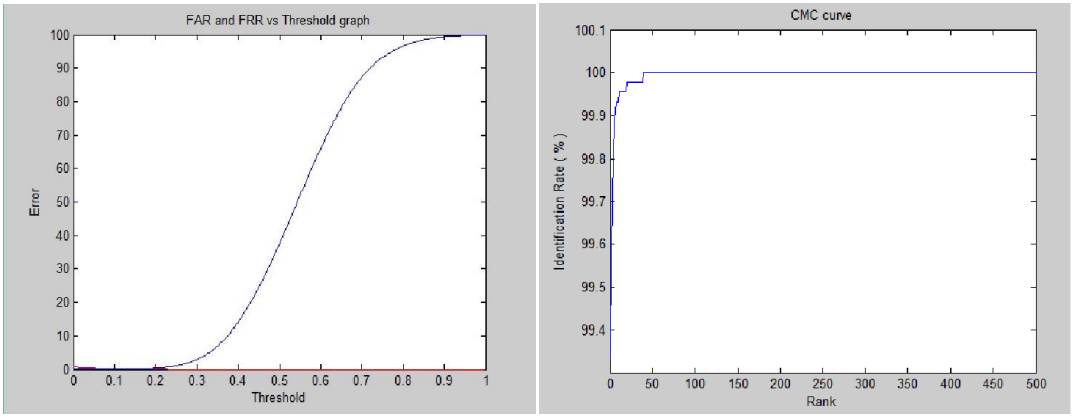


Figure IV-5 band Nir (ERR,CMC curve) TC:0.01

The following table shows the results of EER For the band RED to different Tc

Band RED				
Tc	***ERR***	***TSH***	***ROR***	***RPR***
0.01	0..1334	0.1318	99	50
0.05	0.2911	0.114	98	60
0.1	0.4267	0.117	97	71
0.5	0.6919	0.114	95	80

Tableau IV-2: EER For the band RED to different Tc

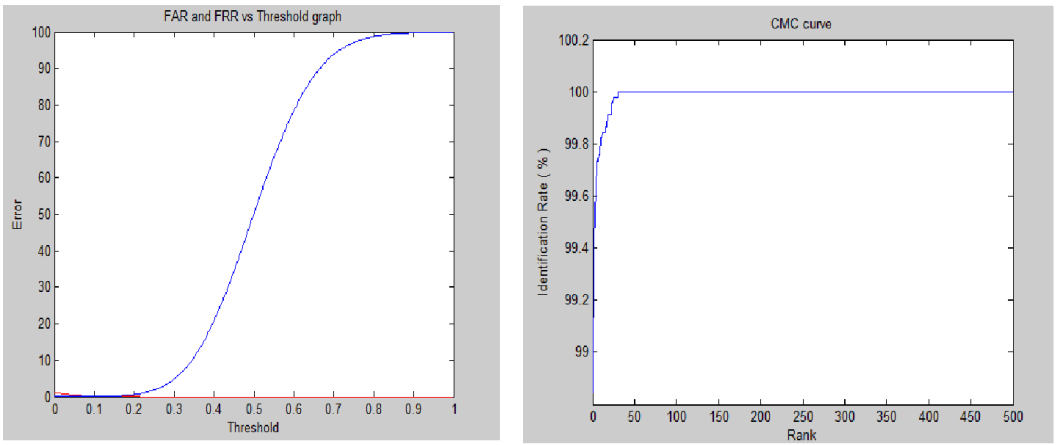


Figure IV-6: band Red (ERR,CMC curve) TC:0.01

The following table shows the results of EER For the band Blue to different Tc

Band Blue				
Tc	***ERR***	***TSH***	***ROR***	***RPR***
0.01	0.1335	0.1306	98.33	90
0.05	0.288	0.123	97	100
0.1	0.497	0.129	96	110
0.5	1.312	0.129	92	120

Tableau 3 EER For the band Blue to different Tc

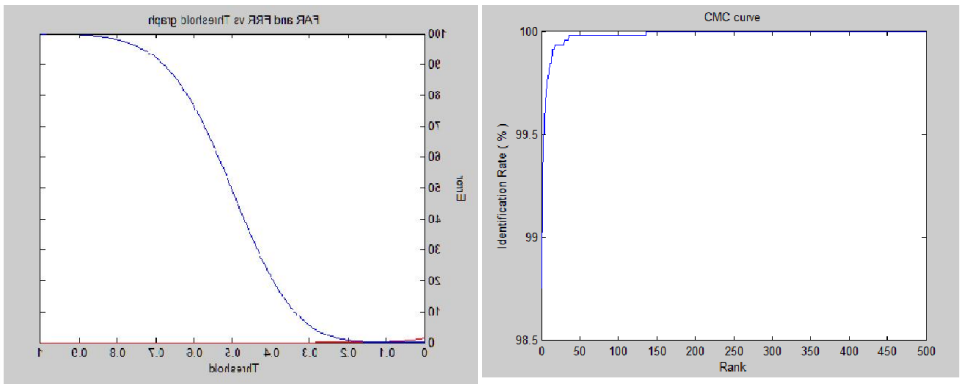


Figure IV-7: band Blue (ERR,CMC curve) TC:0.01

The following table shows the results of EER For the band Green to different Tc

Band Green				
Tc	***ERR***	***TSH***	***ROR***	***RPR***
0.01	0.2358	0.147	98	50
0.05	0.5331	0.135	96	60
0.1	0.687	0.1291	93	80
0.5	1.381	0.1191	86	80

Tableau IV-4: EER For the band Green to different Tc

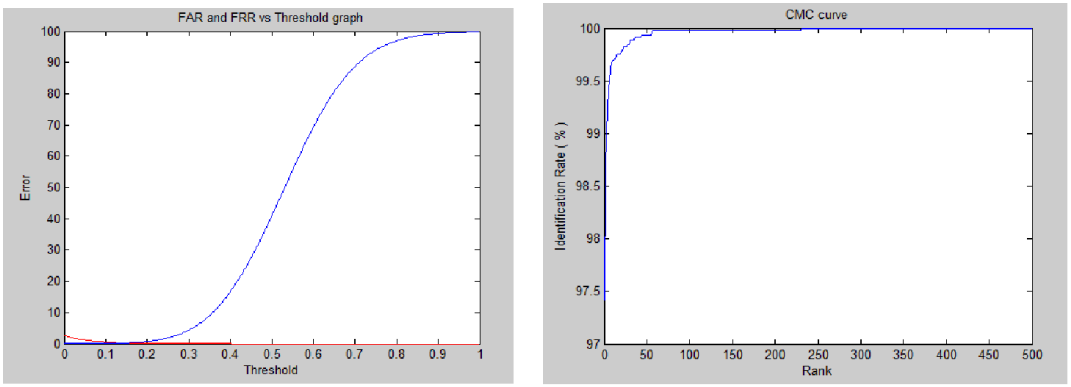


Figure IV-8:band Green (ERR,CMC curve) TC:0.01

IV.9 Discussion

In this work done, we have to change the Tc value on four different bands (NIR; Red; Blue; Green). The given system gives a result different from each band for the value four of parameter Tc.we concluded that the band NIR gives less value to the error, and that the value Tc=0.01 is better among the other Tc

IV.10 Conclusion

The results obtained justify the effectiveness of our biometric system based on a related fuzzy model. An image of dimension 128x128 is modeled at the end by a feature vector of 25-dimension only. The calculation time is acceptable and the results are good.

General conclusion

General Conclusion

The aim of this work is to study one of the most recent biometric systems for the identification of the palm recognition individual using a recursive learning fuzzy logic feature extractor. This biometric technology is considered to be very powerful in terms of safety, of its biometric characteristics that are unique to the individual, with almost no possibility that other individuals may have the same characteristics, even in the case of identical twins.

In order to design our palm recognition system, first, we have given an overview of some biometric systems that exist in the literature and their use as systems for the recognition of the individual in general, in particular palm biometry.

We have worked on the application of fuzzy logic in the biometric system to establish a robust feature extractor in order by the use of recursive learning approach on reading the properties of the image.

We have noticed through the results and after several applications and selection of parameters such as membership functions centers, widths and number, gain of recursive equation and so on, that the establish biometric system achieve satisfactory demands.

In the last part, we have the use of palm technique to extract the benefit of the person has achieved us very satisfactory results have seen a good reputation in this field.

References

References

[1] Hafnaoi Imane "Multimodalal Biometric fusion using Evalutionary Technique", Universitie M'hamed Bougaraa Boumerdes , Memoire de Magister 2013/2014

[2] Mohammed Demri " Multimodalal Biometric fusion using Evalutionary Technique " Universitie Aboubakr Bellaid , Memoire de Magister June 2012

[3] Boulgouris , Plataniotis , and Micheli-Tzanakou "Biometrics Theory Methods ,and Applications" the Institute of Electrical and Electronics Engineers , Inc. , Copyright © 2010

[4] "Multimodalal Biometric fusion using Evalutionary Technique" 2012

[5] James Wayman, Anil Jain, Davide Maltion and Dario Maiom(EDS), "Biometric Systems Disgn and prerform ance Evaluation ", ISBN 185233596, Spinger – varlag london limited 2005

[6] Samir Nanavti Michael Thieme Raj Nanavati, "Biometrics Identification in a Net worked Wordl " Capyright © 2002

[7] Ani K. Jain, Arun AROSS and Kathndnda Kumar, "Introduction to Biomtrics Foreword by James Wayman"

[8] Arun A Ross, Karthik Nandakun, Ani, , "Handbook of Maltibiometrics", East Lamsing, MI 48824-1226 Kluwer Academic Publishers Newyork, Boston, Dordrecht, london, Moscow USA © 2002

[9] David Zhang Anil K.Jain (Eds.) "Advances in Biometrics " Introductional Confernational (LNCS 3832) , ICB , 2006

[10] Jacob Scharcans Ki hogo Proenca Eliza Du Elitons "signal and imag proessing for biometrics "

[11] "Fuzzy logic concepts, Theories and Application" ISBN 978-953-51-0396-7 Hard cover

[12] "Models for Inexact Reasoning Fuzzy logic" –lesson 1 Crisp and Fuzzy Sets, Master in Computational logic

[13] Nikolaosu. Boulg Ouris Konstantinos. Plataniotis. Evangelia Micheli Tzanakou Editors "Biometrics Theory , Methods , and Application " by the Institute of Electrcal and Electonices Engineers , Inc. Copyright © 2010

[14] Julian. Ashbourn, " Biometrics in the New World, DOI 10.1007/978-3-319-04159-92 © Springer International Publishing Switzerland 2010.