ENHANCING CLASSIFICATION STRUCTURES FOR BIOMETRICS APPLICATIONS

A THESIS SUBMITTED TO
THE UNIVERSITY OF KENT AT CANTERBURY
IN THE SUBJECT OF ELECTRONIC ENGINEERING
FOR THE DEGREE
OF DOCTOR OF PHILOSOPHY (PHD).

By
Márcy Cristiany Da Costa Abreu
November 2010
To my husband Carlos Eduardo Da Silva who is always there for me!
Acknowledgements

First and foremost, thanks be to God (and all his saints, that I am never tired of asking for support!), the merciful and the passionate, for giving me strength and perseverance in always carry on even before the difficulties and for all my blessings, for providing me the opportunity to step in the excellent world of science.

To be able to step strong and smooth in this way, I have also been supported and supervised by many people to whom I would like to express my deepest gratitude.

To my husband (Carlos Eduardo Da Silva) who joined me in this adventure of pursuing a Ph.D. He is the one who dried my tears when I was crying (feeling homesick), who warmed my feet in the very cold nights of winter and who celebrated with me my achievements.

A special word of forever gratitude to my mother (Maria Aparecida Costa Abreu) and my father (Francisco das Chagas Abreu) who always gave me total and full support in all my (personal and academic) decisions. They always inspired me to work hard and to be positive at all times.

A very special thanks to Professor Michael C. Fairhurst who is like a father and a dear friend to me. Since the beginning, he helped with my adaptation in this country and was always there for me when I needed. I can truly say that I have had the best supervisor that someone could ask and have learnt not only how to be a good researcher but to be a good person as well.

I must not forget to thank Doctor Anne Magaly de Paula Canuto who is the main responsible for me to be here. She was my first research supervisor and helped me in the early stages of my career.

Many thanks to all the Brazilian friends (from Dr. Rogério De Lemos who kindly opened his house for us, though Erick Lopes who taught Carlos how to cook, and Dr. Fernando Otero who saved us from house hunting in our last year!) who were close by (in Canterbury or in Europe) during the time of my Ph.D. and made my adaptation process easier and the one-week-holidays so great.

I can not forget to thank all my friend and colleagues of the Department of Electronics of the University of Kent who made my day-to-day life so enjoyable and therefore made the journey of getting the Ph.D. less heavy. A special thanks to Dr. James Weston, Dr. Karl Hammer, Dr. Yiqing Liang, Tasmina Islam, Meryem Erbilek, Paul Taylor and Jonh Baptist.

To my brother and sister, and to my in-laws, who all showed belief in me when times were difficult. And to all my dearest friends who are in Brasil but always
have shown interest and love for me even when I was so far away. They always reminded me where I came from.

And finally, I am very grateful to the financial support given from CAPES (Brazilian Funding Agency under grant BEX4903-06-4). Without them, I would never be able to have completed this Ph.D.
Abstract

The effectiveness with which individual identity can be predicted in different scenarios can benefit from seeking a broad base of identity evidence. Many approaches to the implementation of biometric-based identification systems are possible, and different configurations are likely to generate significantly different operational characteristics. The choice of implementational structure is therefore very dependent on the performance criteria which are most important in any particular task scenario. The issue of improving performance can be addressed in a number of ways, but system configurations based on integrating different information sources are a widely adopted means of achieving this. In this thesis, we will evaluate the merits of using very different classification structures, and we will investigate how fundamentally different strategies for implementation can increase the degree of choice available in achieving particular performance criteria. In particular, we propose that the design process could be carried out using three different approaches: multicategory, multiclassifier and multimodal. In the multimodal approach, we will show a new way to improve identification performance, where both direct biometric samples and "soft-biometric" knowledge are combined. In the multiclassifier approach, we will illustrate the merits of an implementation based on a multiagent computational architecture. And finally, in the multimodal approach, we will investigate the benefits of correctly choosing the modalities for a multimodal system using handwritten signature as a case study, more specifically presenting some qualitative analysis as support. The contributions presented in this work are very encouraging and point to new and more flexible paradigms for designing systems based on biometrics.
Contents

List of Tables xiii
List of Figures xvi
List of Publications xvii

1 Challenges in biometrics system design 1
  1.1 Introduction ............................................. 2
  1.2 Research problem and motivation ...................... 4
  1.3 Different approaches: state of the art ............... 7
    1.3.1 Multicategory approach ......................... 8
    1.3.2 Multiclassifier approach ....................... 9
    1.3.3 Multimodal approach .......................... 10
  1.4 Contribution ........................................... 12
  1.5 Chapter conclusions and thesis organisation .......... 13

2 Experimental methodology 15
  2.1 Introduction ........................................... 16
  2.2 Basic system architecture ........................... 16
  2.3 Background ............................................ 18
  2.4 Classifiers ............................................ 19
  2.5 Database .............................................. 21
    2.5.1 Fingerprint Database ........................... 22
    2.5.2 Signature ......................................... 23
    2.5.3 Hand Geometry .................................... 25
    2.5.4 Non-Biometric Information ...................... 26
    2.5.5 Database issues .................................. 26
  2.6 Chapter conclusions .................................. 27

3 Multicategory approach 29
  3.1 Introduction .......................................... 30
  3.2 Review of soft-biometrics data categories .......... 32
  3.3 System design using soft-biometrics categories .... 33
    3.3.1 Categorisation of the soft-biometrics ........ 34
  3.4 Using soft biometric given by the user .......... 36
6.3.2 Further research in multiclassifier approach . . . . . . . . . 117
6.3.3 Further research in multimodal approach . . . . . . . . . . 117
6.4 Chapter conclusions . . . . . . . . . . . . . . . . . . . . . . . . . 118

Bibliography . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>MLP results for different fingerprint training and testing sets</td>
<td>27</td>
</tr>
<tr>
<td>3.2</td>
<td>Literature results when incorporating soft-biometric information</td>
<td>33</td>
</tr>
<tr>
<td>3.3</td>
<td>Error rates and standard deviations for the Unimodal MCS</td>
<td>54</td>
</tr>
<tr>
<td>3.4</td>
<td>$p$ – values when comparing the lowest error rate with the others in each database</td>
<td>56</td>
</tr>
<tr>
<td>3.5</td>
<td>$p$ – values when comparing the lowest error rate among databases</td>
<td>56</td>
</tr>
<tr>
<td>3.6</td>
<td>Literature results when using multiclassifier systems</td>
<td>64</td>
</tr>
<tr>
<td>3.7</td>
<td>The confidence of the two agents</td>
<td>70</td>
</tr>
<tr>
<td>3.8</td>
<td>The payoff matrix for this example</td>
<td>71</td>
</tr>
<tr>
<td>3.9</td>
<td>The cost values for Auction method</td>
<td>72</td>
</tr>
<tr>
<td>3.10</td>
<td>The sensitivity analysis of the identity prediction classifiers</td>
<td>75</td>
</tr>
<tr>
<td>3.11</td>
<td>The training mean of all features according to the enrolled users</td>
<td>75</td>
</tr>
<tr>
<td>3.12</td>
<td>The absolute distance of the test pattern and its training mean for the users</td>
<td>75</td>
</tr>
<tr>
<td>3.13</td>
<td>The sensitivity analysis of the soft-biometric prediction classifiers</td>
<td>78</td>
</tr>
<tr>
<td>3.14</td>
<td>The training mean of all features according to the soft-biometric classes</td>
<td>78</td>
</tr>
<tr>
<td>3.15</td>
<td>The absolute distance of the test pattern and its training mean</td>
<td>78</td>
</tr>
<tr>
<td>3.16</td>
<td>Error rates and standard deviations for the Unimodal MAS</td>
<td>83</td>
</tr>
<tr>
<td>3.17</td>
<td>$p$ – values when comparing the lowest error rate with the other ones in each database</td>
<td>83</td>
</tr>
<tr>
<td>3.18</td>
<td>$p$ – values when comparing the lowest error rate among databases</td>
<td>84</td>
</tr>
<tr>
<td>5.19</td>
<td>Error rates and standard deviations for the Multimodal MCS</td>
<td>107</td>
</tr>
<tr>
<td>5.20</td>
<td>$p$ – values when comparing the lowest error rate for the multiclassifier with the other ones in each databases combinations</td>
<td>109</td>
</tr>
<tr>
<td>5.21</td>
<td>Error rates and standard deviations for the Multimodal MAS</td>
<td>109</td>
</tr>
<tr>
<td>5.22</td>
<td>$p$ – values when comparing the lowest error rate for the multiagent with the other ones in each databases combinations</td>
<td>109</td>
</tr>
</tbody>
</table>
List of Figures

1.1 Various approaches of the problem ........................................... 5
2.2 General look of the biometric-based system ............................. 17
2.3 Optical fingerprint ................................................................... 22
2.4 Thermal fingerprint ................................................................. 22
2.5 Sample of a signature of the BioSecure database ..................... 23
2.6 Sample of a left-hand of the BioSecure database ..................... 25
3.7 Various approaches to the problem: Focusing on the multiclass category approach ........................................... 31
3.8 Fuzzyfication of subject age .................................................... 34
3.9 Soft-biometric as input features .............................................. 37
3.10 Soft-biometric as feature selector .......................................... 39
3.11 System when using soft-biometric prediction approach .......... 43
3.12 System when using soft-biometric prediction approach in the Input Data Processing module ................................. 44
3.13 System when using soft-biometric prediction approach .......... 46
3.14 Results for the individual classifiers using the signature database 50
3.15 Results for the individual classifiers using the hand geometry database 51
3.16 Results for the individual classifiers using the fingerprint database 52
3.17 Results for soft-biometric prediction using all databases .......... 53
3.18 Results for the unimodal multiclassifier systems .................... 55
4.19 Parallel approach .................................................................. 60
4.20 Modular approach .................................................................. 60
4.21 Various approaches to the problem: Focusing on the multiclassifier approach ........................................... 61
4.22 System design when using the multiagent approach .............. 63
4.23 Architecture of the agent ....................................................... 66
4.24 Multiagent-based system workflow ....................................... 67
4.25 Results for the unimodal multiagent systems ...................... 82
5.26 Various approaches to the problem: Focusing on the multimodal approach ........................................... 89
5.27 Individual classifiers error rates broken down into age bands .... 105
5.28 Results for the multimodal multiclassifier systems .............. 106
5.29 Results for the unimodal and multimodal for both multiclassifier and multiagent systems .......................... 108
5.30 Results for the unimodal and multimodal for both multiclassifier and multiagent systems
List of Publications

Journal papers:


Conference papers:


Chapter 1

Challenges in biometrics system design

This chapter will present the fundamental basis for the investigations which are to be reported and analysed in this thesis. The proposed division of approaches for biometric-based system design as well as an overall explanation of each approach and the general state of the art will be discussed.
1.1 Introduction

Security systems which need a high accuracy in identifying individuals, or in confirming their claimed identity, are becoming more important than ever in modern society. The search for new techniques that can improve the performance of an individual identification system is very important to protect identity, as opportunities for fraudulent claims and "identity theft" increase (Kittler and Maltoni, 2007). Identification process is, therefore, an essential part of these systems and biometric information has been widely used for this purpose, often with satisfactory performance, in criminal identification, employee control, access control, etc. (Fairhurst, 2003).

Biometrics (from bio life + metric measure) is the term used to describe the formal and rigorous study of the physiological and/or behavioural characteristics of the living people (Jain et al., 2004c). This term is nowadays most commonly used in connection with the formal study of the characteristics of human beings as a way to identify them. Each different type of source of a biometric measurement (e.g. facial appearance, the pattern of the fingerprint, vocal characteristics, etc.) is generally referred to as a biometric modality and the possible biometric modalities are usually divided into two broad categories: Physiological and Behavioural. The first category refers to any inherent characteristic of, or appropriate to, an individual. The second category refers to the actions or reactions of an individual, usually in relation to the environment (Ives et al., 2005).

Biometrics-based systems for individual identification can base their functioning on many different characteristics of the human body or human behaviour. Common examples include voice (Markowitz, 2000), iris (Daugman, 2000), hand geometry (Polat, 2008), fingerprint (Ross et al., 2005), signature (Jain et al., 2002), etc. The use of biometric information is not a new idea and it is possible to find many well developed devices which perform biometric-based classification/matching with an acceptable accuracy for many applications.

In order to develop a biometric-based system, four distinctive phases are necessary: designing (which is the main focusing of this thesis), enrolment, training and testing. The design phase is the definition of all the components of the system (based on the requirements of the system and of the users). The enrolment phase is the acquisition of representative samples from the individual which will be used in the training phase. The training phase is when the samples collected in the enrolment phase are presented to a classification algorithm in order to define a template for that individual. The template can be described as a group of important characteristics regarding one or many modalities which can be related to that user, therefore can identify him/her. And finally, the testing phase is when the whole system is ready to be used in a real-world scenario.

There are two, different but related, fundamental types of tasks where biometric information can readily be used, usually referred to as either verification or identification (Prabhakar et al., 2003). In verification, the system performs a one-to-one comparison. In this case, the question to be answered is: "is this person who he says he is?". On the other hand, an identification system performs
a one-to-many comparison. In this case, the question to be answered is: "who is this person?". The computational cost of the second task is clearly likely to be greater than the former, because many comparisons are necessary between the sample subject and the stored templates.

The challenge of building more accurate systems to perform verification and identification based on biometric data is growing very fast (Abreu and Fairhurst, 2008b). Among the many issues of concern to a system designer, one of the most crucial in an environment that requires high security is that of error rate, and especially the balance between false positive and false negative rates (Dass et al., 2006). In many important applications it is also important to offer flexible user options in cases where either the user is not able to give a required sample or where social or convenience factors preclude the use of a specific modality in practice. The most common solution in such circumstances is to create a more versatile biometric-based system which can allow the deployment of more than one modality (the multimodal approach), simultaneously offering the user the possibility of a degree of choice and decreasing the chances of the system delivering an incorrect identity prediction (Snelick et al., 2003).

There are two main reasons for this. The first one is that in the biometric field, it is possible to find a huge variety of modalities and there are many ways of using them either alone or combined. The other one is that these kind of systems are essential in the fight against crime, because they are based on what the user is or does and not on what the user has or remembers (compare with, for example, physical tokens such keys, swipe cards, or passwords which can be lost, forgotten or shared).

Despite the fact that biometrics have been used for a long time, there is still a lot of study to be done. The complexity of creating a system which executes biometric classification relies on a number of very important parameters (Abreu and Fairhurst, 2008b), such as the following:

- Using several modalities or focusing on specific and well-developed modalities (such as fingerprint and face).
- Using additional information (soft-biometrics).
- Acquisition of complete dataset or at least statistically significant ones.
- Exploration of multiagent technology.
- Developing more powerful sensors.
- Developing different and less dependent data capture techniques.

Optimising the processing of biometric identity data, whether within modalities or in multimodal form, is a fundamental challenge in system design and deployment. There are many potential options available in relation to the processing engines which might be adopted, and any selection must be made on the
basis both of application requirements and with regard to a knowledge of the de-
gree of match between the underlying population data distributions and system 
operating characteristics (Ives et al., 2005).

The choice of each parameter of the biometrics-based system will inevitably 
bear close relation with a particular set of application requirements. However, 
there is no agreement on which classification/matching method works better 
with any specific modality or which modality represents better a specific prob-
lem (Fairhurst, 2003).

The availability of multiple information sources for biometric data processing 
can suggest various different strategies by means of which to achieve enhanced 
performance. These include, for example, selecting an optimal processing tech-
nique from among many options (it is possible that multiclassifier systems produce 
better results than single classifiers), combining processors to create a multiple 
processor system to work on a unimodal source (they can combine the benefits of 
more than one source of information to find a result) and, ultimately, combining 
multiple biometric modalities to overcome the shortcomings of any one individual 
modality. In each case, however, there are obvious questions to be asked about the 
processing engines implemented, and the performance of which they are inherently 
capable (Jain et al., 2004c) and (Jain et al., 2005).

Nevertheless, biometric-based applications are well established and accepted 
as one of the best and most reliable ways of guaranteeing secure transactions. 
However, it is still not very clear what is the real difference or relationship among 
all these issues (Fairhurst and Abreu, 2009a). In order to improve performance 
without losing the flexibility necessary, several different approaches have been 
proposed but not fully defined and presented in one single work.

1.2 Research problem and motivation

The design of a biometric-based classification system is a particularly challeng-
ing pattern recognition task (Jain et al., 2005). The fundamental nature of this 
specific type of data as well as the application domain where it will be utilised 
makes it very particularly specialised (Poh and Bengio, 2006). Issues such as the 
following can especially lead to poor performance if not addressed appropriately:

- The need, as in many pattern recognition applications, for high levels of 
  accuracy (i.e. low error rates) (Jain et al., 2008),

- Providing choice and preference for users as well as the need to avoid exclu-
  sion of individuals not able to give reliable biometric samples in a particular 
  chosen modality (Alterman, 2003),

- The availability of resources (Faundez-Zanuy et al., 2006),

- Effective matching techniques (Tronci et al., 2009),

- Enrolment issues and sample size requirements (Dass et al., 2006),
1.2. RESEARCH PROBLEM AND MOTIVATION

- Data capture (Toh et al., 2004),
- Data quality (Alonso-Fernandez et al., 2006),
- Safety of the data (e.g. whether to store or not?) (Jain et al., 2008)
- and so on.

At the very least, it is generally necessary to include an appropriate strategy for exception handling in any significant biometric application scenario. Yet, the design of these systems normally focuses on one particular issue rather than analysing the problem as a whole. Exploiting a broader range of information about the task offers improved levels of accuracy, while also increasing the resilience of a system to, for example, spoofing attacks, or inclusiveness.

Conventionally, during the design process, it is possible to divide the development of a biometrics system into three distinct, though, not entirely independent approaches: multicategory approaches, multiclassifier approaches and multimodal approaches. Figure 1.1 shows a schematic representation of these three approaches and their relationship.

![Figure 1.1: Various approaches of the problem](image)

To be more precise, each of these approaches tries to tackle specific problems when designing biometric-based systems.
• Multiclassifier approach: In this case, maximum benefit is derived from using different structures but (usually) working with a single source of identity information. It uses different "classification" and/or fusion techniques to improve flexibility, security and accuracy of the system.

  – Advantages: More powerful structures will provide more flexible and accurate results.
  – Disadvantages: Optimising the error rate performance of a multiclassifier system is not always straightforward (Jain et al., 2008).

• Multimodal approach: On the other hand, this approach capitalises on the benefits of combining different modalities. Its main idea is take advantage of fundamentally different modalities in order to maximise the identification/verification accuracy.

  – Advantages: The availability of multiple modalities simultaneously offers flexibility to the user, since there is then, at least in principle, a choice available in a situation where a user either cannot or does not wish to give a sample in a particular modality (Fierrez-Aguilar et al., 2003b). Also, it potentially offers improved reliability because it uses a greater amount of information, and requires much more effort for successful attack.
  – Disadvantages: Choosing the modalities and system usability issues are the most frequently encountered difficulties (Toledano et al., 2006).

And, undoubtedly, a lot of research has concentrated on the overlap of the multiclassifier and multimodal approaches, developing multimodal fusion techniques mostly. Nevertheless, the often complex analysis required to choose an optimal modality (or many) for an application in the face of such conflicting demands has been a major factor, as has been trying to identify the best classification structures (Jain et al., 2006).
Indeed, all relevant issues must be considered, such as wasting important information (non-biometrics, very often) when this could influence the decision making of the identification process. Likewise, the use of several modalities is not always the best solution, and similar performance rates might be reached with unimodal systems when well balanced or more intelligent structures were used. Even the choice of the best modalities to compose a multimodal system might be unhelpfully influenced by issues about which are currently "in fashion" but which are not necessarily the best suited for the specific task.

The main aim of the work to be presented here is, broadly, to define more clearly what issues must be addressed in order to reach the best optimised biometric-based system. More specifically, the investigation reported will analyse and evaluate different proposed alternatives in order to maximise the chance of finding the best balance among performance, security and flexibility in biometric-based systems.

Section 1.3 will introduce the literature of relevance to each of the three approaches presented (in Sections 1.3.1, 1.3.2 and 1.3.3, respectively), although later chapters will review relevant material in a more detailed and focused way. Section 1.4 will address all the contributions proposed in this thesis in each of these three approaches and Section 1.5 will present the organisation of the thesis as well as the conclusions of the chapter.

1.3 Different approaches: state of the art

The practical deployment of biometric identification/verification systems presents a number of challenges, among which the need in many applications for high levels of accuracy (i.e. low error rates) is a primary concern, but by no means the only one. Issues relating to choice and preference among users, let alone the need to avoid exclusion of individuals not able to give reliable biometric samples in a particular chosen modality, are becoming increasingly important as adoption of biometric systems becomes more widespread (Jain et al., 2005). At the very least, it is generally now necessary to include an appropriate strategy for exception handling in any significant biometric application scenario.

The (by now) well established field of biometrics provides an extensive and diverse literature reporting studies on each of these three broad approaches described above. Discussion of various modalities, fusion techniques, sensor development, security issues, and usability problems, as well as the use of revocable biometrics and soft-biometrics can be found (Kittler and Maltoni, 2007). Nevertheless, determining the modality(ies) to be used, the classification method and the optimal configuration for the overall system is not an easy task. However, where successfully achieved, good results are reported.

Despite all the work that has been carried out using biometrics, it is still quite often very difficult to make strong claims about performance which can be statistically substantiated, largely because it can be difficult to find large enough
databases. Moreover, the experiments which are used to validate proposed techniques are normally executed in a very controlled environment which does not represent real-world scenarios, while the complexity of some techniques would probably cause usability concerns in practical situations.

Sections 1.3.1, 1.3.2 and 1.3.3 will review some of the main literature related to our identified approaches, namely the multicategory, multiclassifier and multimodal approaches, respectively.

1.3.1 Multicategory approach

The term *multicategory*, as already explained, refers to any biometric-based system which uses more than one category of information (always based on biometric information but also drawing upon other sources of identity evidence). The categories can be described often as relating to different types of soft-biometrics, such as gender, age, handedness, height, fat percentage, and so on. The research related with this approach can be divided into three distinct parts:

- Integration of additional information with hard biometrics in the identification process:
  - Iris and fingerprint fused with iris colour (Zewail et al., 2004),
  - Fingerprint fused with gender, ethnicity and height ((Jain et al., 2004d), (Jain et al., 2004a) and (Jain et al., 2004b)),
  - Fingerprint fused with body weight and body fat (Ailisto et al., 2006).

  In publications in this area, the soft-biometric information is generally used in order to decrease the search space, limiting the identity search to users who belong to that specific category.

- Estimation of the soft-biometric information:
  - Gender estimation from face ((Mäkinen and Raisamo, 2008) and (Matta et al., 2008))
  - Age estimation from face ((Takimoto et al., 2007), (Geng et al., 2007), (Lanitis et al., 2004), (Sun et al., 2005), (Guo et al., 2008b), (Guo et al., 2008a) and (Guo et al., 2008c))
  - Age and gender estimation from voice (Metze et al., 2007),
  - Gender and handedness estimation from handwritten signature (Liwicki et al., 2007),
  - Gender estimation from iris (Thomas et al., 2007),
  - Age estimation from voice ((Nishimoto et al., 2008) and (Ajmera, 2006)).
In this case, the biometric data is used to predict soft-biometric information rather than the identity of the user. It has a very important use in forensic applications.

- The implications for the biometric system of the age of the template:
  - Fingerprint ((Modi et al., 2007), (Theofanos et al., 2006), (Uludag et al., 2004) and (Fierrez-Aguilar et al., 2005)),
  - Fingerprint, hand geometry and palmprint (Uhl and Wild, 2009),
  - Face ((Miyoshi and Hyodo, 2006), (Liang et al., 2007), (Patterson et al., 2007), (Ramanathan and Chellappa, 2005) and (Biswas et al., 2008)),
  - Handwritten signature (Guest, 2006)

More specifically, papers in this area deal with the huge issue of what are the effects of the ageing of the biometric templates. Problems such as defining how often and what is the necessary time interval to update the templates are some of these important issues.

The techniques proposed within this strand in the work reported in this thesis focus mainly on how to use the predicted soft-biometric information or only the soft-biometric information given by the user in the overall system decision-making process. A more detailed review of the literature which relates specifically with our contributions will be shown in Section 3.2 of Chapter 3.

### 1.3.2 Multiclassifier approach

The multiclassifier (meaning more than one classifier) approach aim to integrate more than one classification algorithm to determine the correct individual identity label to assign to a test sample and have the advantage of combining different techniques to solve a problem in a cooperative way (Tronci et al., 2009). This approach has been widely used as a basis for biometric-based fusion techniques ((Barbu et al., 2006), (Sirlantzis et al., 2008) and (Chetty et al., 2007)). However, as already noted, this solution relies on a limited input from the base classifiers and a definition of one combination method.

Agent-based technologies, which are central to some of the core work to be described later in the thesis, have been reported in the processing of biometric information, as can be seen in the following example papers:

- Agents technology used for enhancing writer identification ((Heutte et al., 2004), (Mukhopadhyay et al., 2003), (Vuurpijl and Schomaker, 1998) and (Raje et al., 1998)),
- Managing complexity in multimodal biometrics (Deravi et al., 2003)
- Agent-based network protocols for user authentication with biometrics ((You et al., 2005), (Lu et al., 2007b), (Lu et al., 2007a), (Lu et al., 2009), (Yampolskiy, 2008) and (Chetty et al., 2008)),
• Multiagent system used for enhancing performance in distributed biometrics ((Meshulam et al., 2006) and (Bey et al., 2008))
• An interface agent which uses biometrics (Hernández-Trapote et al., 2008),
• Relational agents for user identification (Schulman et al., 2008).

Notwithstanding this, in all the literature presented above, the agent technology is always used as an interface with the user or a managing tool for the biometric data, but in none of them have these agents been used as classification agents in the fusion level (in the decision-making phase).

In order to create more flexible and interactive systems, one of the proposed solutions which will be considered is to use classification agents to decide the ownership of the test sample. A more detail analysis of the related literature of the multiclassifier approach will be presented in Section 4.2 of Chapter 4.

1.3.3 Multimodal approach

The multimodal strategy refers to the process of combining more than one biometric modality in order to increase user flexibility and system security. This approach has already been widely investigated, with the prospect of offering more accurate results and more options to the user, as well as being a very good way to improve overall performance of the individual identification, which are always strong justifications for adopting this approach (Ross and Jain, 2004). In this type of approach, the overall system should be able to exploit the advantages of each of the constituent modalities and these advantages should be able to overcome, in theory, any weakness of others modalities.

More and more databases are been collected in order to test new proposed multimodal fusion techniques (Faundez-Zanuy et al., 2006), but nevertheless, the amount of data available is often not enough to support strong statistical claims. Also, issues with usability are another point of concern (Toledano et al., 2006). The complexity of this type of system is proportional to the number of modalities that it uses. So, there is potentially a huge computational cost of using a multimodal approach as well as the inevitable greater complexity of these systems (Snelick et al., 2003).

There are very well established modalities which tend to be particularly popular for system designers, such as:

• Physiological (i.e. depending on specific physiological measurements):
  - Face ((Czyz et al., 2004), (Prendinger et al., 2005), (Dol et al., 2006), (Boumbarov et al., 2007), (Lahdenoja et al., 2007), (Lee and Sohn, 2007), (Liu et al., 2007), (Mpiperis et al., 2007), (Schwaninger et al., 2007), (Wang et al., 2007) and (Franco et al., 2008)).
  - Iris ((Daugman, 2000), (Daugman and Downing, 2001), (Daugman, 2003a), (Daugman, 2003b), (Daugman, 2006) and (Park et al., 2008)).
1.3. DIFFERENT APPROACHES: STATE OF THE ART

- Fingerprint ((Jain et al., 1997), (Ross et al., 2002), (Zhang et al., 2001), (Dass and Jain, 2004), (Allah, 2005b), (Allah, 2005a), (Chen et al., 2005), (Chikkerur and Ratha, 2005), (Ross et al., 2005), (Khan et al., 2007), (Chikkerur et al., 2007), (Alonso-Fernandez et al., 2007c), (Ross et al., 2007) and (Sheng et al., 2009)).

- Hand geometry ((Jain et al., 1999), (von Hardenberg and Bérard, 2001), (Öden et al., 2001), (Kumar et al., 2003), (Ong et al., 2003), (Amayeh et al., 2006), (Dagher et al., 2007), (Pavešić et al., 2007) and (Polat, 2008)).

- Behavioural (i.e. determined by activity patterns and not solely physiological):

  - Voice/Speech ((Markowitz, 2000), (Al-Shboul et al., 2007), (Bredin and Chollet, 2007), (Crescenzo et al., 2007), (Kimm et al., 2007), (Prasad et al., 2007) and (Tuononen et al., 2008)).

  - Writer classification ((Zhu et al., 2000), (Zois and Anastassopoulos, 2000), (Vielhauer and Steinmetz, 2004), (Thumwarin and Matsuura, 2004), (Schlapbach and Bunke, 2004), (Bandi and Srihari, 2005), (Bensfia et al., 2005), (Pervouchine and Leedham, 2007), (Bulacu and Schomaker, 2007), (Niels et al., 2008), (Chan et al., 2008) and (Tan et al., 2009)).

  - Offline handwritten signature ((Franke and Köppen, 2001), (Franke et al., 2002), (Saeed and Adamski, 2005), (Dyer et al., 2006), (Alonso-Fernandez et al., 2007a), (Alonso-Fernandez et al., 2007b), (Das and Dulger, 2007) and (Shanker and Rajagopalan, 2007)).

  - On-line handwritten signature ((Jain et al., 2002), (Guest, 2004), (Garcia-Salicetti et al., 2007) and (Kuan et al., 2007))

Even though all the work listed above can be a justification for using these modalities in a multimodal system, it not very clear how better, in general, is a multimodal system when compared with, for example, a multiclassifier system using unimodal biometrics. For instance, the complexity of a unimodal multiclassifier is lower than the complexity of multimodal systems. However, the cost to the user is smaller, as he only needs to provide one kind of biometric sample.

Interestingly, the techniques proposed in this thesis in both the multiclassifier and multcategory cases will provide some very positive evidence that using handwritten signature as a biometric modality, despite sometimes being regarded as a relatively unreliable modality, can be very powerful both as a primary modality in its own right as well as in a broader multimodal system. This will be a recurring theme in the new experimental work reported, even though it is secondary to the main focus of the thesis. Section 5.2 in Chapter 5 will provide a more detailed exploration of the advantages and disadvantages of using the most common modalities and will compare these with handwritten signature.
1.4 Contribution

In a summary, this thesis addresses some issues of each of the three different approaches presented previously: multicategory, multiclassifier and multimodal. The main contributions, generally and in each individual approach can be listed as follows:

1. General biometric-based design:

   (a) A basic general architecture which can be used in any biometric-based system is proposed and described in detail.

2. Multicategory approach:

   (a) A detailed discussion of different strategies which can be used to categorise the soft-biometric information is made.

   (b) Two different techniques by means of which to include soft-biometric information when this information is provided by the user are proposed, which are called Soft biometric as an extra input feature and Soft biometrics as a tool for feature selection.

   (c) Also, two different techniques are explored which deal with the use of soft-biometric information when this information is not provided by the user. The predicted information is applied in a modified Majority weighted vote-based fusion method and Weighted sum-based fusion method.

3. Multiclassifier approach:

   (a) A new idea of using more intelligent fusion approach is introduced as well as the introduction of the idea of a classifier agent.

   (b) Four adaptations of conventional negotiation techniques used by the agents are introduced. They are called game theory-based approach, auction-based approach, sensitivity-based approach and sensitivity-based approach using soft-biometrics, which uses soft-biometric information.

4. Multimodal approach:

   (a) A detailed discussion of the reasons of using some different modalities in multimodal applications is presented.

   (b) Qualitative as well as quantitative evidence of the benefits of using the handwritten signature modality will be presented.

The discussion presented in each of the following chapters will present new ideas for more efficiently design biometric-based systems making the most of any information/modalities available as well as in a more inexpensive way.
1.5 Chapter conclusions and thesis organisation

This chapter has introduced the theoretical basis of the main contributions which will be made by this thesis. The idea of having three different ways for designing a biometric-based system was presented. It is very important to understand this first general view in order to maximise the overall performance of any biometrics system.

Also, an initial overall literature review was presented with respect to each of three different approaches, which we have designated: multicategory, multiclassifier and multimodal. A review of relevant work was reported in order to help us to have a clear view of the state of the art and provide us with an important fundamental understanding of the contributions reported in greater detail in later chapters.

Finally, the organisation of this thesis is presented as follows:

- **Chapter 2: Experimental methodology**
  
  *This chapter will present the system architecture followed by all the experiments. Also, all the background concepts as well as the classifiers and databases used will be outlined.*

- **Chapter 3: Multicategory approach**
  
  *This chapter will discuss all the advantages of using soft-biometric information in order to enhance system performance in biometric-based applications. An analysis of how to categorise and use this information as well as four different techniques which either use the soft-biometrics given by the user, or which predicts that information will be presented.*

- **Chapter 4: Multiclassifier approach**
  
  *This chapter will introduce a new and more intelligent concept of dealing with the centralised problem of the biometric-based fusion techniques. The idea of using intelligent agents as well as modified negotiation protocols in order to increase the flexibility and security of the system will be discussed. Four negotiation techniques adapted to be used in a biometrics system will be presented.*

- **Chapter 5: Multimodal approach**
  
  *This chapter will discuss the importance of deciding correctly the modalities which will be used in a multimodal system. Advantages and disadvantages of well established physiological and behavioural biometric modalities will be analysed. As a case study, we will show that the handwritten signature can be very successful in a multimodal system.*
• Chapter 6: Final remarks

This chapter will present a final discussion of all the contributions made in this thesis as well as describing future work which could usefully be undertaken based on the new ideas introduced by this work.

Taken together, the following chapters will present some encouraging and, it is hoped, interesting ideas to support the development of more effective and flexible biometrics-based person identification systems in the future.
Chapter 2
Experimental methodology

This chapter will present the methodology basis used to evaluate the techniques proposed in this thesis. A description is given of three biometric databases used as well as the explanation of the classifier algorithms used.
CHAPTER 2. EXPERIMENTAL METHODOLOGY

2.1 Introduction

The previous chapter presented the fundamental theories proposed in this thesis as well as a definition of approaches which can be followed when designing a biometric-based system. The three approaches are: multiclass, multiclassifier and multimodal and they will be discussed and analysed in the next three chapters (Chapters 3, 4 and 5), which form the core of the work.

To be able to make any valid conclusion based on the results from the techniques which will be presented, it is necessary to analyse these results in a very meticulous and precise way. The analysis of these results is a very important part of the process because it can either give a strong support to or show weaknesses in the techniques proposed.

But before any analysis can be done, in order to support the theoretical processes presented, an empirical background must be defined and all the experiments analysed must follow these standards. Therefore, the use of a wide range of different possible techniques for the classification of biometric data will be discussed, as well as different biometrics modalities which will be adopted.

Statistical performance metrics which show quantitatively how the choice of classifier will determine the performance attainable will be presented. Also a lower-level analysis (component-based division of the whole process), which delivers more targeted selection strategies in situations where the outcome might be guided by the availability of specific information which can inform the decision-making process will be discussed.

The next section (Section 2.2) will present the basic architecture used in all the experiments as well as describe its individual components. Section 2.3 will present all the concepts needed to understand the results and the basic experiments. Section 2.4 will present all the base classifier algorithms used. And Section 2.5 will present the three biometric databases used as well as the soft-biometric information.

2.2 Basic system architecture

Biometric-based systems normally are composed of well defined components with very specific functions. In a unimodal system, the flow of data starts with a capture/extraction process where the biometric features are extracted. Then, a noise removal phase is implemented followed by the classification (identification) of the test samples. If a multiclassifier approach is applied, another phase of organising the outputs of the classifiers is necessary, as well as a fusion phase. In a multimodal system, this process can be even more complex.

The definition of a base system architecture, where the system designer has the flexibility of deciding which components should be modified or not is very important. Defining the sequence in which the information will flow is fundamental for a successful system. Reasons such as that the management of the system is much easier when it is well defined as well as the prompt finding and fixing of
errors makes this component-based architecture very promising.

Generally, the biometric-based system used for the work reported in this thesis is composed of four main components and can be illustrated as shown in Figure 2.2. Inside each of these four modules, different components can be used depending on the application or technique. The general definition of each module/component can be described as follows:

- **Input Data Processing**: This is the first phase of the identification process. In this module, all the input biometric information and, if necessary, the non-biometric (soft-biometrics, in the most usual case) information will be processed. Specifically, any data capture, data feature extraction, feature selection or soft-biometric prediction will happen in this first module. Also, the input features of the next module (Individual classifiers) will be selected and organised in a vector of dimensionality $x$.

- **Individual classifiers**: This second module/component is composed of a selection of classification algorithms which can either classify a user from an input sample or classify soft-biometric information from this same data. The input features (derived from the biometrics and sometimes from the soft-biometrics) will feed all the classifiers and they will all try to label the new input sample with a user identification name (ID) (identity prediction classifiers) and also in some cases they will try to label this input within a soft-biometric category (soft-biometric prediction classifiers). In this case,
there are $x$ features as input, $k$ soft-biometrics categories (sometimes more than one soft-biometric information source is used) and $y$ user IDs as classes.

- **Classifier Outputs Processing**: This module is responsible for receiving information from the **Individual Classifiers** (which is composed of many classifiers, that is why it has this name) and the **Knowledge Database** modules, and presents the structured data to the data combination module for processing by whichever fusion technique is being used.

- **Knowledge Database**: This stores the biometric-related and more general important information from each enrolled user.

- **Fusion Classifier**: This module will implement any fusion technique which will be used to fuse the information from the **Classifier Outputs Processing** module.

The possibility of defining components for a system and modifying only the necessary components is very important for the consistency of the system and the evaluation of the results. In some cases, some components will be included in order to satisfy the requirements of specific approaches.

This architecture is used in all the experiments to be reported and as a basis for the definition of all the techniques presented in this thesis.

### 2.3 Background

Pattern recognition tasks have very particular pre-defined concepts which are important to be kept in mind. This section will present all the necessary concepts to understand the results presented in the subsequent chapters.

The important concepts regarding the classifiers used are as follows:

- Biometric-based systems would normally perform one of two possible different tasks: verification and identification. Verification is the process whereby the system compares an input test sample from a system user with another (from a pre-enrolled template) in order to verify whether that user is who he/she claims to be. That is, it is a 1:1 process. Identification, on the other hand, is the process whereby the system searches a database and compares an input test sample from a user with all the enrolled users in order to find out who that user is. In other words, it is a 1:many process.

- When a verification task is performed, its training and testing sets are created using different variations of matching samples and non-matching samples being assigned with a "Yes" and "No" label, depending on the situation with regard to a known "ground truth".

- A piece of information used as an essential component for the fusion/ negotiation methods is called **confidence degree** and we will designate this $\text{Conf}$. 
2.4. Classifiers

This metric is also called Error Rate in the discussion of the performance of the system. All the classifiers used in the work reported here will produce outputs for all the possible classes and the winner class (the one with the highest output value) is assigned the overall output (decision) of this classifier. In the fusion/negotiation techniques which will be presented here we will use all the outputs or confidence degrees for all the classes of the problem. This error rate or Conf will always be a value between zero and one.

- Despite being a well accepted metric adopted in biometric processing studies, the false acceptance rate (FAR) and false rejection rate (FRR) were not analysed in this thesis. As explained previously, we are using the confidence degrees (which is normally adopted when using intelligent agents) as well as the standard deviations of the system to consistently analyse the performances.

Regarding the evaluation of the system results, the important concepts are:

- Each database was divided in two sets, one of which (containing approximately 90% of the samples) was used to train the classifier and the other of which (10%) was used to validate the method.

- The 10-fold-cross-validation method (Leisch et al., 1998) was used to evaluate classifier performance. In this evaluation method, the training set is divided into ten folds, each with approximately the same number of samples. Thus, a classifier is trained with nine folds and tested with the remaining unused fold. Validation is performed every time the test fold is run.

- The analysis of the resulting classifier performance used the statistical t-test (Mitchell, 1997) with 95% degree of confidence. This test uses the t-Student distribution to compare two independent sets. The use of this test allows us to say whether a classifier is statistically more accurate than another just by observing whether the p value is smaller than the threshold established.

This information will be very important to the understanding of the results and of how each fusion/negotiation technique works.

2.4 Classifiers

One of the more difficult aspects of designing a classification task is making the best choice of the base classifiers for the fusion/negotiation method. A guarantee of diversity among the individual components is indispensable in this context. The pool of classifiers selected for the experimental study here, comprising eight specific classifiers, is now defined, grouped and briefly described. We have chosen the following as our classifier pool:
Neural network-based classifiers:

- Multi-Layer Perceptron (MLP) (Haykin, 1999): MLP is a Perceptron neural network with multiple layers (Rosenblatt, 1958). The output layer receives stimuli from the intermediate layer and generates a classification output. The intermediate layer extracts the features, their weights being a codification of the features presented in the input samples, and the intermediate layer allows the network to build its own representation of the problem. Here, the MLP is trained using the standard backpropagation algorithm (Chauvin and Rumelhart, 1995) to determine the weight values.

- Radial Basis Function Neural Network (RBF) (Buhmann and Buhmann, 2003): This adopts an activation function with radial basis, and can be seen as a feed forward network with three layers. The input layer uses sensory units connecting the network with its environment. The second layer executes a non-linear transformation from the input space through the output space performing the radial basis function. And the third layer uses the output from the second layer to calculate the confidence degree to each class of the problem to be solved.

- Fuzzy Multi-Layer Perceptron (FMLP) (Canuto, 2001): This classifier incorporates fuzzy set theory into a multi-layer Perceptron framework, and results from the direct "fuzzyfication" in the network level of the MLP, in the learning level, or in both. The desired output is differently calculated when compared with the MLP, the nodes which are related with the desired output being modified during the training phase, resulting in a "fuzzy output".

Kernel estimation-based classifier:

- K-Nearest Neighbours (KNN) (Arya, 1998): This embodies one of the most simple learning methods. The training set is seen as composed of n-dimensional vectors and each element represents a point in n-dimensional space. The classifier estimates the $k$ nearest neighbours in the whole dataset based on an appropriate distance metric (Euclidian distance in the simplest case). The classifier checks the class labels of each selected neighbour and chooses the class that appears most in the label set.

Rule-based classifiers:

- Decision Trees (DT) (Quinlan, 1993): This classifier uses a generalised "divide to conquer" strategy, splitting a complex problem into a succession of smaller sub-problems, and forming a hierarchy of connected internal and external nodes. An internal node is a decision point determining, according to a logical test, the next node reached. When this is an external node, the test sample is assigned to the class associated with that node.
2.5. DATABASE

- Optimised IREP (Incremental Reduced Error Pruning) (JRip) (Furnkranz and Widmer, 1994): The Decision Tree usually uses pruning techniques to decrease the error rates of a dataset with noise, one approach to which is the Reduced Error Pruning method. Specifically, we use Incremental Reduced Error Pruning (IREP). The IREP uses a "divide to conquer" approach. This algorithm uses a set of rules which, one by one, are tested to check whether a rule matches, all samples related to that rule then being deleted. This process is repeated until there are no more samples or the algorithm returns an unacceptable error. Our algorithm uses a delayed pruning approach to avoid unnecessary pruning, resulting in a JRip procedure.

Linear-based classifiers:

- Naive Bayesian Learning (NBL) (Elkan, 1997): This algorithm relates to a simple probabilistic classifier based on the application of Bayes theorem with the assumption of strong independence. The principle adopted is to estimate the conditional probability of each class label with respect to the test sample. In this method, it is assumed that each attribute is independent of the others.

- Support Vector Machines (SVM) (Nello and John, 2000): This approach embodies a functionality very different from that of more traditional classification methods and, rather than aiming to minimise the empirical risk, aims to minimise the structural risk. In other words, the SVM tries to increase the performance when trained with known data based on the probability of a wrong classification of a new sample. It is based on an induction method which minimises the upper limit of the generalisation error related to uniform convergence, dividing the problem space using hyperplanes or surfaces, splitting the training samples into positive and negative groups and selecting the surface which keeps more samples.

These particular classifiers were chosen in order to emphasise the diversity of the overall system implemented. Although some of them employ similar basic operational principles, they each deliver the process underpinning the class separation task in very different ways.

2.5 Database

The Multimodal database used in the work reported here was collected in the Department of Electronics of the University of Kent (Ortega-Garcia et al., 2006) as part of the Europe-wide BioSecure Project. In this database, there are samples of Face, Speech, Signature, Fingerprint, Hand Geometry and Iris biometrics from 79 users collected in two sessions. In the work reported in this thesis, samples from the fingerprint, hand geometry and the signature samples (from both sessions) were used. These subsets, as well as the soft-biometric information used, will
be described in the next four sections. Further comments about possible issues related with these modalities will be addressed in Section 2.5.5.

2.5.1 Fingerprint Database

The BioSecure database contains samples from sensors based on both thermal and optical fingerprint capture methods, producing images from the same finger (index finger of the right hand). Samples from each of these techniques can be seen in Figures 2.3 and 2.4, respectively.

![Optical fingerprint](image1)
![Thermal fingerprint](image2)

In each case samples corresponding to right thumb, index and middle fingers and left thumb, index and middle fingers are collected. In the working database, features based on the minutiae of the fingerprint samples were extracted, as follows:

- X-pixel Coordinate
- Y-pixel Coordinate
- Minutia Type
- Direction
- Ridge Curvature
- Ridge Density
The minutiae were extracted using the VeriFinger (Neurotechnologija, 2008) software. As each fingerprint image generates a different number of detectable minutiae, while the classifiers adopted need a common number of entries, it is necessary to normalise the number of minutiae. Here, a standard algorithm for core detection (Khan et al., 2007) was used and the 10 minutiae closest to the core to use as input to the classifier were identified (which is the basic number used in the literature (Hsu and Martin, 2008)). Both optical and thermal samples of all six fingerprints were used.

### 2.5.2 Signature

The database contains 25 signature samples for each subject, where 15 are samples of the subject’s true signature and 10 are attempts to imitate another user’s signature. In this investigation, only the 15 genuine samples of each subject were used. The data was collected using an A4-sized graphics tablet with a density of 500 lines per inch and a sample can be seen in Figure 2.5. There are 21 representative biometric features extracted from each signature sample, as follows:

- Execution Time: The total time taken to execute the signature.
- Pen Lift: The number of times the pen was removed from the tablet during the execution time.
- Signature Width: The width of the image in mm.
- Signature Height: The height of the image in mm.

![Figure 2.5: Sample of a signature of the BioSecure database](image)
• Height to Width Ratio: The division of the signature height by the signature width.

• Average Horizontal Pen Velocity in X: The pen velocity in the $x$ plane across the surface of the tablet.

• Average Horizontal Pen Velocity in Y: The pen velocity in the $y$ plane.

• Vertical Midpoint Pen Crossings: The number of times the pen passes though the midline of the signature.

• $M_{00}$: Number of points comprising the image.

• $M_{10}$: Sum of horizontal coordinate values.

• $M_{01}$: Sum of vertical coordinate values.

• $M_{20}$: Horizontal centralness.

• $M_{02}$: Vertical centralness.

• $M_{11}$: Diagonality - indication of the quadrant with respect to centroid where image has greatest mass.

• $M_{12}$: Horizontal Divergence - indication of the relative extent of the left of the image compared to the right.

• $M_{21}$: Vertical Divergence - indication of the relative extent of the bottom of the image compared to the top.

• $M_{30}$: Horizontal imbalance - location of the centre of gravity of the image with respect to half horizontal extent.

• $M_{03}$: Vertical imbalance - location of the centre of gravity of the image with respect to half vertical extent.

• Azimuth: is an angular measurement in a spherical coordinate system using the pen as parameter.

• Altitude: is the steepness of the pen position relative to the tablet surface.

• Pressure: is the measurement of the pressure exercised by the user during the writing of the signature.

These features were chosen to be representative of those known to be commonly adopted in signature processing applications, as identified from a study of the relevant literature and in-house experience. All the available biometric features are used in the classification process as input to the system.
2.5.3 Hand Geometry

The hand geometry database contains four hand image samples for each subject, where two samples are from the right hand and the other two are from the left hand. A digital camera was used to capture an image of these user’s hands in a wide open position (Amayeh et al., 2006). From each sample, 19 geometric distance measures were extracted as follows:

- Five distances from the tip of the finger to its border with the palm of the hand.
- From each finger, except the thumb, we use the medial-lateral distance of the distal end of the middle phalanx, the medial-lateral distance of the proximal end of the proximal phalanx and the medial-lateral distance of the distal end of the proximal phalanx.
- From the thumb, we use only the medial-lateral distance of the distal end of the proximal phalanx.

Figure 2.6: Sample of a left-hand of the BioSecure database

Figure 2.6 shows the markings of the measurements extracted as features of the hand geometry of the BioSecure. These geometrical features are chosen to
be representative of those known to be commonly adopted in hand geometry processing applications.

2.5.4 Non-Biometric Information

During the acquisition of this database, the participating subjects were required to provide some additional information which, although non-biometric in nature, may nevertheless have relevance to the process of determining or verifying their identity. This information is of particular relevance and importance to some of the work to be reported in this thesis.

In particular, following information about each user was recorded:

- **Gender**: Male or Female.
- **Age information**: For the purposes of this work, three age groups were identified, namely: under 25 years, 25-60 years and over 60 years. This is in line with a number of other reported studies (Ajmera, 2006), (Metze et al., 2007), (Miyoshi and Hyodo, 2006) and (Modi et al., 2007).
- **Visual Defects**: Any visual problem (ranging from simply whether the user wears glasses, to more serious conditions such as the presence of cataracts) was recorded. For simplicity, although recognising the implications of the real diversity of differing conditions, all recorded defects were considered as a single condition, giving a binary YES/NO label in the relation to this characteristic.
- **Handedness**: Right, Left or Ambidextrous.
- **Occupation**: This relates to the occupation of the subject, but here only in general terms, since it is important to know the occupational factors which might have a direct bearing on sample quality. However, for simplicity, although again recognising the implications of the potential diversity of differing conditions, all occupations which could typically carry a significant risk of hand damage (e.g. damages such as the ones normally inflicted in someone who works in the construction field would have an influence in fingerprint quality) were considered as a single category, giving a binary YES/NO label in relation to this characteristic.

In the study reported here, the users’ characteristics with respect only to the three categories relating to the age information, the handedness and gender were used. The addition of this information will depend on the application and the technique used and will be explained in greater detail in the following chapters.

2.5.5 Database issues

The selection of a database in order to validate a theoretical study is a very important step in the methodology process and it must take into consideration
any ambiguity, inconsistency or unfairness that can be extended to the results analysis and comparison.

The first problem that arises from this dataset is the fact the signature database contains more samples than the fingerprint database and, even more evident, the hand geometry. In order to evaluate the advantages of using all 15 signature samples against the 12 of the fingerprint or the 4 of the hand geometry, experiments using 12 and 4 signature samples were performed with some of the base classifiers adopted. The results have shown that there is only a 3.8% improvement when 15 signatures are used rather than 4 signatures which validates the use of the total number of signatures without having an unfair comparison.

Another issue to be dealt with is the fact that there are fingerprint samples which were captured using different sensors (thermal and optical) as well as there being samples from 6 different fingers. In order to demonstrate the validity of using this database, an MLP using different training and testing sets was created and the results can be seen in Table 2.1.

<table>
<thead>
<tr>
<th>Training</th>
<th>Thermal</th>
<th>Optical</th>
<th>Thermal</th>
<th>Optical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing</td>
<td>Thermal</td>
<td>Optical</td>
<td>Optical</td>
<td>Thermal</td>
</tr>
<tr>
<td>Error Rate</td>
<td>18.93%</td>
<td>17.14%</td>
<td>19.24%</td>
<td>18.54%</td>
</tr>
</tbody>
</table>

Table 2.1: MLP results for different fingerprint training and testing sets

Based on these results, the variation in error rate when changing the training and testing sets is of around 1% which is acceptable in a statistical comparison when samples collected using different samples are used together.

2.6 Chapter conclusions

In this chapter, the basic necessary concepts to understand and evaluate the experimental results of this thesis were presented.

In order to evaluate correctly and fairly the results regarding the new techniques proposed in each approach, the same base infrastructure must be used. Therefore, the standard system architecture used in all experiments was described as well as each of its four basic components.

The experimental infrastructure was detailed in three sections: Background (where all the basic concepts were defined), Classifiers (where all the base classifiers used were presented) and Database (where the three experimental databases employed in the study were explained, as well as the soft-biometrics used). Possible problems of using this database were also presented.

It is important to point to the fact that all three databases used in this investigation are hand-based modalities. Because they are related only to one part of the body, the results presented in the next three chapters will have limitations (because of the localised data source), but nevertheless, will contain important insights in the relationship of data that genuinely relates to itself (i.e. all the three different modalities belong to the same user).
The next chapter will discuss the first of the proposed paradigm: Multicategory approach.
Chapter 3

Multicategory approach

This chapter will investigate one of the approaches introduced in this thesis: the multicategory approach. In particular, the use of soft-biometric information as a tool for enhancing system performance, system flexibility and system usability is presented.
3.1 Introduction

The use of multiple categories of information in biometric-based applications is not new, notwithstanding the fact that this topic has been neglected in the literature compared with other structural approaches. The term "multicategory" as used here denotes, as the term suggests, the use of more than one category of information. In this case, we use the term to imply using both biometric data and also some other different information, usually that which is typically called "soft-biometrics".

The term soft-biometrics (also referred in the literature as meta biometrics or simply non-biometrics), in the context of this work, signifies every information source which relates to the user, but which does not have all the necessary characteristics to be considered directly as a true biometric data, but which nevertheless can be used to narrow the search or even to group the population in some way (Fairhurst and Abreu, 2009a).

Essentially, any information which is not considered a biometric but, nevertheless, is a characteristic of the user and can be extracted from (or given by) him/her can be used as a soft-biometric. However, in the same way as biometric information, soft-biometrics need to be measurable and/or categorisable. Hence, data such as age (Jain et al., 2004a), (Jain et al., 2004d), gender (Jain et al., 2004d), (Jain et al., 2004a), handedness (Abreu and Fairhurst, 2008a), iris colour (Zewail et al., 2004), height (Jain et al., 2004d), (Jain et al., 2004a), percentage of body fat (Ailisto et al., 2006) and so on are natural choices for this type of information source.

The soft-biometric category is a very powerful ally of the system designer when developing a biometric-based system. It is normally very cheap to acquire (it does not need another sensor for its capture), it is not invasive (the user gives some of the most used soft-biometrics as secure questions readily and often routinely), it is usually inclusive (everybody has this information) and, as is going to be demonstrated here, it is relatively simple to be incorporated in the identification process.

Therefore, while the primary objective of biometric processing is to establish individual identity, it is increasingly recognised that there is a close link between identification of individuals and situations commonly targeted by biometric systems where the prediction of important characteristics from that individual is also necessary (Jain et al., 2002), (Pervouchine and Leedham, 2007), (Dyer et al., 2006). Part of the analysis of data might well include the need to estimate a more general characteristic (such as age or gender, for example) of the "owner" of the specific piece of information under consideration. Predicting an individual’s characteristics has wider application, but the investigation reported in this chapter will be focused on how this predicted information can be of use in helping the prediction of the user's identity.

Thus, this chapter will investigate both the impact of the use of soft-biometric information on overall performance, complexity and usability in the design of
3.1. INTRODUCTION

Figure 3.7: Various approaches to the problem: Focusing on the multicategory approach

biometric-based systems as well as the predictive capabilities of biometric systems in relation to individual characteristics. Based on the general structural diagram presented in Chapter 1, we will here investigate the shaded area shown in Figure 3.7 which explores the representation of the different categories and how this information can be used in the intersection with the other two identified approaches.

Furthermore, because of the nature of the data in this specific category (population data characteristics) and as a consequence of a lower-level analysis, it is possible to point to more specific strategies both for potentially improving error-rate performance achievable in a biometric system and also increasing the flexibility with which specific implementation configurations can be designed, and consider a range of solutions of different levels of complexity.

Section 3.2 will describe the related literature which uses in different ways information such as gender, age and height in biometric-based systems. Following this idea of using soft-biometrics to enhance biometric-based system performance, Section 3.3 will discuss the different strategies which can be used to categorise the soft-biometric information. Section 3.4 will explore two different techniques to include soft-biometric information when this information is provided by the user. On the other hand, Section 3.5 will explore the use of soft-biometrics when
this information is not provided by the user, where the idea here is to predict this information. And finally Sections 3.6 and 3.7 will present some interesting results as well as discuss the implications of the new techniques proposed here.

3.2 Review of soft-biometrics data categories

The use of soft-biometric information to improve identity verification has not been as widely investigated as most other options for improving accuracy and reliability in biometric processing. Nevertheless, it is possible to find some interesting relevant work in the literature. Following the first high level review presented in Chapter 1 about the use of soft-biometrics in the biometrics field, this Section will present a more detailed specific review of the relevant work.

In (Jain et al., 2004a) and (Jain et al., 2004d), the authors investigate characteristics such as gender, ethnicity, and height which are extracted automatically to provide some information about the user in a fingerprint verification task. This information is incorporated into the decision making process of the primary biometric system, using the probability related to that specific soft-biometric. The database adopted contains 160 users, each providing four samples of their left index finger, left middle finger, right index finger and right middle finger, where minutiae features were extracted for the biometrics-based processing. Their experiments, using synthetically generated soft-biometric data based on known statistics, show results with 80.1% accuracy.

In (Jain et al., 2004b), a hybrid verification biometric system that uses face and fingerprint as the primary characteristics and gender, ethnicity, and height as the soft characteristics is described. The fingerprint database used contains 160 users, each providing four samples of their left index finger, left middle finger, right index finger and right middle finger, where minutiae features were again extracted. The face database contains images of 263 users, with 10 images per user where linear discriminant analysis (LDA) features were extracted (score vector of length 8). The experiments use an ethnicity classifier (Asian or non-Asian with 96.3% accuracy), a gender classifier (89.6% accuracy) and the height information already available. As in (Jain et al., 2004a), this information is incorporated into the decision making process of the primary biometric system and uses the probability related to that specific soft-biometric characteristic. The results show that neither ethnicity nor gender improve the performance of the systems. However, the system that uses height, face and fingerprint returns an accuracy of around 95.5%.

In (Zewail et al., 2004), a framework for integrating the colour of a human iris within a multimodal biometric system is described which combines fingerprint and iris in a verification task. Steerable pyramid filters and multi-channel log-Gabor filters are used for extracting features of the fingerprints and iris respectively. Weighted averaging and a Parzen classifier are used for fusion of these features. The DSP-AAST Iris database and FVC fingerprint database are used. The Parzen classifier generates the best results with an accuracy of around 97%.

In (Ailisto et al., 2006), a fingerprint verification system which also makes
3.3. SYSTEM DESIGN USING SOFT-BIOMETRICS CATEGORIES

use of body weight measurements is presented. Weighted sum of scores, support vector machines (SVM), multilayer Perceptron (MLP) as well as logical OR and AND are the methods employed in data fusion. A database containing fingerprints (minutiae were extracted), body weight and fat percentage data for 62 individuals was collected for this study. The results reported show a decrease in the total error rate of about 3.9% when incorporating the soft-biometric information.

The literature reports many studies related to the prediction of gender and age using modalities such as the face ((Patterson et al., 2007) and (Matta et al., 2008)), voice (Metze et al., 2007) and iris (Thomas et al., 2007). Nevertheless, none of the work in the literature uses this predicted information in the identification process.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Modality</th>
<th>Soft-biometric</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Jain et al., 2004a)</td>
<td>fingerprint</td>
<td>gender, ethnicity and height</td>
<td>80.1%</td>
</tr>
<tr>
<td>(Jain et al., 2004b)</td>
<td>face and fingerprint</td>
<td>height</td>
<td>95.5%</td>
</tr>
<tr>
<td>(Zewail et al., 2004)</td>
<td>fingerprint and iris</td>
<td>iris colour</td>
<td>97%</td>
</tr>
<tr>
<td>(Ailisto et al., 2006)</td>
<td>fingerprint</td>
<td>body weight</td>
<td>96.1%</td>
</tr>
</tbody>
</table>

Table 3.2: Literature results when incorporating soft-biometric information

In summary (the related work with accuracies can be seen in Table 3.2), the amount of related work is not very extensive. Generally, it can be said that the majority of work reported in the literature includes the categories of soft-biometrics in the fusion phase as a probabilistic parameter in either multimodal or unimodal systems. In this thesis, the use of soft-biometric categories is extensively explored in several levels of a biometric-based system.

3.3 System design using soft-biometrics categories

In spite of the apparent under-use of soft-biometrics information reported in the literature, this is indeed a very versatile source of information data. In general, there are two ways in which the soft-biometric information can be obtained:

- Working with the information given by the system user,
- Predicting the information from the biometric data extracted from the user.

In the first approach, the user gives the information at the same time at which the biometric data is collected. The problem with this approach is that the user might provide wrong information and in some situations, that the data is examined without the presence of the user (an example of such a situation might be a forensic investigation, for instance), can make it impossible to obtain this information.

The second approach, where the system predicts the soft-biometric from the biometric sample, is less directly dependent on the user. This is a very convenient opportunity to maximise the information extracted from the user without any extra interaction.

Section 3.3.1 will discuss the most common soft-biometrics and how they are used in a biometric-based system, and Sections 3.4 and 3.5 will describe different
techniques by means of which it is possible to use soft-biometric information in a biometric-based system.

### 3.3.1 Categorisation of the soft-biometrics

The choice of which soft-biometrics to use is as difficult as the choice of which full biometrics to use. It is very much dependent on the population characteristics and in the modalities which will be used in the system.

Three of the most common soft-biometrics will be described in the following section. They are age, gender and handedness.

#### Age

The age of an individual is clearly a very important information. It is used in security transactions as well as in legal matters. Besides, the age of a subject has an impact on the overall design of the system as well as the planning of the enrolment and update of user. In this sense, it is as important to know how and which modalities and information it will be necessary to collect in the first enrolment process as well as the frequency the re-enrolment which will be necessary. There are three ways of integrating this information, as follow:

![Figure 3.8: Fuzzyfication of subject age](image)

- The use of an absolute age parameter,
- The use of groups of users in different age bands,
• The use of fuzzy sets in different age bands.

The first option is to use directly the number which represents the age of the user. This is generally not a precise measurement, but rather an approximation, because age is a continuous variable. The second approach divides the population into age bands creating a categorical feature which will indicate to which groups each user will belong. The number of groups (child, adult or elderly, < 25, 25 − 60, > 60) is still very empirical, as there has not been an extensive study of the effects of age in biometrics and, therefore, there is incomplete knowledge of how the age affects each different modality. Nevertheless, although using age groups considers the biological differences among the biometric samples in different age groups, it is still a "sharp" division.

As age itself is not such a "sharp" characteristic (i.e. age is a continuous variable) and the way people age is relatively different in each age group, in order to retain this idea of the continuous nature of this information source, the third approach uses fuzzy groups to represent age, as illustrated in Figure 3.8.

Figure 3.8 shows the fuzzy representation of age as a continuous feature. In this approach, degrees of pertinence will be given to all the different age groups to each user. As an example, if the user is 25 years old, the values to each fuzzy set would be: Young = 0.2 (20%), Adult = 0.8 (80%) and Elderly = 0.0 (0%).

Even though the focus of this chapter is the investigation of how to improve accuracy using soft-biometrics, it is also very important to understand the real effect of the ageing process in the identification task as a whole. It is expected that the age will have a bigger impact in the identification process. In that sense, some of the results must be interpreted more as age characteristic effects than simply the addition of age information.

**Gender**

In a simpler way, subject gender is a very easy item of information to categorise. Naturally, male and female are used as the two possible categories. Nevertheless, these days, this information is not always simply one or the other.

A small proportion of the population claim they belong to one group, but they once belonged to the other. Or, it is very easy to find facial features of some people from one group which could easily be claimed to show characteristics of the other group.

**Handedness**

As in case of gender, the categorisation of "handedness" is also a very easy process. Naturally, right-handed and left-handed are used as the two possible categories. However, ambidextrous writers must also be considered.

Arguably, handedness can indeed be considered as a continuous soft-biometric. The ambidextrous user can provide the proportion of use in each hand and this information can be very valuable as an identifier for this small proportion of the population.
Choosing the soft-biometrics

In the same way that choosing the biometric modalities is very dependent on the population characteristics, the system designer must take into account which soft-biometric information will have any effect over the modalities used in the system. It is very important to make sure the information used is adding accuracy or helping the grouping of the population in relation to that specific modality.

Naturally, age information affects most of the biometric modalities, but this is not the only obvious choice. Combinations such as: Gender and fingerprint or signature; Handedness and hand geometry or signature (Abreu and Fairhurst, 2008a) can generate interesting results as will be shown later in this chapter.

3.4 Using soft biometric given by the user

In this section, two different techniques which combine/use soft-biometric information when it is provided by the user will be introduced. The first level of the biometric-based system design introduced in Chapter 2 uses soft-biometrics is the Input Data Processing module (presented in Figure 2.2).

At this level, there are two different ways in which the soft-biometric information can be used: As a simple extra input or as a feature selector. Sections 3.4.1 and 3.4.2 will explain the two approaches in more detail.

3.4.1 Soft biometric as an extra input feature

In this approach, the soft-biometric information functions, in essence, as an extra input feature. The soft-biometric information is used in the same way as any other biometric feature and is simply added to the input vector. Figure 3.9 shows a schematic illustration of this process.

This information can be added into our analysis of system performance, where these additional characteristics effectively define sub-groups within our overall test population. These new information sources contribute to the system input information in the same way as the extracted sample features are used, which requires the integration of the further features.

The modules of the system may be described as follows:

- Inside the first module shown in Figure 3.9 (corresponding to the Input Data Processing first presented in Figure 2.2):
  - Categorisation of the soft-biometrics: This module, as its name suggests, performs the categorisation (introduced in Section 3.3.1) of whichever soft-biometric information the system is using.
  - Feature extraction from the biometrics: This module is responsible for extracting the features from the real (hard) biometric sample(s) collected from the user through the appropriate sensor.
3.4. USING SOFT BIOMETRIC GIVEN BY THE USER

Figure 3.9: Soft-biometric as input features

- **Concatenation of input features**: This module will organise all the input features (hard biometrics and soft-biometrics) in a vector which will be sent to the next module of the system.

- In the *Individual Classifiers* module, the features vector will be used as input to the classifiers and these classifiers will produce their outputs.

- The *Classifier Outputs Processing* module will organise all the outputs from the classifiers and will generate a vector which will be sent to the *Fusion Classifier* module.

- The final output of the system will be produced by the *Fusion Classifier* module (contains one classifier which will decide according to the base classifiers opinions what is the best identity prediction for the input sample).

In this sense, the individual classifiers will be trained with all the biometric input features as well as the categorised soft-biometric features. The flow of information during the test phase in the system can be explained as follows:

1. The input sample $F$ is extracted from the user in the *Feature extraction from the biometrics* in the *Input Data Processing* module, where

   $$ F = [f_1, f_2, f_3, ..., f_n] $$

   where $n$ is the number of features from the modality.
2. \( F \) is sent to Concatenation of input features module.

3. Also, the soft-biometrics information is collected and directed to the Categorisation of the soft-biometrics also in the Input Data Processing module.

4. The categorisation is performed and this information is sent to the Concatenation of the input features module as

\[
F_{\text{softbiometrics}} = [f_{1,1}, \ldots, f_{1,s_1}, \ldots, f_{h,1}, \ldots, f_{h,s_h}]
\]

where \( h \) is the number of soft-biometrics used and each soft-biometric element will have a different number of categories which are represented by \( s_h \).

5. \( F_{\text{softbiometrics}} \) is also sent to Concatenation of input features module.

6. The Concatenation of the input features module simply organises the features which will be fed to the Individual Classifiers module. This vector will be formed by

\[
F_{\text{withSoftBiometrics}} = [f_1, f_2, f_3, \ldots, f_n, f_{1,1}, \ldots, f_{1,s_1}, \ldots, f_{h,1}, \ldots, f_{h,s_h}]
\]

where \( n \) is the number of features from the modality and the remaining features are the ones corresponding to the soft-biometrics information. The total number of features plus the soft-biometrics is given by \( n + h \times s_h \).

7. Individual Classifiers module will contain only classifiers which will label the input sample as one of the enrolled users, producing the following confidence degrees:

\[
CD_c = [cd_{1,1}, cd_{1,2}, \ldots, cd_{1,y}, \ldots, cd_{c,1}, \ldots, c_{c,y}]
\]

where \( y \) is the number of enrolled users and \( c \) represents the number of the classifier.

8. All the confidence degree values are sent to Classifier Outputs Processing module which will then organise this information and send the relevant data to the fusion technique used in the Fusion Classifier module.

9. The Fusion Classifier module will then produce a final output of the system which will label the input sample as one of the enrolled users.

As shown above, this is a very simple technique, which just includes any additional information (in this case, soft-biometric information) in order to improve the system performance. It does not have any restrictions as it can be used either in unimodal or in multimodal systems. Also, its complexity is very low when compared with techniques which the focus is on fusion techniques or classifier algorithms.
3.4.2 Soft biometrics as a tool for feature selection

In this approach, the soft-biometric information works as a feature selector, the selection being related to the demographic information which is saved in the *Knowledge Database* module of the system. This technique differs from the one presented in Section 3.4.1 just slightly in the training phase of the individual classifiers and one of the modules of the *Input Data Processing*. Figure 3.10 shows how the process is realised.

![Figure 3.10: Soft-biometric as feature selector](image)

During the training phase, it is important to understand the relationship between the features and the soft biometric information, from which the system is able to choose the most suitable features for each user. This is one element of the information which will be stored in the *Knowledge Database* module and will be used in the *Select the feature using soft-biometrics* module. The feature analysis is carried out, after training the system with all the biometric features, as follows:

1. Categorise the soft-biometric information which is going to be used.

\[
SoftBiometricsCategories = [sb_{1,1}, ..., sb_{1,s_h}, ..., sb_{h,1}, ..., sb_{h,s_h}]
\]
where \( h \) is the number of soft-biometrics used and each soft-biometric will have a different number of categories which are represented by \( s_k \). For example, when using age and gender, the vector will look like as follows:

\[
\text{SoftBiometricsCategories} = [\text{Age}_{\text{young}}, \text{Age}_{\text{adult}}, \text{Age}_{\text{elderly}}, \text{Gender}_{\text{male}}, \text{Gender}_{\text{female}}]
\]

2. From the validation set, group the samples into the defined categories.

3. Using the groups from the validation set, test the system and save the error rates for each classifier. The confidence vector for each classifier will be as follows:

\[
\text{CD} - \text{validation} = [\text{cdVal}_{s_1,1}, ..., \text{cdVal}_{s_1,s_k}, ..., \text{cdVal}_{s_h,1}, ..., \text{cdVal}_{s_h,s_k}]
\]

where \( s_b \) are the soft-biometric categories and \( \text{cdVal} \) are the error rates of this classifier for the samples from each group category.

4. For each soft-biometric source:
   (a) Select all the samples from users in this category of soft-biometric information.
   (b) For each biometric feature, test all the validation set samples ignoring this one feature. The value of this evaluated feature will not be considered by the classifiers.
   (c) Save the error rates to each feature related to each soft-biometric, which should be as follows:

\[
\text{CD} - \text{validation}_f = [\text{cdVal}_{f,s_1,1}, ..., \text{cdVal}_{f,s_1,s_k}, ..., \text{cdVal}_{f,s_h,1}, ..., \text{cdVal}_{f,s_h,s_k}]
\]

where \( s_b \) are the soft-biometric categories and \( \text{cdVal} \) are the error rates of this classifier with respect to the samples from each group category making the feature \( f \) a null feature.

5. Once the system is tested with all different feature combinations and the error rates saved, for each feature \( f \) in each soft-biometrics category \( s_b \), the following process is executed:
   (a) Calculate the difference between the confidence when all the features are used and when feature \( f \) is null:

\[
diff_f = \text{cdVal}_{f,s_b} - \text{cdVal}_{s_b,}\!
\]

(b) If \( \text{diff}_f < \text{threshold} \) (which is defined by the system designer), then this feature is not representative for this group (category) and it is
not going to be used in the classification. Otherwise, the feature is representative and will be included in the classification.

(c) Save this information in the Knowledge Database module.

The definition of the threshold will depend on the level of security associated with the identification process. Having a big value will mean that less representative features will be used in the process and, therefore, more information (even though not necessary) will be taken into consideration. Having a small value will mean that only more representative features will be taken into consideration, but less information will be available during the identification process.

As an example to illustrate the general operation of this method, a hypothetical three-feature (fea1, fea2 and fea3) biometric-based identity prediction task is considered. The soft-biometric information of the user is known and is recorded as either "X" or "Y" (these labels representing appropriate values depending on the particular instance of soft biometric information. For instance, for gender the labels will be "male" and "female").

One classifier is trained with all users for which the soft-biometric information is "X" and with all the users for which the soft-biometric information is "Y" using all the features (fea1, fea2 and fea3) and generates two confidence degrees: cdVal_{X} and cdVal_{Y} respectively.

Then, the system is tested with samples from the validation set which are from users of the group "X" in the following combination:

- fea1 and fea2 generating cdVal_{fea3,X}.
- fea1 and fea3 generating cdVal_{fea2,X}.
- fea2 and fea3 generating cdVal_{fea1,X}.

Once the confidence degrees are calculated, the diff values are calculated as follows:

- \( \text{diff}_{\text{fea3}} = \text{cdVal}_{\text{fea3},X} - \text{cdVal}_{X} \).
- \( \text{diff}_{\text{fea2}} = \text{cdVal}_{\text{fea2},X} - \text{cdVal}_{X} \).
- \( \text{diff}_{\text{fea1}} = \text{cdVal}_{\text{fea1},X} - \text{cdVal}_{X} \).

These diff values will be compared with a threshold value (defined by the designer/operator of the system). If there is any gain in accuracy with respect to the feature-dependent error rates, then this feature is seen to improve performance. The information stored in the Knowledge Database module (Figure 3.10) will be the list of features which should be used when a user which belongs to a specific soft-biometric category is tested.
CHAPTER 3. MULTICATEGORY APPROACH

3.5 Using predicted soft-biometrics

By assuming that the users will provide any information necessary for the identification process, the system designer risks being given wrong information either by mistake or as an attempt deliberately to circumvent the use of the system. The natural step to overcome this problem is to use only the biometric data collected from the sensor and use it to predict all the other information which would be necessary for the identification.

This section therefore introduces some new ideas on how to obtain the soft-biometric information. Most of the information from predicted soft-biometrics is going to be fused in some way with the predicted identity from the biometric data, this technique being located in the intersection between the multicategory approach and the multiclassifier approach described in the overview set out earlier in Figure 3.7.

3.5.1 Addition of soft-biometric prediction classifiers

In this proposed new approach, the soft-biometric information is predicted using the biometric data which is also used to predict identity. This means that the use of soft-biometric information will be in the Individual Classifiers module, where as well as identity prediction classifiers, soft-biometric prediction classifiers will also be incorporated.

Soft-biometric information, as already explained before earlier, is not a unique identifier of an individual and does not carry enough information to identify a single user when used alone. Nevertheless, even though the idea of using the soft-biometric predicted data combined with the identity predicted data in order to enhance performance might seem not justified, there is indeed gain in doing this extra processing phase. Biometric data is very complex and very often, if appropriately utilised, can produce disappointing results. In the same way that there is potentially a gain in using different classifiers to predict identity from one sample, there is also gain to be made in predicting other information (soft-biometrics, for example) from this same sample. The diversity of opinions generated by this different set of "experts" (classifiers) can give a broader view of the (identity) searching problem, therefore enhancing the final performance rate.

Figure 3.11 illustrates the system structure when using classifiers to predict soft-biometric information.

The base classifiers (for identity prediction and soft-biometric prediction respectively) each process the available input data to give their prediction. In pattern recognition terms, the identity prediction classifiers will classify any input samples as defining one of the enrolled users. On the other hand, the soft-biometric prediction classifiers will classify any input sample as one of the possibilities regarding that specific information. For example, if the soft-biometric is gender, the classifiers will try to classify the input sample as either "male" or "female".

The process in this system can be described as follows:
3.5. USING PREDICTED SOFT-BIOMETRICS

1. The input sample $F$ is extracted from the user in the Feature extraction from the biometrics in the Input Data Processing module (shown in Figure 3.10), where

$$F = [f_1, f_2, f_3, \ldots, f_n]$$

where $n$ is the number of features from the modality.

2. $F$ is sent to the Individual Classifiers module.

3. This feature $F$ will feed both groups of classifiers in the Identity prediction classifiers and soft-biometric prediction classifiers modules.

4. Each classifier inside the Identity prediction classifiers module will produce a vector of confidence degrees as follows:

$$CD_c = [cd_{c,1}, cd_{c,2}, \ldots, cd_{c,y}]$$

where $y$ is the number of enrolled users and $c$ represents the number of the classifier.

5. Each classifier inside the soft-biometric prediction classifiers module will produce a vector of confidence degrees as follows:

$$CD_s = [cd_{s,1}, cd_{s,2}, \ldots, cd_{s,l}]$$

where $l$ is the number of categories for this specific soft-biometric information.

Figure 3.11: System when using soft-biometric prediction approach
and \( s \) represents the number of the classifier. Each classifier will only predict one specific soft-biometric category.

6. Both these vectors \( C_{D_c} \) and \( C_{D_s} \) will be sent to the Classifier Outputs Processing module.

The importance of this type of approach has been generally neglected in the literature. Although there has been some investigation reported on how to predict soft-biometrics, this type of study has not been extensive and is still very poorly researched. The other use of the Soft-prediction classifiers is in the Input Data Processing module as can be seen in Figure 3.12.

![Figure 3.12: System when using soft-biometric prediction approach in the Input Data Processing module](image)

In this approach, the available data can be used either as a feature selector or simply as an extra feature which will be used by the individual classifiers.

Sections 3.5.2 and 3.5.3 will describe how simple fusion techniques, such as Majority vote and sum, can use the soft-biometrics prediction classifier outputs.

### 3.5.2 Majority weighted vote-based fusion method

Majority Voting (Kuncheva, 2004) is a non-linear fusion-based classifier combination method that takes into account only the top outputs of the component experts. The outputs of the classifiers are represented in a winner-takes-all form (for each classifier, the output of the winner is 1 and the remaining outputs are 0) and the weights for all the component experts are equal to 1.
3.5. USING PREDICTED SOFT-BIOMETRICS

A schematic of this fusion-based configuration can be seen in Figure 3.13. After all the features are extracted and sent to the Individual Classifiers module, an adaptation of the general method can be described as follows:

1. Each classifier inside the Identity prediction classifiers module will produce a vector of confidence degrees as follows:

\[ CD_c = \{cd_{c,1}, cd_{c,2}, ..., cd_{c,y}\} \]

where \( y \) is the number of enrolled users and \( c \) represents the number of the classifier.

2. Each classifier inside the soft-biometric prediction classifiers module will produce a vector of confidence degrees as follows:

\[ CD_s = \{cd_{s,1}, cd_{s,2}, ..., cd_{s,l}\} \]

where \( l \) is the number of categories for this specific soft-biometric information and \( s \) represents the number of the classifier. Each classifier will only predict one specific soft-biometric category.

3. In the Classifier Outputs Processing module, only the user and the soft-biometric with the highest confidences will be considered. From that, both Vectorisation modules will generate two vectors:

\[ ID_{\text{winners-identity}} = \{id_{1,\text{winner}}, id_{2,\text{winner}}, ..., id_{c,\text{winner}}\} \]

where \( cd \) is the label of the winner for each identity prediction classifier and \( c \) is the number of identity prediction classifiers,

\[ SB_{\text{winners-soft}} = \{cat_{1,\text{winner}}, cat_{2,\text{winner}}, ..., cat_{s,\text{winner}}\} \]

where \( cat \) is the value of the winner for each soft-biometric prediction classifier and \( s \) is the number of soft-biometric prediction classifiers.

4. The Knowledge Database module provides the respective characteristics of each winner user which is as follows:

\[ SB_{\text{winner-soft-real}} = \{catReal_{1,\text{winner}}, catReal_{2,\text{winner}}, ..., catReal_{c,\text{winner}}\} \]

where \( catReal \) is the real soft-biometric value for each identity prediction classifier winner and \( c \) is the number of identity prediction classifiers.

5. Each identity prediction classifier will "vote" for its winner user and this winner will also receive the votes from the soft-biometric prediction classifiers where its winner is a characteristic from that user.

6. Because the classifiers are voting based on different information (which differs from a traditional voting system, where all the classifiers vote based on
the same information), it is necessary to assign weights to each group of classifiers.

7. The output of this method will be the winner identity label with the majority of votes.

8. When there is a tie, the identity prediction classifier with the greatest confidence provides the output of the system.

The use of soft-biometric information in this context is very interesting and provides another example of how to use additional information which is available in a particular scenario. The use of weights is explained in more detail in Section 3.5.3.

![Figure 3.13: System when using soft-biometric prediction approach](image)

### 3.5.3 Weighted sum-based fusion method

Sum-based fusion (Kittler and Alkoot, 2003) is a linear fusion-based method that takes into account the confidence degree for each class of each classifier. In this sense, when an input pattern is presented to the base classifiers, the degrees of confidence for each class output are added to the other related outputs giving an overall score for that class. The winner class, and hence the identity label of the system, is the class with the highest score.

The same general system structure as for the majority voting approach is used, as shown in Figure 3.13. We also need to adapt this method to our current purpose, as follows:
3.5. USING PREDICTED SOFT-BIOMETRICS

1. In the same way as in the Voting technique, each classifier inside the **Identity prediction classifiers** module will produce a vector of confidence degrees as follows:

\[ CD_c = [cd_{c,1}, cd_{c,2}, ..., cd_{c,y}] \]

where \( y \) is the number of enrolled users and \( c \) represents the number of the classifier.

2. Each classifier inside the **soft-biometric prediction classifiers** module will produce a vector of confidence degrees as follows:

\[ CD_s = [cd_{s,1}, cd_{s,2}, ..., cd_{s,l}] \]

where \( l \) is the number of categories for this specific soft-biometric information and \( s \) represents the number of the classifier. Each classifier will only predict one specific soft-biometric category.

3. Differently from the voting system, in the **Classifier Outputs Processing** module, all the users and the soft-biometric categories will be considered. From that, both **Vectorisation** modules will generate two vectors:

\[ CD_{identity} = [\sum_{i=1}^{c} cd_{c,1}, \sum_{i=1}^{c} cd_{c,2}, ..., \sum_{i=1}^{c} cd_{c,u}] \]

where \( cd \) is the confidence of the each user calculated by the classifier \( c \) and \( u \) is the number of enrolled users,

\[ CD_{soft} = [\sum_{i=1}^{s} cd_{s,1}, \sum_{i=1}^{s} cd_{s,2}, ..., \sum_{i=1}^{s} cd_{s,l}] \]

where \( cd \) is the confidence of the winner for that classifier \( l \) is the number of categories and \( s \) is the number of soft-biometric prediction classifiers.

4. The **Knowledge Database** module provides the respective characteristics of each enrolled user, as follows:

\[ SB_{soft-real} = [catReal_1, catReal_2, ..., catReal_u] \]

where \( catReal \) is the real soft-biometric value for each identity prediction classifier winner and \( u \) is the number of enrolled users.

5. The confidences related to the soft-biometric information will be added to the users which have that characteristic.

6. Because the confidences added are based on different information (which differs from a traditional sum-based implementation, where all the classifiers’ confidences correspond to the same information), it is necessary to assign weights to each group of classifiers.
7. The output using this method will be the label which has the highest confidence degree.

8. When there is a tie, the identity prediction classifier with the greatest confidence provides the output of the system.

The use of soft-biometric information in this context is also very interesting and takes into account even more details than the previously presented method. Here, not only is the opinion of each classifier observed but the confidence with which this classifier is giving its result is also taken into consideration.

Definition of the weights

The weights can be chosen taking into account important information about the quality of the database, the population characteristics and/or can be related to a specific task.

The justification for using these classifiers with different purposes (identity prediction and soft-biometric prediction) giving them different degrees of importance (weights) is that, in many cases, the least reliable classifier can nevertheless give valuable information about specific samples that the most reliable classifier might struggle to supply by themselves.

The idea is that each group of classifiers will have a degree of confidence or relative importance with respect to a specific identification task. Analysing this importance has to consider the characteristics of the database (information about the target population, for example) and the effects of including soft-biometric information in the classification is very important.

3.6 Some experimental results and general remarks

The investigation reported in this chapter aims to evaluate the impact of adding additional non-biometric information to biometric-based systems considering the division of approaches presented in Figure 3.7.

In order to show the effectiveness of these different techniques, an experimental analysis is carried out comparing results using the BioSecure database (described in Section 2.5) applied to the techniques presented in this chapter as well as some traditional fusion techniques.

All the techniques presented in this chapter as well as the traditional techniques which will be used as comparison are performing identity prediction. In general, the techniques and variations which are investigated experimentally as well their parameters empirically chosen can be listed as follows:

- Proposed methods for identity prediction:
  - Soft-biometric as an extra input feature using as the fusion method traditional vote and sum approaches (which will be designated as SB-ExtraInput-Vote and SB-ExtraInput-Sum, respectively).
Soft-biometric as feature selector using as the fusion method traditional vote and sum approaches (which will be designated as SB-FeatureSelector-Vote and SB-FeatureSelector-Sum, respectively) and using the threshold as 10.

Predicted soft-biometric using the majority weighted vote fusion method (designated as Pred-SB-Weighted-Vote), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.

Predicted soft-biometric using the weighted sum fusion method (designated as Pred-SB-Weighted-Sum), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.

- Traditional methods for identity prediction:

  Biometric data only using as the chosen the fusion method traditional vote and sum approaches (designated as No-SB-Vote and No-SB-Sum, respectively).

Also, as a basis for comparison, results from each of the unimodal configurations (in this case: handwritten signature, fingerprint and hand geometry) will be considered for all different system configurations and will be presented in Section 3.6.1. In these systems, all seven base classifiers (explained in Section 2.4) were used for both the identity prediction and soft-biometric prediction classifiers fusion.

As soft-biometric categories and methods for their exploitation are the main topic of this chapter, three soft-biometric categories are selected to be included in the experiments, these are: Age, gender and handedness (as discussed in Section 3.3.1).

Results from different approaches will be presented in two sections. In Section 3.6.1, the results of the multicategory approach only will be discussed as the addition of soft-biometrics for enhancing performance without compromising complexity and the results from predicting soft-biometrics from biometric data. In Section 3.6.2, the intersection between multicategory and multiclassifier approaches will be presented.

### 3.6.1 Multicategory results

The first important task to address is the analysis of the performance of the individual classifiers with the different configurations. Figures 3.14, 3.15 and 3.16 show the identity prediction results (error rates) for the Signature, Hand geometry and Fingerprint databases, respectively. Clearly, there is a gain in performance when simply adding soft-biometric information in the first level of the system. Generally, some useful conclusions can be taken from these results:
• As already noted, in all three cases (Fingerprint, Hand geometry and Signature), there is gain in performance when adding soft-biometric information as an extra input. This is a very valuable result with significant practical implications which points to the fact that even the "least significant" information, when used properly, can (and does) improve biometric systems performance.

• When using selected features, this gain in performance does not always happen. This is because the tuning of the threshold is not an easy task, the value adopted is not ideal and therefore, the characteristic selected (features) are not relevant to a specific modality. This also points to the importance of the correct selection of the soft-biometric information.

• As expected (and mentioned in Section 3.3.1), the soft-biometric with highest impact in the results is the age characteristic. This is likely to happen because the effects of ageing are greater than the difference between gender and between handedness in the population distribution.

• Even more, the use of fuzzy age results in a greater improvement in performance than when using "sharp" age groups. The fuzzy age represents better
3.6. SOME EXPERIMENTAL RESULTS AND GENERAL REMARKS

Figure 3.15: Results for the individual classifiers using the hand geometry database

the smoothness/continuity of the ageing process, and that is the reason for this observed effect.

- The performance of different classifiers (in relation to their sophistication and the base algorithms they use) can be clearly seen in these results. As expected, the results from KNN (the simplest classifier) are the poorest, but when analysing the more complex classifiers, different results occur depending on the modality used. This happens because the more complex classifiers use very specific algorithms which focus on different ways of doing the space search. Because we are using fundamentally different modalities, this difference in the classifier performance is expected.

On the other hand, Figure 3.17 shows the results for soft-biometric prediction for all three databases. When analysing the soft-biometric prediction classifiers, the following observations can usefully be made:

- It is clear (as expected) that the measured performance concerning the prediction of non-biometric information from biometric data is lower than prediction of identity. That can be explained by the fact that different users
belonging to the same group will have very different characteristics. Nevertheless, the measured performance is at least at a level which suggests that it could have real practical value, especially when used, for example, in conjunction with other information.

- The prediction of age showed a higher degree of accuracy than the prediction of either gender or handedness in all three modalities. In the same way as explained before, the age groups are likely to contain specific characteristics which help the classifiers in the class separation. Also, differently from the gender or the handedness, the ageing process is proved to be responsible for substantial changes in the biometric data.

- Despite what is often reported in the literature (see, for example (Metze et al., 2007), (Abreu and Fairhurst, 2008a) and (Thomas et al., 2007)), gender appears to be identifiable not only from the face data, but it is also possible to identify gender from the fingerprint, handwritten signature and hand geometry. The same can also be said about handedness. For example, there are specific signature features which are very much linked with the handedness, such as azimuth and altitude. Also, the hand geometry carries important distinctive characteristics when gender is taken into account.
• Again, the performance of different classifiers can be seen in these results to vary considerably and also, as expected, the results follow broadly the same pattern as was observed for the identity prediction classifiers.

• The signature database presented the best results when compared with fingerprint and hand geometry. The behavioural biometrics naturally inherit more individual characteristics (psychological, for example) than the physiological biometrics. This type of information can create very unstable samples, but, on the other hand, very often provides more detailed information about the user.

These results are dependent on these specific databases but, nevertheless they are strong indicators of how optimisation can be achieved by using simple non-biometric information.

![Figure 3.17: Results for soft-biometric prediction using all databases](image)

3.6.2 Multiclassifier system results

This section will present and analyse the methods which can be described as being applications using concepts from both multiclassifier and multicategory approaches. Figure 3.18 shows the results for the multiclassifier systems for the
individual databases. For simplicity, when soft-biometric information is included, only the base classifiers with the best performance were used in the systems. Some conclusions from the results presented can be drawn as follows:

- Comparing the traditional vote and sum methods with and without the inclusion of soft-biometric information in the base classifiers:

  - As expected, because the inclusion of soft-biometric information improved the accuracy of individual classifiers, it also improved performance based on the fusion of these classifiers.
  
  - The results when the soft-biometric information is used to select the input features were better than when the soft-biometric was used directly as an extra input feature. This happens because unnecessary features were taken away from the process and only important features were used.
  
  - Generally, the sum method produced better results than the vote method in both situations. This is expected because the sum method considers not only which user is the winner but all the confidences in all other users.

<table>
<thead>
<tr>
<th></th>
<th>Signature</th>
<th>Fingerprint</th>
<th>Hand Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB-ExtraInput-Sum</td>
<td>4.99±2.14</td>
<td>5.87±2.14</td>
<td>6.27±3.27</td>
</tr>
<tr>
<td>SB-ExtraInput-Vote</td>
<td>5.09±2.37</td>
<td>5.99±2.29</td>
<td>6.33±3.49</td>
</tr>
<tr>
<td>SB-FeatureSelector-Sum</td>
<td>3.94±2.69</td>
<td>5.06±2.75</td>
<td>5.99±2.51</td>
</tr>
<tr>
<td>SB-FeatureSelector-Vote</td>
<td>4.72±3.26</td>
<td>5.64±3.99</td>
<td>6.33±2.89</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Sum</td>
<td>3.28±3.85</td>
<td>4.97±3.59</td>
<td>5.74±3.04</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Vote</td>
<td>4.21±3.41</td>
<td>5.33±3.26</td>
<td>6.08±3.85</td>
</tr>
<tr>
<td>No-SB-Sum</td>
<td>5.67±3.59</td>
<td>6.09±3.29</td>
<td>6.59±3.64</td>
</tr>
<tr>
<td>No-SB-Vote</td>
<td>5.33±3.91</td>
<td>6.27±3.74</td>
<td>6.74±3.79</td>
</tr>
</tbody>
</table>

Table 3.3: Error rates and standard deviations for the Unimodal MCS

- Comparing the traditional vote and sum approaches without soft-biometric information and the variations of these methods with predicted soft-biometric information:

  - The techniques using predicted soft-biometric information performed considerably better than the fusion method without it. This shows the potential of this approach, and the reasons for not waste any available information.
  
  - The difference in performance among the different modalities is even more apparent when the predicted soft-biometric information is fused. Using the *t*-test (with the information shown in Table 3.3), in all cases the technique using soft-biometric is statistically better than the case when this is not used (as shown in Table 3.4).
Figure 3.18: Results for the unimodal multiclassifier systems
Comparing the traditional vote and sum approaches with two modified vote and sum approaches using predicted soft-biometric information:

- The difference in performance increases when comparing these fusion techniques with and without predicted soft-biometrics. This is an encouraging reason for using soft-biometrics, this data can overcome shortage of information when using one modality.

<table>
<thead>
<tr>
<th>Pred-SB-Weighted-Sum vs</th>
<th>Signature</th>
<th>Fingerprint</th>
<th>Hand Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB-ExtraInput-Sum</td>
<td>7.05E-005</td>
<td>0.016</td>
<td>0.118</td>
</tr>
<tr>
<td>SB-ExtraInput-Vote</td>
<td>4.41E-005</td>
<td>8.77E-003</td>
<td>0.102</td>
</tr>
<tr>
<td>SB-FeatureSelector-Sum</td>
<td>0.081</td>
<td>0.421</td>
<td>0.263</td>
</tr>
<tr>
<td>SB-FeatureSelector-Vote</td>
<td>2.39E-003</td>
<td>0.107</td>
<td>0.081</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Vote</td>
<td>0.036</td>
<td>0.229</td>
<td>0.245</td>
</tr>
<tr>
<td>No-SB-Sum</td>
<td>4.87E-006</td>
<td>0.011</td>
<td>0.037</td>
</tr>
<tr>
<td>No-SB-Vote</td>
<td>1.23E-004</td>
<td>6.48E-003</td>
<td>0.020</td>
</tr>
</tbody>
</table>

Table 3.4: \( p \) values when comparing the lowest error rate with the others in each database

Again, as already noted, these results are dependent on the data used. Nevertheless, the addition of soft-biometric information in the fusion phase has proved to be very successful (Abreu and Fairhurst, 2009c). Moreover, Table 3.5 shows the \( t \)-test comparison between the best signature-based multiclassifier system and the best fingerprint-based and hand geometry-based multiclassifier system. As can be seen, in both cases, the signature database is statistically better, which highlights the fact that signature data contains important characteristics which points to a special advantage of combining soft-biometrics with this modality.

<table>
<thead>
<tr>
<th>Signature vs</th>
<th>Pred-SB-Weighted-Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>7.73E-004</td>
</tr>
<tr>
<td>Hand geometry</td>
<td>5.88E-007</td>
</tr>
</tbody>
</table>

Table 3.5: \( p \) values when comparing the lowest error rate among databases

Even though different databases and modalities were used, the results shown in Table 3.2 (which were found in the literature) are comparable with the ones presented in this section. This is very encouraging and can be considered another indicator that the inclusion of soft-biometrics is able to improve identity prediction.

### 3.7 Chapter conclusions

This chapter has presented some extensive experimental investigation (based on the theoretical new techniques presented in this chapter) and a detailed discussion about a number of important issues concerning the relationships between
biometric solutions in system implementations which involve biometric data and non-biometric data (soft-biometrics), and where many optional configurations can be considered.

More specifically, a number of different new techniques by means of which to include soft biometric information to improve identity prediction accuracy have been introduced. The results presented are very encouraging, and show how additional information which is often available, explicitly collected in practical scenarios or even predicted from biometric data can be exploited in a way which can enhance the identification process. Some general conclusions based on the empirical results presented in this chapter, and some interesting database-related and algorithm-related points can be drawn from these results about the impact in the designing of such system configurations:

- The importance of soft-biometric information is normally underestimated (because this kind of data is not considered distinct enough to be used in security-based applications, as was discussed in Section 3.2). Nevertheless, its incorporation in different fusion algorithms has proved very promising.

- The choice of the soft-biometrics is very much dependent on the modality which is going to be used as well as the population which is going to form the basic user-group for a particular system implementation.

- Relating soft-biometric information with biometric modalities can be straightforward in most causes, but a lot of work needs to be done in the investigation of the details of how the integration of soft-biometric data will affect the performance of a identity prediction system.

- The categorisation of the soft-biometrics (as discussed in Section 3.3.1) is another important factor which the system designer should take into account. This also depends on the population characteristics.

- When comparing results from the three different modalities investigated here, it is interesting to see their relation with the inclusion of the soft-biometrics. All three presented improvements in adding the three different soft-biometrics (age, handedness and gender).

- Also, when resource limitation is a main factor in the system design, it is extremely important to be able to use cheap, easy to collect and well accepted information which can enhance a unimodal system performance.

More importantly, however, is that the work reported offers some practical options to a system designer in seeking to improve error rate performance in unimodal systems (but which can also be applied to multimodal system, as will be explored in Chapter 5), providing alternatives to the increased complexity and reduced usability incurred in multibiometric systems.

The next chapter will explore the multiclassifier approach and will present further possible intelligent system configurations and techniques which can improve
flexibility as well as accuracy in the implementation of biometric-based identification system for practical applications.
Chapter 4

Multiclassifier approach

This chapter will present the second approach introduced by this thesis: the multiclassifier approach. Multiclassifier techniques used in biometric-based systems will be discussed and a more intelligent solution (based on Multiagent systems) is proposed.
4.1 Introduction

The demands of a computational system which deals with pattern recognition efficiently and with high performance has especially motivated the study of machine learning techniques in recent years ((Kittler et al., 1998), (Alkoot and Kittler, 1999) and (Bittencourt et al., 2005)). Despite the fact that many classification algorithms appear to produce satisfactory performance, they are nevertheless often found to fail to generate reliable results in real world tasks (with very complex databases, for instance) (Fumera and Roli, 2005). Thus, while optimising the performance attainable with any single particular classifier remains an important consideration, in order to make significant progress towards improving performance levels, the idea of using the different (often complementary) characteristics of different classifiers within a single task domain started to be considered as a more effective strategy, and the concept of multiclassifier systems (MCS) has become paramount in recent years ((Kuncheva, 2004), (Kuncheva and Rodriguez, 2007)).

Multiclassifier systems can be divided into two categories: Parallel and Modular (Mitchell, 1997). The first category (which can be seen in Figure 4.19) can be described as defining a configuration where all the classifiers in the system perform the same recognition task, each classifier producing its own output for a specific input test sample. A single classifier then decides, based on all these outputs (which can only be given once), what is the overall output of the system. On the other hand, the second category (which can be seen in Figure 4.20) defines a structure where each classifier or group of classifiers is responsible for the classification of a part of the problem. In the same way as in the Parallel category, in the Modular category, the base classifiers will produce their outputs and will send them to a single classifier (again, only once) which will be responsible for deciding what is the overall output of the system.

![Figure 4.19: Parallel approach](image1)

![Figure 4.20: Modular approach](image2)
Multiclassifier systems have been widely used in a range of pattern recognition problems such as speech recognition ((Mukhopadhyay et al., 2003)), writing recognition ((Heutte et al., 2004)), face recognition ((Lee and Sohn, 2007), (Czyz et al., 2004)), multimodal biometrics ((Tronci et al., 2009)), protein classification ((Bittencourt et al., 2005)) and many more.

Regardless of the widespread use and development of multiclassifier techniques (most often focusing on the fusion techniques adopted), the choice of the base classifier components of these systems and especially determining the optimal choice of a combination method which is most suitable for a specific application, is often a difficult process. Indeed, optimisation often requires the execution of exhaustive testing to choose the best implementation (Canuto et al., 2004). The main reason for this is that although a multiclassifier approach can be effective, the final decision-making process will always be based on a limited input from the base classifiers (they do not have a chance of changing their output once the process has started) sent to a unique method (which is normally one single classification algorithm and is referred as the fusion classifier).

Since identifying an individual person by means of the analysis of biometric data is, at its core, one specific application of generalised pattern recognition techniques, this general problem is a very important, even crucial, part of the
design of a practical system. Indeed, a scan of the available literature quickly identifies a large number of surveys about fusion techniques applied to biometrics ((Fierrez-Aguilar et al., 2003a), (Kryszczuk et al., 2007) and (Noore et al., 2007)).

Recalling the overview schematic diagram presented in Figure 1.1, the second approach which will be discussed in this chapter, corresponds to the shaded area shown in Figure 4.21 (and is referred to as the multiclassifier approach).

Most of the work reported in the literature uses fusion techniques (based on the multiclassifier approach) in identity prediction biometric-based systems (some of the relevant references were cited previously and in Chapter 1). However, as already noted, such systems present the problem of limiting the insight or feedback which the base classifier have the potential to provide. One alternative way to make the decision-making process of a multiclassifier system more dynamic, interactive and flexible is to include the base classifiers within an agent-based architecture, where an agent is able to carry out the classification task and make its decision in a more autonomous, distributed and flexible way ((Canuto et al., 2004) and (Abreu and Canuto, 2006)).

Although some research studies have been reported which use intelligent agents to address the problem of identity prediction ((Deravi et al., 2003), (You et al., 2005), (Toh et al., 2004), (Prendinger et al., 2005), (Meshulam et al., 2006) and (Bey et al., 2008)), none of these studies has used the agents to determine the overall output of the system. In seeking to refocus this type of approach using a multiagent classification system to predict identity, two main aspects are addressed, as follows:

1. The internal architecture of the agent and action plan during the communication phase of the system needs to be appropriately structured.

2. The functioning of this multiagent classification system adopts a process as follows:
   
   (a) When a new biometric sample is clamped into the system, all agents predict the sample identity.

   (b) However, instead of providing the outputs to a combination algorithm, the agents "negotiate" with each other in order to reach an optimal agreed identity decision for that sample which takes into account a variety of available information.

   The agent-based system is illustrated schematically as in Figure 4.22. The main difference between this approach and the one presented in Figure 2.2 is the possibility of the agents to have an interactive decision-making process with the elimination of the centralised components. In this sense, rather than having Individual Classifiers, Classifier Outputs Processing and Fusion Classifier modules, the system is instead built around a unique module (Intelligent Classifier Agents module) which will contain a group of intelligent agents.

   In principle, multiagent systems applied in classification scenarios offer a powerful alternative paradigm, allowing the possibility of overcoming the difficulties
4.1. INTRODUCTION

Figure 4.22: System design when using the multiagent approach

involved in efficiently handling the combination problem, since they are structured to make their own decisions about the classification output of the system as well as to change opinions (change the first predicted identity) and persuade the other agents to do the same (Abreu and Fairhurst, 2009a).

This chapter will present and evaluate a range of processing structures which will be used as alternatives to multiclassifier biometric-based systems in appropriate circumstances, and will present some experimental results relating both to multiclassifier unimodal and multiagent unimodal systems, in order to provide some insights into competing options for improving performance in biometric-based system.

Section 4.2 will review the relevant specialised literature in this area (following the introductory review presented in Section 1.3.2 of Chapter 1) and identify the main differences between the various approaches previously reported and the new approaches presented in this chapter. Section 4.3 will present the classifier agent and its internal architecture, describing particularly the internal information flow within the agent. Section 4.4 will present the negotiation techniques used by the agents in our implementation, which will then be discussed in more detail in the subsequent Sections 4.4.1, 4.4.2 and 4.4.3.
4.2 Review of agent-based solutions in biometrics applications

Despite its evident potential advantages, the multiagent classification approach in biometrics has not been extensively investigated to date. Again, following the first high level review presented in Chapter 1 about the use of the multiagent approach in the biometrics field, this Section will present a more detailed specific review of the relevant work.

As a benchmark, because the aim of this chapter is to compare the best fusion techniques with our proposed approach, it is interesting to see the best accuracies that can be found in the literature. This accuracies can be seen in Table 4.6.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Modality</th>
<th>Best accuracies</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Barbu et al., 2006)</td>
<td>face</td>
<td>95%</td>
</tr>
<tr>
<td>(Alonso-Fernandez et al., 2007c)</td>
<td>fingerprint</td>
<td>98.78%</td>
</tr>
<tr>
<td>(Fahmy et al., 2008)</td>
<td>iris</td>
<td>99.8%</td>
</tr>
<tr>
<td>(Garcia-Salicetti et al., 2007)</td>
<td>handwritten signature</td>
<td>95.6%</td>
</tr>
<tr>
<td>(Polat, 2008)</td>
<td>hand geometry</td>
<td>93.3%</td>
</tr>
<tr>
<td>(Goffredo et al., 2008)</td>
<td>gait</td>
<td>96.3%</td>
</tr>
<tr>
<td>(Tuononen et al., 2008)</td>
<td>voice</td>
<td>91%</td>
</tr>
</tbody>
</table>

Table 4.6: Literature results when using multiclassifier systems

In (Deravi et al., 2003), the authors use the agent-based approach in order to deal with the issue of complexity management in multimodal biometric systems. In this context, the agents in the system will handle the multiple authorisation levels, location of data across several repositories, and user interface and performance modification as required by the user or necessitated by the environment. This management-oriented use of the flexibility of agent-based solutions is important in its own right but fundamentally different from the focus of the work reported in this thesis.

Security in network access is addressed in (You et al., 2005) using an approach focusing on efficient and effective personal identification combining techniques in biometrics with the use of mobile agent technology. The approach adopts a hierarchical structure which combines extracted multiple personal features with the speed of mobile agents as a navigational tool in a distributed environment.

In (Chetty et al., 2008), a novel agent-based protocol for computer and network security based on fusion of passwords and facial biometrics for user authentication is proposed. The user identification process using the biometric data (which is stored on a smart card) is performed by a traditional classification technique and the authentication is carried out by a mobile agent coming from a reliable server.

A new solution to make the interface of a speaker recognition system more robust and acceptable is presented in (Hernández-Trapote et al., 2008). In the configuration proposed, there is an agent (referred to as the Embodied Conversational Agent (ECA)) which is visually represented by a robot with the features of
a human being) which will react based on the quality or precision of the sample given by the user. In the test application, the ECA asks the user to speak a different sequence of numbers each time the identification process is initiated.

Relational agents are used in (Schulman et al., 2008), in an Internet environment, to identify different users based on the websites they access, the items they buy and so on. The technique uses both hand geometry and previous saved dialogues in order to authenticate the transactions. In this approach, the agent is configured according to the user’s tastes and behaviour while interacting (i.e. the agent will learn the user’s characteristics) and will create "social bonds" with the user.

In (Bey et al., 2008), fingerprint matching issues (such as high computational processing and multiple samples requirements) are addressed using an agent-based distributed approach (giving greater flexibility and independence). The task is divided among the available local Network resources in order to ensure a fast matching process. Once the biometric sample is collected, the agent will perform a statistical test, select the best suited host and then generate an appropriate work distribution plan.

A combination of a barcode reader and a biometric identification system for payment transactions is presented in (Lu et al., 2009) for use in mobile commerce. In this application, the mobile phone containing barcode readers will scan the products and the biometric adopted will validate the payment. The agent will manage the transaction using stand-alone tools to increase security.

As these typical examples illustrate, most of the work reported in the literature is concentrated in only a few areas of application, such as:

- Managing the transaction between the data acquisition and the identification process with the main objective of increasing security.
- Increasing the usability of biometric-based systems by using a relational agent which can interact with the user during the data acquisition.
- Reported work (one example only) focusing on the management of complexity issues in large scale biometric applications by choosing the most suited host to deal with a specific request.

The novel use of agent-based techniques proposed in this thesis goes beyond managing the biometrics or any other information, but is embedded in the actual decision-making process for identification.

### 4.3 Intelligent agents

In order to understand the use of agent-based technology applied to biometric-based problems, it is important to understand precisely what is an agent and how agent-based configurations work. This section will explain the internal functioning of an agent.
An intelligent agent is a software-based computer system that has autonomy, social ability, reactivity and pro-activeness (Wooldridge, 2002). Agents are entities which can communicate, cooperate and work together to reach a common goal. They interact using negotiation protocols.

Figure 4.23 shows the architecture of an agent. As the main goal of all agents is the same, the general structure for all agents is the same. This agent has four main modules, which are:

- **Controller module**: This receives the user queries and defines the activation order of its internal processes. For instance, this module decides, based on the negotiation result, if it is important for the agent to change its existing result in order to reach a common result.

- **Decision-making module**: This is responsible for reasoning about its knowledge in order to define the best output for a classifier. The main idea of this module is to search for a result, eliminating those which do not fit the existing conditions. Then, it ranks the results in decreasing order, according to a set of evaluation criteria. Finally, it picks the first (best) one and defines this as the correct result.
4.3. INTELLIGENT AGENTS

Figure 4.24: Multiagent-based system workflow
CHAPTER 4. MULTICLASSIFIER APPROACH

- **Negotiation module**: This is responsible for the communication with other agents in order to reach a common result. It builds an action plan for negotiation or uses a previously determined action plan. During the negotiation process, it can be suggested that an agent should change its result. However, has autonomy to decide whether to change or to confirm its current result.

- **Classifier module**: This is responsible for executing the classifier algorithm of the agent. It is beneficial that each agent should have a different classifier structure, thereby providing different results for an input pattern.

The main idea behind the functioning of an agent is that once an input pattern is provided, the **Controller module** passes the required information to the **Decision making module**, which accesses the **classifier module** to produce its output. The **Classifier module** will produce a degree of confidence measure with respect to each enrolled user and this information will be used as a weight in order to provide degree of importance to each output of the agent (remember that each classifier agent will generate an individual degree of confidence to each possible output of the system, therefore, each enrolled user).

The **Controller module** can decide to communicate with other agents in order to reach an agreed result. During the negotiation process, it might be necessary for the agent to change its opinion about its current output or to perform a new decision-making process. Also, an agent may decide to perform the decision making process one more time, analysing other criteria or pattern features or, indeed, not changing the output at all.

The agents can also deal with other issues related with the system itself. For instance, the agents can decide which methods are more reliable when the system receives as input some specific modalities. The possibilities are many when more intelligent and autonomous elements are part of the biometric-based system.

A schematic view of this multiagent-based system can be seen in Figure 4.24. All agents should allow their **Classifier module** to be trained and to negotiate an agreed result for a test pattern. The methods for the production of an action plan will be described in Section 4.4.

It is very important to have in mind the main benefit of this approach. This is an interactive and much more flexible process which differs from the traditional fusion approach by allowing the classifiers (here embedded in the agents) to change opinions, to discuss differences and to take into account the other classifiers (agents) opinions as well as previous "life experience". Therefore, this is an extremely powerful approach which provides new ways of designing biometric-based systems.

### 4.4 Negotiation Methods

The negotiation process embodied in a multiagent approach is of fundamental importance for the functionality of the overall system (Abreu et al., 2005). However, most of the negotiation protocols used in traditional multiagent systems cannot
easily be used in a classification context. For instance, during the negotiation process in an auction system, two agents (buyer and seller) try to agree a common value of a "good". In contrast, two classification agents have to decide to which class an input pattern belongs.

In a multiagent system performing a classification task, each agent can produce a different class label for the same pattern. Changing the value of the output of one agent will not benefit the other agent, as happens in an auction system. In this sense, one agent (or both) will have to change its result and accept the output of the other agent. Two well-known negotiation methods, appropriately adjusted to be suitable for application in a classification task, are evaluated in the work reported here, while two new methods are also proposed. These different methods will be described in Sections 4.4.1, 4.4.2, 4.4.3, and 4.4.4.

4.4.1 Game theory-based approach

The game theory-based negotiation method has been used as a cooperation tool in multiagent systems (Wooldridge, 2002). In game theory, the systematic description of the results can be carried out through the use of strategic games. A strategic game is a game in which a player chooses a plan of action only once and at the same time as his opponent. In order to help the players to make their decisions, a payoff matrix is used, in which each cell represents the payoff values which the players will have in a situation where these actions are chosen. The cell with the highest value is chosen (Orsini and Rizzuto, 2005).

Based on this approach, the game theory strategy has been adjusted to be able to implement a biometric classification task. It is important to remember that each agent is labelling an input sample based on all the enrolled users. Therefore, each agent will give an identity to this input sample.

The negotiation process starts after each agent receives the input sample and assign an identity to it. Then, all agents always have the option of two possible actions, which are the following: keep the chosen identity for the input test sample (keep) or change to the identity chosen by the other agent (change). It is also important to define a payoff measure to fill the matrix, which is based on the confidence of the chosen identity and of the identity to be changed (the chosen identity of the other agent). When an agent chooses to change its chosen identity, its payoff can be calculated as the average between the confidence of the chosen identity and the confidence of the identity to be changed. On the other hand, when an agent keeps its chosen identity, its payoff is the difference between the confidence of the chosen identity and the confidence of the identity corresponding to the alternative choice (Abreu and Canuto, 2006). The formal definition of the corresponding formulae can be seen in Equations 1 and 2 between the negotiation of two agents $a_i$ and $a_j$.

\[ \text{Keep}_{a_i} = Conf_{a_i}[Winner_{a_i}] - Conf_{a_i}[Winner_{a_j}] \] (1)
\[ \text{Change}_{a_i} = \frac{\text{Conf}_{a_i}[\text{Winner}_{a_i}] + \text{Conf}_{a_i}[\text{Winner}_{a_j}]}{2} \] (2)

where:

- \( \text{Conf}_{a_i}[\text{Winner}_{a_i}] \) is the confidence produced by the agent \( a_i \) related to the winner of the agent \( a_i \);
- \( \text{Conf}_{a_i}[\text{Winner}_{a_j}] \) is the confidence produced by the agent \( a_i \) related to the winner of the agent \( a_j \);
- \( a_i \) and \( a_j \) are the classifier agents currently negotiating.

As an example to illustrate the operation of this method, a completely hypothetical three-user (A, B and C) classification task is considered, where pattern vectors containing three attributes (att1, att2 and att3) are used. It is clear that the process is the same independent of the modality used. The presented system is composed of two classifier agents \( (a_1, a_2) \). After the training process of their corresponding classifiers is applied, the following test sample is presented to the agents: att1: 0.7, att2: 0.4 and att3: 0.22.

The classifier module of each agent produces its identity predictions, which will generate the confidence of the agent that its identity label is correct. The confidence of the agents in this example can then be expressed as shown in Table 4.7.

<table>
<thead>
<tr>
<th></th>
<th>( a_1 )</th>
<th></th>
<th>( a_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>User identity</td>
<td>Conf</td>
<td>User identity</td>
<td>Conf</td>
</tr>
<tr>
<td>A</td>
<td>0.90</td>
<td>A</td>
<td>0.56</td>
</tr>
<tr>
<td>B</td>
<td>0.30</td>
<td>B</td>
<td>0.87</td>
</tr>
<tr>
<td>C</td>
<td>0.25</td>
<td>C</td>
<td>0.34</td>
</tr>
</tbody>
</table>

Table 4.7: The confidence of the two agents

In this case, the chosen user identity of \( a_1 \) is A, this having the highest confidence, followed by B and C. The chosen user identity of \( a_2 \) is B, followed by A and C. A payoff value is calculated for each action of the agents. In this example, the \textbf{keep} payoff for \( a_1 = 0.9 - 0.3 = 0.6 \) and for \( a_2 = 0.87 - 0.56 = 0.31 \). Also, the \textbf{change} payoff is \( a_1 = ((0.9 + 0.3)/2) = 0.6 \) and \( a_2 = ((0.87 + 0.56)/2) = 0.71 \). In this sense, a payoff matrix is defined (Table 4.8). In each cell, two values are presented, which represent the new confidence for both agents if this cell is chosen.

As can be seen from Table 4.8, \( a_1 \) can choose both actions and the best choice for \( a_2 \) is the \textbf{change} action. In this sense, the best choice for both is for \( a_1 \) to choose the \textbf{keep} action and \( a_2 \) to choose the \textbf{change} action.

The payoff matrix is most appropriately used by two agents. As the multiagent system proposed allows the use of more than two agents, negotiation then proceeds on the basis of pairwise interaction, dealing with two agents at any one time.
4.4. NEGOTIATION METHODS

Table 4.8: The payoff matrix for this example.

<table>
<thead>
<tr>
<th></th>
<th>(a_1)</th>
<th>(a_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>change</td>
<td>0.60; 0.715</td>
<td>0.60; 0.715</td>
</tr>
<tr>
<td>keep</td>
<td>0.60; 0.31</td>
<td>0.60; 0.31</td>
</tr>
</tbody>
</table>

Usually agents are ranked in an increasing order of confidence and the first two are picked to start the negotiation. This is defined as one round and the winner is then compared to the third agent in a second round. This process continues until there is only one agent. If both agents choose different actions, the agent which has chosen the \textit{change} action is discarded.

Clearly, the agent of the \textit{keep} action is considered the winner and remains in the negotiation process. However, its confidence is replaced by its payoff value of the chosen cell. In the specific example above, \(a_2\) would be discarded and \(a_1\) would continue in the negotiation process.

If both agents choose the same action, they both continue in the negotiation process, but their confidence values are replaced by their payoff values. In all cases, the \textit{change} in the confidence value may modify the chosen identity for the input test of the agent. In this way, the agent decides either to \textit{keep} the chosen identity as winner or to \textit{change} the winner identity.

In relation to its threshold, an agent can decide to leave the negotiation process in the case where its confidence is lower than its threshold. Also, an agent can decide to change, by itself, the winning identity of the input test sample. These decisions are generally based on internal rules and specified individually for each agent, depending on past experience.

4.4.2 Auction-based approach

The auction-based negotiation method is another negotiation protocol that can be modified so as to be adopted for use in a biometric classification task. The auction approach is a method in which a series of rules has to be followed. It can also determine resources and values for a good based on an initial proposal made by one of its participants. This method is popular in the Internet environment, such as in typical buying and selling websites (e.g. eBay, Amazon and so on). This is because the auction can be seen as a commercial transaction in which there is a seller and several buyer agents. An auction process can, in principle, take a considerable amount of time. For instance, an Internet auction can spend days in order to define a winner agent (Wooldridge, 2002).

Unlike the original Auction, in a biometric classification task, all agents are considered as buyers, trying to reach an agreement in relation to the classification of an input pattern. In an analogy with the original sense of an auction process, this is similar to a situation in which all buyers decide to meet in order to define the ideal price for a good in advance of the auction taking place.

As in the previous method, this method also uses the confidence measure as a
basis for its functioning. Once an auction section starts, a cost for each agent is calculated. This cost is based on the sum of the differences between the winner confidence and the confidences related to the chosen users of the other agents. This sum is divided by a constant that will depend on the problem. The formula can be broken-down (for simplicity) into components defined by Equations 3 and 4 as follows:

\[
\text{PartialCost}_{a_i,a_j} = \text{Conf}_{a_i}[\text{Winner}_{a_i}] - \text{Conf}_{a_i}[\text{Winner}_{a_j}]
\]  

\[
\text{Cost}_{a_i} = \frac{\text{PartialCost}_{a_i,a_1} + \ldots + \text{PartialCost}_{a_i,a_N}}{\text{constant}}
\]

where:

- \(\text{Conf}_{a_i}[\text{Winner}_{a_i}]\) is the confidence produced by the agent \(a_i\) related with the winner of the agent \(a_i\);
- \(\text{Conf}_{a_i}[\text{Winner}_{a_j}]\) is the confidence produced by the agent \(a_i\) related with the winner of the agent \(a_j\);
- \(a_i\) is the classifier agent currently negotiating.
- \(N\) is the total number of agents.

The choice of this constant depends on the level of acceptance when an agent disagrees with another agent. A low value, such as a value which will cause a small punishment in the confidence degree of the agent, for example, will produce a slow and less flexible negotiation process, while a high value, such as a value which will cause a big punishment in the confidence degree of the agent, for example, will produce a quick negotiation process.

The agent with the highest cost is considered the loser. The confidences of the chosen user identity of all agents are changed to the difference between the current confidence and its cost. When an agent loses twice in succession, it is discarded from the negotiation. The remaining agent is considered as the winner and the chosen user identity of this agent is seen as the overall chosen user identity (Canuto et al., 2004).

Using the example described in Section 4.4.1, a third agent can be added to the multiagent system. Based on Table 4.7 and the confidence for each identity of the third agent (C = 0.85, B = 0.4 and A = 0.37), cost values for all three agents can be calculated and shown as the main diagonal of Table 4.9.

<table>
<thead>
<tr>
<th>Cost</th>
<th>(a_1)</th>
<th>(a_2)</th>
<th>(a_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a_1)</td>
<td>0.125</td>
<td>0.9 - 0.3 = 0.6</td>
<td>0.9 - 0.25 = 0.65</td>
</tr>
<tr>
<td>(a_2)</td>
<td>0.87 - 0.56 = 0.31</td>
<td>0.084</td>
<td>0.87 - 0.34 = 0.53</td>
</tr>
<tr>
<td>(a_3)</td>
<td>0.85 - 0.37 = 0.48</td>
<td>0.85 - 0.4 = 0.45</td>
<td>0.093</td>
</tr>
</tbody>
</table>

Table 4.9: The cost values for Auction method.
4.4. NEGOTIATION METHODS

The cost value for \( a_1 \), for instance, is calculated as the sum of the cells \( C1,2 \) (0.6) and \( C1,3 \) (0.65) divided by 10 (slow negotiation, so low constant) \( \frac{1.25}{10} = 0.125 \). Cells \( C1,2 \) and \( C1,3 \) are calculated as the difference between the confidence of \( a_1 \) for the chosen user identity and the confidence of \( a_1 \) for the chosen user identity of the corresponding column agent. In this example, \( a_1 \) is considered as the loser and the new confidence values for the chosen user identity of the agents are: \( a_1 = 0.775; a_2 = 0.786 \) and \( a_3 = 0.757 \). As in the previous method, once the confidences of the agents are changed, they may need to choose a different user identity or decide to keep the same user identity. In this example, for instance, the new confidence for identity A of \( a_1 \) makes it still keep identity A as the winner. This process proceeds until only one agent remains in the auction.

As in the previous method, an agent can decide either to change or to keep the winning class. Also, it can decide to leave the negotiation process after each round based on the prevailing internal rules.

4.4.3 Sensitivity-based approach

This section presents the third of the proposed techniques, which is based on an intelligent agent model. This is an adaptation of a game theory negotiation method, which uses the punishment metric to punish an agent when it disagrees with the others and it is called sensitivity because each agent takes into account the "sensitivity" of the other agents regarding the users in the database.

The basic idea underpinning this method is that a decrease in the confidence level of the agents is considered through the use of a sensitivity analysis during the testing phase. This analysis can be achieved by excluding and/or varying the values of an input feature and analysing the variation in the performance of the classifier method. The main aim of this analysis is to investigate the sensitivity of each agent to a certain feature and to use this information in the negotiation process. This analysis is performed with respect to all features of the input patterns in the identity prediction classifier inside the agents.

All agents should allow their classifier module to be trained and to negotiate a common result for a test pattern. A schematic view of this multiagent-based system can be seen in Figure 4.24. An action plan of this method can be described as follows:

1. Allow all the classifiers (which in Figure 4.23 are inside the Classifier Module) in the system to be trained. During the training phase:
   
   (a) Carry out the sensitivity analysis for all the biometric features in each classifier.
   
   (b) Calculate the training mean for all features of each user class;

2. Start the negotiation process by trying to show the other agents that their results are not good ones (in the case when a disagreement occurs), using information about the predicted identity of the users. The best way to do
this is to suggest a decrease in the agent’s confidence level with respect to
the predicted user identity, which can be achieved in the following way:

(a) Calculate the difference between the input biometric feature (test pat-
tern) and the training mean of that biometric feature for all user classes
(users’ predicted identities);

(b) Rank the features in decreasing order of the dissimilarity (from the
least similar feature to the most similar) for each user class;

(c) For the first $N$ features, do the following:

i. Choose an agent and let it choose another agent to "attack" (ne-
gotiate).

ii. Check the class assigned by the attacked agent and the sensitivity
of the corresponding classifier to this feature.

iii. Send a message to the other agent suggesting a decrease (punish-
ment) in the confidence level corresponding to the predicted user
class of that agent;

3. After the negotiation process, the classifier agent with the highest confidence
level is assumed to be the most suitable one to classify the test pattern and
its output is considered as the overall identity output.

It is important to emphasise that once one agent sends a suggestion to decrease
the confidence level of the other agent, the second agent will also send a suggestion
to punish the first agent. Each cycle within which all agents suggest punishment
constitutes a "round". This process proceeds until all $M$ features are seen or when
only one of the agents has non-negative confidence.

The principal idea behind this process is that the more distant a feature is
from the training mean, the higher is the probability that a sensitive classifier
is wrong. This fact is used to suggest a decrease in the confidence degree of an
agent. The punishment value is calculated in the following way.

$$Pun_i = \frac{D_i \times S_i}{R_i \times C_a}$$

where:

- $D_i$: is the difference between the current $i$ feature of the test pattern and
  its training mean for the identity classifier;

- $S_i$: is the sensitivity of the classifier to the corresponding $i$ feature of the
  chosen class for the identity classifier;

- $R_i$: is the ranking of the $i$ feature in its difference from the training mean
  for the identity classifier;

- $C_a$: constants $a$ defines the intensity of the punishments.
Again, the choice of the constant depends on the level of acceptance when an agent disagrees with another agent. In the same way as the previous method, a low value, such as a value which will cause a small punishment in the confidence degree of the agent, for example, will produce a slow and less flexible negotiation process, while a high value, such as a value which will cause a big punishment in the confidence degree of the agent, for example, will produce a quick negotiation process. The sensitivity analysis and the training mean are transformed into rules and constitute the overall domain knowledge base of the classifier agent.

An agent can be asked to change its result. This occurs when the punishment parameter is higher than a threshold during a set of rounds (which is determined by the number of features $M$). Then, an agent can choose an alternative user class (usually a classifier provides a decreasing likelihood list of possible classes to which a pattern belongs) or undertake a new decision making process.

As an example to illustrate the operation of the action plan, the hypothetical scenario of Section 4.4.1 shown in Table 4.7 is used. The sensitivity analysis regarding the two agents $a_1$ and $a_2$ can be seen in Table 4.10.

<table>
<thead>
<tr>
<th></th>
<th>fea1</th>
<th>fea2</th>
<th>fea3</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_1$</td>
<td>7.7%</td>
<td>0.9%</td>
<td>6.2%</td>
</tr>
<tr>
<td>$a_2$</td>
<td>8.0%</td>
<td>3.4%</td>
<td>10.7%</td>
</tr>
</tbody>
</table>

Table 4.10: The sensitivity analysis of the identity prediction classifiers

According to steps 1.(a) and 1.(b) of the action plan, it is now necessary to calculate the training mean for all features of all classes for the enrolled users, which can be seen in Table 4.11.

<table>
<thead>
<tr>
<th>Identity</th>
<th>fea1</th>
<th>fea2</th>
<th>fea3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>0.40</td>
<td>0.50</td>
<td>0.25</td>
</tr>
<tr>
<td>User B</td>
<td>0.20</td>
<td>0.70</td>
<td>0.35</td>
</tr>
<tr>
<td>User C</td>
<td>0.10</td>
<td>0.47</td>
<td>0.46</td>
</tr>
</tbody>
</table>

Table 4.11: The training mean of all features according to the enrolled users

The training mean is independent of the agents because it refers to demographic information related to the overall population distribution. Then, step 2.a requires that the difference (absolute difference) from the testing pattern features and the training mean is calculated (Table 4.12).

<table>
<thead>
<tr>
<th></th>
<th>fea1</th>
<th>fea2</th>
<th>fea3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>0.30 ($=-0.70-0.40$)</td>
<td>0.10 ($=-0.50-0.40$)</td>
<td>0.03 ($=-0.25-0.22$)</td>
</tr>
<tr>
<td>User B</td>
<td>0.50 ($=-0.70-0.20$)</td>
<td>0.30 ($=-0.70-0.40$)</td>
<td>0.13 ($=-0.35-0.22$)</td>
</tr>
<tr>
<td>User C</td>
<td>0.60 ($=-0.70-0.10$)</td>
<td>0.07 ($=-0.47-0.40$)</td>
<td>0.24 ($=-0.46-0.22$)</td>
</tr>
</tbody>
</table>

Table 4.12: The absolute distance of the test pattern and its training mean for the users
According to Step 2.(b), the features have to be ranked in a decreasing order of difference and this is as follows:

- **Identity prediction decreasing order of distance of the features**
  - User A: fea1, fea2, fea3
  - User B: fea1, fea2, fea3
  - User C: fea1, fea3, fea2

In the first round of steps 2.(c).(i) and 2.(c).(ii), let us imagine that agent $a_2$ starts the negotiation, convincing the other agent ($a_1$) about the correctness of its solution. The chosen identity of $a_1$ is A and fea1 is the least similar feature. Also, the sensitivity of $a_1$ to fea1 is 7.7% and its difference to the training mean of class A is 0.30. Thus, because of this, the punishment regime will consider this information. Using equation 5, the punishment, using a constant = 10 (which will generate a slow punishment) is shown below.

$$Pun_{a_1-fea1} = \frac{0.30+0.077}{3*10} = 0.00077$$

This value is therefore suggested to be subtracted from the confidence of $a_1$ about user A. Its new confidence for user A will consequently be 0.89923 (=0.90-0.00077). The number of rounds progresses until either all features have been analysed or until only one of the agents has a non-negative confidence for a number of rounds.

### 4.4.4 Sensitivity-based approach using soft-biometrics

In order to investigate how the idea of using soft-biometrics in a fusion technique of a biometric-based system can enhance performance without having to add a new modality, the methods presented in Sections 3.5.2 and 3.5.3 were proposed. Continuing this line of thinking and still investigating the possibilities in this approach, an adaptation of the sensitivity methods is presented in this section.

As already discussed in the previous section, originally, this method was based only on identity classifier agents. However, in this adaptation, the aim is to incorporate soft-biometric classifiers to help the agents make their decision and thus refine the decision-making process.

In the **Classifier Module** there will not only be identity prediction classifiers, but soft-biometric prediction classifiers as well. Some modifications in the overall process can be listed as follow:

- The sensitivity analysis is performed not only with respect to all features of the input patterns in the identity prediction classifier in the agents but in the soft-biometric prediction classifier. The step 1.(a) will be performed with respect to all classifiers.
In the negotiation process, the agents will try to show the other agents that their results are not good ones, using both information about the predicted identity and information about the soft-biometric information related to the predicted identity.

In step 2.(b), the same ranking of the dissimilarity of the features between the test samples and the training mean is carried out for the soft-biometric classifiers.

In step 2.(c), however, there will be an extra step, after the step 2.(c).(ii) which will be as follows:

- Check the soft-biometric information related to the predicted identity.

If there is evidence in the soft-biometric classifiers that the agent is wrong, using the same idea of feature sensitivity, this information is used in the punishment. A modification is made in Equation 5, in order to take into account the soft-biometric prediction information. The new punishment value is calculated according to Equation 6.

\[
P_{\text{uni}} = \frac{D_i \ast S_i}{R_i \ast C_a} + \sum_{j=1}^{n} \frac{D_{j,i} \ast S_{j,i}}{R_{\text{soft},i} \ast C_{mb}}
\]

where:

- \(D_i\): is the difference between the current \(i\) feature of the test pattern and its training mean for the identity classifier;
- \(D_{j,i}\): is the difference between the current \(i\) feature for the current winner class \(j\) of the test pattern and its training mean for the soft-biometric classifier;
- \(S_i\): is the sensitivity of the classifier to the corresponding \(i\) feature of the chosen class for the identity classifier;
- \(S_{j,i}\): is the sensitivity of the classifier to the corresponding \(i\) feature for the current winner class \(j\) of the chosen class for the soft-biometric classifier;
- \(R_i\): is the ranking of the \(i\) feature in its difference from the training mean for the identity classifier;
- \(R_{\text{soft},i}\): is the ranking of the \(i\) feature in its difference from the training mean for the soft-biometric classifier;
- \(C\): constants \(a\) and \(mb\) define the intensity of the punishments.
- \(n\): is the number of soft-biometric classifiers that do not agree with the attacked agent.
Once again, the constants $C_a$ and $C_{mb}$ will depend on the level of acceptance when an agent disagrees with another agent. A low value, such as a value which will cause a small punishment in the confidence degree of the agent, for example, will produce a slow and less flexible negotiation process, while a high value, such as a value which will cause a big punishment in the confidence degree of the agent, for example, will produce a quick negotiation process.

The sensitivity analysis and the training mean, along with further environmental information related to the soft-biometric prediction classifiers are transformed into rules and constitute the overall domain knowledge base of the classifier agent.

Using the same example from Section 4.4.3, the hypothetical scenario of Section 4.4.1 shown in Table 4.7 may be considered further. In order to include the soft-biometric information in the negotiation, two agents ($a_{s1}$ and $a_{s2}$) which will perform gender prediction are introduced. In this case, the two possible classes will be Female and Male. The sensitivity analysis regarding two soft-biometric prediction agents $a_{s1}$ and $a_{s2}$ can be seen in Table 4.13. The sensitivity analysis of the identity prediction classifiers can be seen in Table 4.10.

| $a_{s1}$ | 5.3% | 6.9% | 0.98% |
| $a_{s2}$ | 4.6% | 9.0% | 2.37% |

Table 4.13: The sensitivity analysis of the soft-biometric prediction classifiers

According to step 1 of the action plan, it is now necessary to calculate the training mean for all features of all soft-biometric classes, which can be seen in Table 4.14.

<table>
<thead>
<tr>
<th>Gender</th>
<th>fea1</th>
<th>fea2</th>
<th>fea3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>0.84</td>
<td>0.73</td>
<td>0.75</td>
</tr>
<tr>
<td>Male</td>
<td>0.61</td>
<td>0.88</td>
<td>0.91</td>
</tr>
</tbody>
</table>

Table 4.14: The training mean of all features according to the soft-biometric classes

As already noted, the training mean is independent of the agents, and in this case, step 2.(a) requires that the difference (absolute difference) from the testing pattern features and the training mean is calculated. The effects of this can be seen in Table 4.15.

<table>
<thead>
<tr>
<th>$\text{Female}$</th>
<th>fea1</th>
<th>fea2</th>
<th>fea3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.14 (=-0.84-0.70)</td>
<td>0.33 (=-0.73-0.40)</td>
<td>0.53 (=-0.75-0.22)</td>
</tr>
<tr>
<td>$\text{Male}$</td>
<td>0.21 (=-0.61-0.40)</td>
<td>0.18 (=-0.88-0.70)</td>
<td>0.69 (=-0.91-0.22)</td>
</tr>
</tbody>
</table>

Table 4.15: The absolute distance of the test pattern and its training mean for the soft-biometric classes

According to step 2.(b), the features have to be ranked in a decreasing order of difference and this is as follows:
• **Identity prediction decreasing order of distance of the features**
  - User A: fea1, fea2, fea3
  - User B: fea1, fea2, fea3
  - User C: fea1, fea3, fea2

• **Gender prediction decreasing order of distance of the features**
  - Female: fea3, fea2, fea1
  - Male: fea3, fea1, fea2

In the first round of steps 2.(c).(i) and 2.(c).(ii), again, let us imagine the identity prediction agent \( a_2 \) starting the negotiation process, convincing the other identity prediction agent \( a_1 \) about the correctness of its solution. The chosen user identity of \( a_1 \) is A and fea1 is the least similar feature. Also, the sensitivity of \( a_1 \) to fea1 is 7.7% and its difference to the training mean of class A is 0.30. Furthermore, both the gender prediction classifiers report that the user to whom the sample belongs is female and that user A is male. Thus, the punishment regime will need to take account of this information. Using equation 6, the punishment calculation, using the same constant which produces a slow punishment \( (10) \) as in the previous example, is as shown in the following equation.

\[
Pun_{Ag1-fea1} = \frac{0.30 \times 0.077}{3 \times 10} + \frac{0.21 \times 0.053}{3 \times 10} + \frac{0.21 \times 0.046}{3 \times 10} = 0.001393
\]

A new value is suggested to be subtracted from the confidence of \( a_1 \) about user A. Its new confidence for user A will consequently be 0.898607 \( (=0.90-0.001) \). It is important to notice the difference in the punishment procedure when using this method compared with the previous case. Including soft-biometric prediction agents, indeed, gives more information and consequently more power to the punishment process.

### 4.5 Some experimental results and general remarks

The investigation reported in this chapter aims to evaluate the impact of having a more intelligent approach to solving the centralised problem potentially affecting most of the common multiclассifier fusion techniques.

As was reported for the work presented in Chapter 3, an experimental analysis is carried out comparing results using real biometric data using both these techniques and the traditional techniques.

The techniques and various configurations which are considered in this experimental study as well their parameters empirically chosen can be listed as follows:

• Proposed negotiation methods for identity prediction:
  - Game theory-based negotiation method (**Game**).
– Auction-based negotiation method (Auction) with a threshold of 50.
– Sensitivity-based negotiation method (Sensitivity) with $C_a$ of 100.
– Sensitivity-based with soft-biometrics negotiation method (Sensitivity-SB) with $C_a$ of 100 and $C_{mb}$ of 500.

• Proposed multiclassifier methods for identity prediction:
  – Predicted soft-biometric using the majority weighted vote fusion method (designated as Pred-SB-Weighted-Vote), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.
  – Predicted soft-biometric using the weighted sum fusion method (designated as Pred-SB-Weighted-Sum), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.

• Traditional methods with and without soft-biometrics for identity prediction:
  – Soft-biometric as feature selector using as the fusion method traditional vote and sum approaches (which will be designated as SB-FeatureSelector-Vote and SB-FeatureSelector-Sum, respectively) and using the threshold as 10.
  – Soft-biometric as an extra input feature using as fusion method traditional Vote and Sum (SB-ExtraInput-Vote and SB-ExtraInput-Sum, respectively).
  – Biometric data only using as fusion method traditional vote and sum (No-SB-Vote and No-SB-Sum, respectively).

Again, unimodal results using the three databases: handwritten signature, fingerprint and hand geometry, will be considered for all different system configurations. The soft-biometric categories used in the Sensitivity-SB technique are the three presented in Chapter 3: Age, gender and handedness. Again, in these systems, all seven base classifiers (explained in Section 2.4) were used for both the identity prediction and soft-biometric prediction classifiers fusion.

4.5.1 Multiagent unimodal results

This section will analyse the results from the individual base classifiers methods compared with the Multiagent unimodal system results as well as the different negotiation methods based on unimodal results.

As the databases used in these experiments are the same as those used in the work reported in Chapter 3 and the results from the base classifiers for the individual databases were presented and discussed in that chapter, only a comparison
4.5. SOME EXPERIMENTAL RESULTS AND GENERAL REMARKS

with these results and the proposed multiagent approach is going to be presented here.

From Chapter 3, Figures 3.14, 3.15 and 3.16 show the identity prediction results for the Signature, Hand geometry and Fingerprint databases, respectively. In the present chapter, Figure 4.25 shows the unimodal multiagent results.

- Comparing the results from the unimodal multiagent systems with its base classifiers (without soft-biometric information):
  - Obviously, the base classifiers have a lower performance than when used in a multiclassifier approach as a multiagent system.
  - In the same way as in the previous approach, the difference between the accuracy from base classifiers and multiclassifier systems is, unsurprisingly, significant. Nevertheless, when observing the multiagent approach, this difference is much larger (around 10% of improvement) than what was found in the previous case.

- Comparing the results from unimodal multiagent system with the classifiers using soft-biometrics information:
  - The base classifiers using soft-biometric information (either as an extra input or as a feature selector) presented better results than those without, and still the difference between these results with multiagent systems is around 8%.

It is always important to compare individual classifier performance with any fusion technique, because it gives a measurement of improvement which can be significant or not. In this case, the improvement, although expected, was very significant. Comparing the proposed negotiation methods, it can be said that the multiagent unimodal systems presented some very interesting results.

- The best result is achieved with the Sensitivity-SB negotiation method. The use of soft-biometrics information has once again been demonstrated to lead to a surprising enhancement of performance.

- Both the adaptations of the game theory approaches (Sensitivity and Sensitivity-SB) generated a better result than the game theory. This is explained by the fact the modified methods utilise more information in their negotiation process such as the sensitivity of the different features of each user. This type of information is very important in order to evaluate the validity of the confidence of a specific agent to a input test sample.

- And the Auction negotiation method generated the highest error rate, which is expected because its agents use the least amount of information during the negotiation.
Figure 4.25: Results for the unimodal multiagent systems
Moreover, when the \textit{t-test} is performed between the best multiagent system (\textbf{Sensitivity-SB}) and the other three, it can be said that the \textbf{Sensitivity-SB} is statistically better than \textbf{Auction} and \textbf{Game}. These results can be seen in Table 4.17.

Overall, the results attainable using the negotiation techniques are very good when using only one modality. However, in order to have a better understanding of the impact of these results, it is necessary to compare the results with traditional fusion techniques.

- Analysing the results from the multiagent unimodal systems compared with the multiclassifier unimodal systems:
  - The performance achieved with the multiagent unimodal configuration is around 2\% higher than the performance of the multiclassifier solutions.
  - Particular characteristics of agents (their knowledge of the environment, of each other and their capability for intelligent interaction) provide an acceptable explanation of these improved results.
  - Although differences may at first sight appear to be modest, when the statistical test is performed (using the data from Table 3.3 and Table 4.16), it can be seen that all the multiagent unimodal configurations are statistically better than the equivalent multiclassifier unimodal configurations. These results can be seen in the last row of Table 4.17.

<table>
<thead>
<tr>
<th></th>
<th>Signature</th>
<th>Fingerprint</th>
<th>Hand Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction</td>
<td>3.46±2.23</td>
<td>4.01±2.78</td>
<td>4.36±2.30</td>
</tr>
<tr>
<td>Game Theory</td>
<td>3.25±3.44</td>
<td>3.96±3.44</td>
<td>4.05±2.59</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>2.47±3.17</td>
<td>3.05±3.29</td>
<td>3.25±2.61</td>
</tr>
<tr>
<td>Sensitivity-SB</td>
<td>1.98±2.14</td>
<td>2.97±3.59</td>
<td>2.74±3.13</td>
</tr>
</tbody>
</table>

Table 4.16: \textit{Error rates and standard deviations for the Unimodal MAS}

<table>
<thead>
<tr>
<th></th>
<th>Signature</th>
<th>Fingerprint</th>
<th>Hand geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction</td>
<td>1.67E-006</td>
<td>0.012</td>
<td>2.27E-005</td>
</tr>
<tr>
<td>Game</td>
<td>9.94E-004</td>
<td>0.024</td>
<td>7.38E-004</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>0.101</td>
<td>0.435</td>
<td>0.106</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Sum</td>
<td>1.77E-003</td>
<td>5.66E-005</td>
<td>3.94E-011</td>
</tr>
</tbody>
</table>

Table 4.17: \textit{p – values when comparing the lowest error rate with the other ones in each database}

Finally, when comparing the best signature-based multiagent system with the other two databases, based on the results of the \textit{t-test} shown in Table 4.18, it can be said that the signature is statistically better than both the other two cases.
Table 4.18: \textit{p – values when comparing the lowest error rate among databases}

<table>
<thead>
<tr>
<th>Signature vs</th>
<th>Sensitivity-SB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>9.41E-003</td>
</tr>
<tr>
<td>Hand geometry</td>
<td>0.023</td>
</tr>
</tbody>
</table>

The unimodal results for the multiagent systems presented already point to a very encouraging level of performance. Also, even though different databases and modalities were used, the results shown in Table 4.6 (which were found in the literature) are comparable with the ones presented in this section. The experiments reported demonstrate that by exploiting even a very small amount of additional information, but in an intelligent way, can significantly improve performance, offering the possibility of utilising a much simpler and user-friendly system configuration than if a structure based on several different modalities were adopted.

4.6 Chapter conclusions

This chapter has introduced and discussed some new ways of dealing with the centralised problem of traditional fusion techniques that have been applied to biometric-based systems. Several ways of improving flexibility and making better use of a range of available information from the user have been discussed.

More specifically, four different multiagent negotiation methods were presented. As was found when considering the multicategory approach, the results presented in this chapter are very encouraging, and show how using more intelligent ways of managing information, and also by exploiting the soft-biometrics information often already available, can improve the identification process without necessarily increasing the system complexity.

Following the pattern of the previous chapter, some general conclusions based on the empirical results presented in this chapter, and some interesting algorithm-related points, can be drawn which can increase the impact in the design of more intelligent system configurations:

- Using a more interactive solution (by eliminating the fusion module) to deal with the identification process is clearly not always the most effective processing structure. Biometric data is very distinct and usually used in real-world applications which would benefit highly by using a more intelligent approach.

- The simplest of the negotiation methods presented the highest error rates, but even this still presented better results when compared with the most complex or the one with the lowest error rate of the multiclassifier systems.

- The results regarding each database are very interesting. Despite what might have been expected, the hand geometry and the fingerprint-based experiments produced very similar results.
When the soft-biometric information is included, the improvement is not substantial. Therefore, in this type of system, the inclusion of additional information does not make as big an impact as when it is added in traditional fusion methods because the interactive process already gives the agents many opportunities to maybe change their opinion about their own outputs and this alone is already a big improvement.

Once more, the work reported here offers some more practical options to a system designer in seeking to improve error rate performance in unimodal systems (but which again can be applied to multimodal, as will be explored in Chapter 5), providing alternatives to the increased complexity and reduced usability incurred in multibiometric systems.

As already mentioned before, using a more flexible, autonomous and interactive approach where the components of the system have a memory (in this case a multiagent solution) move the whole decision-making identification process closer to a real world situation where human specialist would try to provide identity by analysing an input test sample.

The next chapter will explore the multimodal approach and will present a discussion about the comparison of different modalities and the reasons they should be combined. A special emphasis is given to the case of the handwritten signature, and the results observed will show that this is a more reliable modality than has sometimes been suggested.
Chapter 5
Multimodal approach

This chapter will present the third approach introduced by this thesis: the multimodal approach. The use of multimodal systems as well as the modalities mostly used will be discussed. A more detailed study will be presented focused on the use of the handwritten signature in a multimodal processing environment.
5.1 Introduction

It has been increasingly recognised that no single biometric modality is universally optimum in dealing with all the challenges arising from any biometric-based system requirements (Ross and Jain, 2004). In order to overcome this problem, the idea of using more than one modality combined (into what is termed a multimodal system) to increase performance has become established as an approach to address this issue. In this context, the term "multimodal" refers to all applications in which more than one biometric modality is used in combination for the identification/verification of an individual.

Building a system around a configuration which can consider identity evidence drawn from more than one biometric source offers a number of potential advantages over a system which relies on only a single source and, indeed, it is often necessary to trade off different factors in choosing an appropriate modality for a given application (Jain et al., 2006).

Moreover, the simultaneous availability of multiple modalities offers flexibility to the user, since there is then, at least in principle, a choice available in a situation where a user either cannot or does not wish to give a sample in a particular modality. Thus, a multimodal biometrics approach combines the advantages of greater robustness, user choice, and an inherent exception handling option all in one package (Fierrez-Aguilar et al., 2003b).

Even more important (according to the bulk of work reported in the literature), exploiting a broader range of identity information (mostly from physiological modalities, such as fingerprint, iris and face) should offer improved levels of accuracy, while also increasing the resilience of a system to, for example, spoofing attacks, where an impostor will need to reproduce a wider range of false biometric data for a successful attack (Jain et al., 2008).

Nevertheless, the potential benefits of a multimodal solution to many practical problems is also accompanied by a number of disadvantages that are not always fully assessed. A range of different issues can be very challenging during this type of system design, such as:

- There are still choices to be made about which, and how many, modalities to include in a particular system. There are a number of "fashionable" modalities which tend to be an easy choice in many cases, even though these modalities may not be the most well accepted by all the users or the best suited to a given situation. Some modalities are popular because they are easy to collect, or simply because they have acquired a reputation as "strong" biometrics. Behavioural biometrics are particularly discriminated against in many such applications, sometimes on the basis of perceived poor performance rather than hard data. The handwritten signature is a good example of a modality which has sometimes suffered from such a reputation, even though it offers many advantages in terms of user convenience.

- Optimising the error rate performance of a multimodal biometric system is not always straightforward, and there is a growing literature which shows
what a difficult problem this can be in practice. Also, choosing inappropriate modalities makes this process more complicated ((Toh et al., 2004), (Snelick et al., 2003) and (Faundez-Zamuy et al., 2006)).

Figure 5.26: Various approaches to the problem: Focusing on the multimodal approach

- Evaluation databases are often small, few in number, and often skewed in relation to the ultimate target population, which often makes any claims about achievable performance statistically weak. Failure in choosing the best suited modalities to specific applications is a major weakness for most of the systems.

- Another difficulty is the effect which a multimodal implementation can have on the usability of a system, both from an end-user perspective and from the viewpoint of a system designer. User interaction should be a prime concern, for a variety of reasons, not least because poor interaction can lead to poor quality raw biometric data being collected (e.g. poor image quality post capture), but also because acceptability to intended user is often a prerequisite for successful uptake.

- Enrolment can be a problem, bringing the added complexity of having to donate multiple samples, where each separate donation interface carries with it an overhead in terms of cognitive load and additional interaction complexity.
There is also the issue that requiring multiple samples, generally using different sensors and interaction strategies, can impose a significant time penalty on each user interaction, which in some time-critical applications can render a multimodal biometric solution non-viable.

In many situations, therefore, when focusing on the multimodal approach, the system designer is presented with an even greater challenge than when focusing on either the multicategory or the multiclassifier approaches, such as have been described in detail in the two previous chapters.

In this chapter, an analysis of the existing options for multimodal systems is presented. Advantages and disadvantages of commonly adopted (both physiological and behavioural) modalities will be presented pointing to the applications and situations for which each of this is the best suited.

In order to illustrate some of the general issues which are important to the overall work reported, but which will also show how some modalities which have traditionally received, relatively speaking, little exposure, can be seen actually to have considerable merits in practice, the handwritten signature is chosen as a case study. The benefits of using this modality as well as the effects when considering all its particular demographically characteristics, will be presented. Experimental results based on the combination of the three explored databases (handwritten signature, fingerprint and hand geometry) used in this thesis will be reported.

Section 5.2 will present the advantages and disadvantages of each of the main modalities showing important related work regarding choosing the modalities to be incorporated in a multimodal system. Section 5.3 will present qualitative reasons for using the handwritten signature as part of a wider configuration. Section 5.4 will present some interesting results which point to some general issues worthy of future development and Section 5.5 will present some conclusions from this chapter.

5.2 Choosing the modalities: Specialist literature review

The often complex analysis required to choose optimal modalities for an application in the face of conflicting demands of a multimodal system has been one of the major issues with which a system designer can be faced. The basic requirements of a unimodal system become significantly magnified in a multimodal context. Issues such as the following are just a few among the many which have to be taken into consideration:

- System usability:
  - Utilising more than one modality generally means using more than one sensor to collect the required data from the system user. Collecting good quality samples, depending on the modality, can also often be extremely inconvenient.
5.2. CHOOSING THE MODALITIES: SPECIALIST LITERATURE REVIEW

- **User acceptance:**
  - Because many sensors are required, often, the user interaction with the system can be very problematic. Also, in order to collect physiological modalities (which the literature clearly shows are those most often adopted in practical applications) very precise procedures need to be followed. Usually, these procedures (such as the user having to provide a frontal pose picture when the face modality is used, for example) are not very familiar to most of the users and this alone can cause a rejection of a very powerful modality by a typical population of users.

- **Fusion techniques:**
  - The complexity of the fusion techniques required increases because, in a multimodal environment, the categories of information fused are different.

- **Complementary modalities,**
  - The choice of the modalities used is a critical factor. Demographic characteristics must be taken into account when choosing the modalities, because different modalities can have different degrees of impact on the identification process.

- **Cost limitations:**
  - Increasing the number of modalities will inevitably increase the necessity of requiring different sensors or, at the least, a more powerful sensor which can collect more than one modality simultaneously. It also increases the complexity of the system, thereby demanding more powerful processing units.

- **Time limitations:**
  - Even when it is possible to use one single sensor to collect more than one modality, the processing time (collection time + feature extraction time + identification time) will be in some ways proportional to the number of modalities used.

Following the first high level review presented in Chapter 1 about the choice of the modalities which will be used in the multimodal system, it is accepted that each modality demonstrates specific strengths and weaknesses which will be described and discussed in Sections 5.2.1 and 5.2.2, the first one referring to the main physiological modalities and the second one listing the commonly used behavioural modalities.
5.2.1 Physiological modalities

A biometric modality is characterised as physiological when it is related with any human body metric which is unique, measurable and relatively non-changeable. This type of biometric modality is generally expected to be more stable and is less likely to suffer from psychological influence, being mostly susceptible to environmental or physical influence (such as ageing, for example as prevailing environmental conditions).

Physiological metrics have been used as a key element in biometrics (typical examples are the fingerprint, hand geometry, face and iris), although some are still in very early stages of research (for example, electrocardiogram, palm vein patterns, and ear shape). The most commonly chosen modalities adopted in practical biometrics system design are physiological.

The principal advantages and disadvantages of the more commonly used physiological modalities will be discussed below.

Face

Face is one of the few biometrics which humans use in typical everyday situations to perform identity recognition in a very natural and effective way. Normally, environment feature information is used in the recognition process but, nevertheless, face memory is highly dependent on the viewpoint. Likewise, analysis of facial expressions as well as the integration of demographic and racial characteristics are accomplished in parallel to face recognition (Schwaninger et al., 2007).

From a machine processing/automation point of view, face recognition is a very complex process. Commonly, unless great care is taken in controlling an operating environment, a system must first detect the face in a more general scene, hence normalising any variation in information content arising from distortions such as image translation, scale changes, and in-plane rotation. Many approaches to locating faces are based on weak models of the human face that model facial characteristics in terms of face shape and facial skin texture.

Once a prospective face has been identified in a scene, the feature detection process starts and normally is divided into two parts: face appearance and face geometry. Some of the main challenges in face recognition processes are, for example, to ensure appropriate illumination conditions, take into account head pose and eliminate occlusion of features as far as possible.

However, among the many advantages of using face features as a biometric measure, some of the more important are listed below:

- There is a wide public acceptance for this biometric modality (Theofanos et al., 2008).

- Photographs of faces are widely used in passports and driving licenses where the possession authentication protocol is still based on a photograph used for human visual inspection purposes (Dol et al., 2006).
5.2. **CHOOSING THE MODALITIES: SPECIALIST LITERATURE REVIEW**

- Face recognition systems are among the least intrusive from a biometric sampling point of view (Heseltine et al., 2008), requiring no physical contact, nor even the immediate awareness of the subject (Mpiperis et al., 2007).

- This biometric offers the apparently, at least in theoretical terms, of being available for use with legacy photograph databases, videotape, or other image sources (Bounbarov et al., 2007).

- Face recognition can, at least in theory, be used for screening of unwanted individuals in a crowd, in real time (possible to be captured on-the-move) (Czyz et al., 2004).

- Face recognition systems can be integrated with existing surveillance systems (Prendinger et al., 2005).

- It is a very appropriate biometric identifier for small-scale verification applications (Lahdenoja et al., 2007).

Nevertheless, some disadvantages also accompany this modality, such as:

- Face currently is often found to be a relatively poor biometric for use in a pure identification protocol, and does not always produce high accuracy performance rates (Wang et al., 2007).

- There is sometimes a perceived "criminal" association with face identifiers since this biometric has long been used by law enforcement agencies (the "mugshot" idea), so there may be a certain resistance in this sense on the part of the general public (Liu et al., 2007).

- As already mentioned, pose, illumination and occlusion can cause serious problems for face recognition the systems (Theofanos et al., 2008).

- Spoofing is not difficult even sometimes with disguises, photography or, in more extreme cases, with plastic surgery (Franco et al., 2008).

- Cultural or religious traditions can lead to problems when the face image is used (for example, the use of the burca), so this is not completely inclusive.

**Iris**

The awareness that the iris image is an unique characteristic able to identify its owner is relatively recent when compared to other biometric modalities. Nevertheless, this modality has been shown to be able to achieve very impressive accuracy rates (very often 100%), when acquired properly (Daugman, 2000).

Biometric systems based on iris images for identification are normally divided into three distinct phases: capture of the iris image, segmentation of the iris and recognising the iris. Using a camera, the system captures an eye image suitable
to support iris recognition. Then, the system needs to identify any noise present in the image and select only the important information (Daugman, 2000).

This is a very powerful modality and some of the advantages of its use can be listed as follows:

- The iris is fully developed within 18 months after birth, and is highly protected by eyelashes and the eyelids (Daugman and Downing, 2001).
- The iris features hardly change so that it has higher consistency in that respect compared to other biometric characteristics.
- The changing of pupil size in response to changes in incident light can be used to confirm natural physiology and thus be used as a basis for detecting spoofing attempts (Park et al., 2008).
- Its features are apparently stable throughout life (Daugman, 2003a).
- Its higher uniqueness in shape (high randomness among different subjects) than a face or fingerprints ensures that an authentication system using the iris can be immensely reliable.

On the other hand, this modality should not always be considered the best solution for all applications because of some disadvantages, such as the following:

- It is a small target (1 cm) to acquire from a distance (1 m) (not very reliable for capture on-the-move). Nevertheless, recent research has shown it is increasingly possible to capture viable images on the move (Daugman, 2006).
- It is located behind a curved, wet, reflecting surface which can influence the quality of the image.
- It easily can be obscured by eyelashes, lenses (either from glasses or from contact lenses) or reflections (from glasses) (Daugman, 2006).
- It is naturally partially occluded by eyelids.
- The elasticity of the pupil can help the verification of the liveness of the individual iris, but it can change the quality of the extracted features (Daugman, 2003b).
- Appropriate illumination is an essential key to a good quality iris image.
- The equipment for iris capture may be costly relative to several used in other modalities.
5.2. CHOOSING THE MODALITIES: SPECIALIST LITERATURE REVIEW

Fingerprint

The idea that the fingerprint could be used to identify an individual was first applied in forensic investigation in the late 19th century. The individual "design" of the lines appearing on the tips of the fingers is believed to be unique (Ross et al., 2007). The flows of the lines are called ridges, the space between the adjacent ridges is called a valley and the flows of the ridges that continue or are divided constitute a particular fingerprint (Chikkerur et al., 2007). An ending point is the point at which a ridge ends, and a bifurcation point is the point at which a ridge is divided into two ridges (Alonso-Fernandez et al., 2007c). Such points are called minutiae and are really important information for the classification of an automatic fingerprinting system ((Jain et al., 1997) and (Ross et al., 2002)).

There are several different types of sensors suitable for collecting fingerprints: optical, thermal, capacitive and subcutaneous (Haggerty et al., 2008). This is a well developed and well established modality, since its study has a long history, and its main advantages are:

- Fingerprints are the composition of protruding sweat glands. It is believed, and long experience suggests, that everyone has unique fingerprints. They do not change naturally (Zhang et al., 2001).

- The reliability and stability of fingerprint recognition is high when compared with voice or face recognition methods (Dass and Jain, 2004).

- Because research into the use of fingerprints for person recognition is relatively well advanced, fingerprint recognition equipment is low-priced compared to other biometric system ((Allah, 2005a) and (Allah, 2005b)).

Despite the fact that the fingerprint is a well studied and highly developed modality, there are still disadvantages of adopting it, such as:

- Fingerprint sensors are vulnerable to noise and distortion caused by dirt and sweat (Chen et al., 2005) and (Chikkerur and Ratha, 2005).

- It might be considered an intrusive modality because some people may feel offended about placing their fingers on the same place where many other people have continuously touched (Ross et al., 2005).

- Also, it can be considered a non-inclusive modality, because some people have damaged or eliminated fingers/fingerprints (Khan et al., 2007).

- Regardless of the fact that fingerprints are considered unique, there are cases where individual identity has been mistaken because two different individuals had very similar fingerprints.

- Fingerprints have a long association with criminal investigations and fingerprint databases are held by all police forces and other Government bodies. This can raise privacy issues and civil liberties concerns (Ross et al., 2002).
Hand geometry

Hand geometry is a biometric which identifies users based on the geometric shape of their hand, taking into account measurements such as size of the palm, length and width of the fingers, distance between the knuckles and so on (Dagher et al., 2007).

The development of reliable hand geometry capture devices in the early 1980s has made this modality the first biometric to find widespread computerised use. Hand geometry capture devices measure the individual hand characteristics based on many dimensions and compare those measurements to measurements derived and stored from an enrolment process. The technique remains popular in simple applications such as access control and attendance operations, but is not regarded as suitable for high accuracy or large-scale implementations (Polat, 2008).

The uniqueness of hand geometry is not conclusively proved, which makes fingerprints and iris more reliable modalities to be used in high-security applications. Nevertheless, hand geometry is known to be very reliable when combined with other modalities (Jain et al., 1999).

Some of the significant advantages of hand geometry are listed below.

- It is a simple (one of the easiest to use and administer) as well as inexpensive modality (Jain et al., 1999).

- The features generally used are easier to collect than fingerprints (a good frictional skin contact is necessary to generate a good quality image) (von Hardenberg and Bérard, 2001).

- Hand geometry is not affected by environmental factors, such as dry weather, which can cause the drying of the skin. Also, it has been proved to work in the most extreme atmospheric climates, ranging from very hot to very cold (Amayeh et al., 2006).

- It is considered less intrusive than fingerprints and iris.

- It is a viable technology, it has been researched for a reasonably long time and has shown good development in capture devices (Ong et al., 2003).

- The capture devices are very robust and able to withstand a considerable amount of rough usage from end users, making them especially useful for application in, for example, large factories, warehouses, retail settings, and other challenging operational environments.

- This modality is one of the least susceptible to privacy rights issues mainly because of its simple enrolment and verification procedures.

- The hand shape is a stable biometric whose physical characteristics are not susceptible to major changes (except for natural growth and illnesses such as arthritis, swelling, or deep cuts) (Pavešić et al., 2007).
5.2. CHOOSING THE MODALITIES: SPECIALIST LITERATURE REVIEW

However, a number of disadvantages are associated with this modality, such as the following:

- Because this biometric is not comprehensively established to be unique, it cannot be used by itself in high-security level identification applications (Öden et al., 2001).
- The hand shape changes with the natural growth patterns during childhood, and therefore it is not ideal for this population category.
- It can be challenged by the use of jewelry (rings, etc), limited dexterity (arthritis, etc) and so on (Kumar et al., 2003).

5.2.2 Behavioural modalities

A biometric modality is said to be **behavioural** when it is determined by a unique and specific action carried out by the user. This category of biometrics is considered less stable than the physiological-based measures because behavioural biometrics can be susceptible to influences not only from the changes in body structure and illness but from less controllable factors such as mood changes and mentally stressful situations.

Nevertheless, behavioural metrics have been used in defining biometrics (such as voice, speech, gait, handwritten signature, and so on), although, as with the case of physiological modalities, some are also still in very early stages of research. Behavioural biometrics can be especially attractive in some forensic applications such as tracking individuals from video surveillance, analysing documents and so on.

The principal advantages and disadvantages associated with the more commonly used behavioural modalities will be discussed below.

**Voice**

As is the case with the face, the voice is one of the biometric modalities which most human beings naturally use to recognise other human beings. The basic assumption is that the voice produces singularly characterised acoustic waves and emanations that are interpreted as words and sounds and can be used to identify the individual speaker (Tuononen et al., 2008).

In order to predict identity from the acoustic sounds produced by an individual event, a model that characterises a speaker’s voice must be created. Once this model is created, the verification is carried out by comparing enrolled models with this sample.

Some of the main advantages of voice used as a biometric can be listed as follows:

- Voice is a behavioural characteristic, which has great physiological dependence, but where forgery mechanism have been studied extensively (Markowitz, 2000).
• The enrolment process is fast when compared with many physiological modalities.

• Biometric samples are not expensive to collect and are very easily stored with all sorts of devices available to achieve this (Bredin and Chollet, 2007).

• As a modality, voice has great use in improving the quality of life of, for example, blind people (allows user to operate a computer by speaking to it, for example) (Al-Shboul et al., 2007).

• Because of the previous point, automated voice recognition applications are relatively well developed.

However, being a behavioural modality, the voice modality also creates a number of disadvantages, such as the following:

• This biometric is highly dependent on the language of the user.

• Voice samples generate large templates which can require very high compression rates in practical use (Crescenzo et al., 2007).

• The voice modality suffers a lot with noise interference, normally requiring adjustment to the noise level in the environment (for applications in environments such as: factories, offices, busy households, etc) (Kimm et al., 2007).

• Even when a system is perfectly trained, some words will have to be corrected manually, especially if they are new words, or an individual’s voice changes due to a cold, or if some sudden loud noise interrupts a communication (Prasad et al., 2007).

Gait

The way one walks is very distinctive. Gait recognition is the process of identifying an individual by the way in which they walk (Goffredo et al., 2008). It is a relatively new modality of biometrics and it has been demonstrated in a number of applications to be relatively reliable ((Gafurov, 2007), (Tahmoush and Silvious, 2009) and (Lai et al., 2009)).

It is a relatively unobtrusive biometric and it offers the possibility to identify people at a distance, without any interaction or co-operation from the subject. Therefore, it can be extremely useful in covert identification, for example in particular situations where the individual has a reason for wanting to avoid being no identified. It has been suggested to be a very attractive as a method of identification in some forensic scenarios (Samangoei et al., 2008).

Some of the main advantages of this modality are as follows:

• As already mentioned, this modality requires no contact (in this respect it is similar to, for example, automatic face recognition) and, it has been argued, it is less likely to be obscured than other biometrics. (Gafurov, 2007)
5.2. CHOOSING THE MODALITIES: SPECIALIST LITERATURE REVIEW

- It is captured at a distance which makes it perfect to be used in video analysis (visual surveillance) (Tahmoush and Silvious, 2009).
- Because it is captured from a distance, it is a non-invasive modality.
- Soft-biometric characteristics, such as gender and age, have been successfully predicted from this modality (Ran et al., 2008).

Nevertheless, although a very promising modality, because its investigation is still in an early stage when compared with the more well established alternatives, some disadvantages can be listed, as follows:

- Gait is not highly stable, and can be influenced by (Lai et al., 2009): weight, health condition, emotion, clothes, and shoes.
- Another problem is that most gait recognition algorithms depend on a specific view (Seely et al., 2008).

Handwritten signature

The handwritten signature is the basis of one of the oldest identification methods ever used. The need for a means of document authentication is long established, and the act of signing is associated with this. Handwritten signature verification has therefore been a well established modality for many years, dating to the time when the verification depended only on the skill of human experts (Shanker and Rajagopalan, 2007).

Signature-based identification/verification processes have played a very important role in document forensic analysis (Fairhurst, 2003), and many studies have shown that for particular applications, it can be a reliable modality (Coetzer et al., 2006).

There are two different ways of capturing and analysing handwritten signature data:

1. Off-line or static signatures are scanned from paper documents, where they were written in the conventional way. Off-line signature analysis can be carried out with a scanned image of the signature using a standard camera or scanner (Franke and Köppen, 2001).

2. On-line or dynamic signatures are written with an electronically instrumented device and the dynamic information (pen tip location through time) is usually available at high resolution, even when the pen is not in direct contact with the paper (Jain et al., 2002).

Each of these different approaches has its specific field of application, which makes this modality already a very important and interesting one. Among many of its advantages, some of the more important are as follows:
• The signature is a "man-made" biometric where forgery has been studied extensively (both on-line and off-line) (Franke et al., 2002).

• The enrolment process is intuitive and fast, not demanding the user to do any unfamiliar action (again both on-line and off-line) (Saeed and Adamski, 2005).

• Signature-based verification systems, in general, perform with a fast response time.

• A signature verification system is not dependent on the native language of the user.

• The storage requirements of typical signature templates are generally quite modest (Dyer et al., 2006) and even very high compression rates do not affect the basic signature characteristics or the performance of the signature recognition process (in the case of off-line processing, the storage required is just the image itself which can be highly compressed, and in case of on-line processing, the features captured from the tablet are recorded in pure text form, which allows very efficient storage).

• It is an especially user-friendly modality and well accepted socially, because of its familiarity and the fact that it is a non-invasive (and non-intrusive) modality.

• It has a very high legal importance (Saeed and Adamski, 2005).

• It has long history of use in forensic environments (most of the applications in this particular domain use off-line processing for obvious reasons) (Abreu and Fairhurst, 2009b).

• It is already acquired routinely in a number of applications, even though it may not be used (there is a huge amount of data stored relating to off-line signature which can be used in a database). However, an alternative biometric is often adopted in situations where the signature is ignored (Alonso-Fernandez et al., 2007a).

• The hardware necessary for the acquisition of the handwritten signature is simple and cheap: for off-line capture only an ordinary pen and paper is required, and for on-line capture the required capture tablet is inexpensive and already integrated in some devices (Garcia-Salicetti et al., 2007).

• It is a modality which offers the possibility of "natural revocability" (Teoh and Yuang, 2007), which in a world worried about privacy and identity protection can be very useful.

• Soft-biometrics can be predicted from this modality with relatively high accuracy (Fairhurst and Abreu, 2009b).
5.3. CASE STUDY: USE OF SIGNATURE IN A MULTIMODAL SYSTEM

The advantages are great, but some disadvantages can be found in this modality, nonetheless. Some problems include the following:

- There are still people who cannot write (which makes it non-inclusive in very specific cases).
- Also, a number of individuals have a highly unstable signature which makes the verification process very difficult (Alonso-Fernandez et al., 2007b).
- Skilled forgeries are still a problem, mainly in off-line application (to mimic the geometrical characteristics from a static signature is easier than to mimic the way an individual writes as well as its shape and form).

Section 5.3 will compare the advantages of handwritten signature with a few physiological modalities already presented and show some justification of the benefits which might be available when adopting the handwritten signature in a multimodal system.

5.3 Case study: use of signature in a multimodal system

As already stated, in order to illustrate how important it is to correctly choose the modalities in a multimodal solution, an analysis of the advantages of combining handwritten signature with some of the most commonly used physiological modalities will be presented in this section.

As already noted, the handwritten signature is a very versatile modality and when compared with others, it can be a very powerful option. Very often it overcomes naturally the weaknesses found in other modalities, especially some of those often occurring in a multimodal system, even though the signature is not always considered to be a highly reliable modality.

For example, modalities which have very precise acquisition mechanisms, often fail to capture good quality images. In this sense, poor quality image currently found in such circumstances could be counterbalanced by the addition of signature images which are relatively easy to capture.

The advantages of combining the handwritten signature with other physiological modalities and how the signature can be very useful in a multimodal system will be discussed in Sections 5.3.1, 5.3.2, 5.3.3 and 5.3.4.

5.3.1 Signature and Face

The acquisition of the signature is very simple and considered a very natural action to most people. When combined with signature, bad quality face images producing low performances in isolation can benefit from considerable inverses of accuracy, even when using off-line signature, which usually uses less information.
Another advantage is the prevention of spoofing or any sort of occlusion (such as bad image capture partially or totally occluded images). By using an on-line signature verification process in the multimodal system, it is possible to identify, using dynamic features together with the partial face image, the authenticity of the user and this information.

5.3.2 Signature and Iris

Similarly to the case for face, iris can be a very difficult modality within which to collect samples, the process often generating bad quality images. Therefore, in order to enhance the performance, a multimodal system based on both signature and iris offers the possibility to combine the best of each of these two modalities.

On the one hand, the iris modality can produce very impressive accuracy levels when good samples are available, but these are difficult to collect. On the other hand, signature samples (either on-line or off-line) are very easy to capture, but this modality is known often to show a higher performance variability.

Also on balance, the signature modality requires very little hardware space for sample storage as well as very simple feature extraction software. On the other hand, the iris modality needs much greater storage space and the segmentation phase, essential to a successful practical implementation, can be very complex and challenging.

5.3.3 Signature and Fingerprint

When using the fingerprint modality, the issues to be overcome are slightly different from the two modalities (face and iris) discussed in the previous cases. Users unable to donate a fingerprint sample, or with damaged fingers, are not uncommon and the use of handwritten signature can overcome such potential weaknesses arising in practice.

Also, when taking into account population characteristics, the effects of soft-biometrics (age, handedness or gender, for example) are different in relation to fingerprint and signature. This difference is advantageous in a fusion method in order to improve performance levels.

5.3.4 Signature and Hand geometry

Hand geometry is naturally associated in a general way with fingerprint and in an appropriate set-up could possibly be captured using one only sensor, but they also have very similar weaknesses which makes their combination not necessarily a very attractive proposition.

In the same way as with the fingerprint, population characteristics can be very important when choosing the best modalities to include in a multimodal system. Age and handedness play an even more important role when considering hand geometry.
Again, the less well established uniqueness of the hand geometry can be addressed using the handwritten signature focusing on the dynamic features for authentication (when using on-line) or even just the off-line characteristics.

5.4 Some experimental results and general remarks

A comprehensive analysis of the different available modalities and a careful consideration of their advantages and weaknesses is very important when deciding which modalities to combine in a multimodal system. This section will present some results using the same three modalities that have been the focus of the previous chapters, in order to support some of the statements made about how beneficial handwritten signature (our case study) can be in a multimodal system.

As a matter of comparison, unimodal (handwritten signature, fingerprint and hand geometry) and multimodal (based on the combination of handwritten signature and fingerprint, handwritten signature and hand geometry, fingerprint and hand geometry and the three together) data will be considered for all different system configuration presented in Chapters 3 and 4.

The techniques and various configurations which are considered in this experimental study as well their parameters empirically chosen can be listed as follows:

- Proposed negotiation methods for identity prediction (from Chapter 4):
  - Game theory-based negotiation method (Game).
  - Auction-based negotiation method (Auction) with a threshold of 50.
  - Sensitivity-based negotiation method (Sensitivity) with $C_a$ of 100.
  - Sensitivity-based with soft-biometrics negotiation method (Sensitivity-SB) with $C_a$ of 100 and $C_{mb}$ of 500.

- Proposed multiclassifier methods for identity prediction (from Chapter 3):
  - Predicted soft-biometric using the majority weighted vote fusion method (designated as Pred-SB-Weighted-Vote), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.
  - Predicted soft-biometric using the weighted sum fusion method (designated as Pred-SB-Weighted-Sum), using the weights for identity prediction classifiers as 0.8 and for soft-biometric prediction classifiers as 0.2.

- Traditional methods with and without soft-biometrics for identity prediction (from Chapter 3):
  - Soft-biometric as feature selector using as the fusion method traditional vote and sum approaches (which will be designated as SB-FeatureSelector-Vote and SB-FeatureSelector-Sum, respectively) and using the threshold as 10.
CHAPTER 5. MULTIMODAL APPROACH

- Soft-biometric as an extra input feature using as fusion method traditional Vote and Sum (SB-ExtraInput-Vote and SB-ExtraInput-Sum, respectively).

- Biometric data only using as fusion method traditional vote and sum (No-SB-Vote and No-SB-Sum, respectively).

Again, unimodal and multimodal results using the three databases: handwritten signature, fingerprint and hand geometry, the combination of these modalities two-a-two and the three together will be considered for all different system configurations. The soft-biometric categories used in the Sensitivity-SB technique are the three presented in Chapter 3: Age, gender and handedness. Again, in these systems, all seven base classifiers (explained in Section 2.4) were used for both the identity prediction and soft-biometric prediction classifiers fusion. For the multimodal systems, all seven classifiers for each database are included (i.e. if a multimodal system uses hand geometry and fingerprint, there will be 14 classifiers in it).

First of all, in order to demonstrate the potential advantages of signature as an individual modality, the demographic distribution in the error rates for the individual classifiers using the handwritten signature will be presented in Section 5.4.1 as well as a general analysis of these results. Continuing the analysis for the multimodal systems, Section 5.4.2 will present the multic和平ular multimodal results for the three individual modalities as well as their different combinations. In Section 5.4.3, the multiagent multimodal results are presented for all the combinations as well.

5.4.1 Signature characteristics with age

Figure 5.27 shows the partitioned error rates for the three chosen age bands with respect to each individual classifier for the handwritten signature database. The error rates returned by these classifiers are rather instructive here. First, it is possible to note that the capacity for correctly predicting the identity according to different age groups varies according to the algorithm used. This is a very important information when designing a biometric-based system because the system designer can choose the classifier which will produce the best results according to its population characteristics.

Next, it is useful to analyse performance in greater detail. What is clear from these results is that MLP and SVM generated a greater error rate when they were predicting identity from the "young" age group (< 25). On the other hand, FMLP, RBF, DT and KNN (Jrip is more well balanced in this respect) clearly presented their worst rates of identity prediction for the "elderly" group (> 60). Again, this type of analysis can also be very important during a system design phase as well as the modality choice process, because the target population have to be considered, and making the wrong choices can increase unnecessarily subsequent problems with respect to performance.
It is interesting to note that the most common incorrect prediction for an individual who is actually younger than 25 years would place him/her in the age grouping at the high end of the age range (i.e. in the > 60 group) with approximately half of the probability, errors towards the middle age range accounting for the overall performance difference.

The evidence here suggests that if using handwritten signature and checking age (in this case age added as an extra feature in an identity prediction task) in a scenario where meeting a minimum age requirement at the lowest end of the age range is the principal aim, then there is less to choose in performance between the classifiers than is the case when checking age is carried out against a minimum age at the other end of the age scale. The error categories are also more distinct, and perhaps therefore more easily corroborated by other means when checking in the lower age group.

This is a very good indicator which points to the importance of considering the age characteristics when designing any biometric-based system. Even though these results are strongly related with the database used, the effects of different age groups are still very much highlighted.
Figure 5.28: Results for the multimodal multiclassifier systems
5.4.2 Multiclassifier multimodal system results

This section will compare the results of the unimodal multiclassifier systems (UMCS) with the multimodal multiclassifier systems (MMCS). Figure 5.28 shows the different multimodal combination results using the three modalities adopted for our investigation, as well as the individual database UMCS results.

Overall, UMCS using hand geometry results showed the highest error rates when comparing with the other modalities or the other MMCS results. What is perhaps surprising is that the MMCS using fingerprint and hand geometry sometimes presents a higher error rate than the UMCS using only hand geometry, although performing the t-test (the results of which can be seen in Table 5.20), does not produce any conclusive observation.

On the other hand, when comparing any of the UMCS scenarios with any of the MMCS scenarios using the signature modality, it can be seen that the difference in performance is quite substantial. Performing the statistical test between the best unimodal signature multiclassifier system with the best of all different databases combinations, it can be said that the unimodal signature is statistically better than the combination of fingerprint and hand geometry (based on the data of Tables 3.3 and 5.19 and shown in the last row of Table 5.20).

<table>
<thead>
<tr>
<th>Model Type</th>
<th>Sig + Fin</th>
<th>Sig + Han</th>
<th>Fin + Han</th>
<th>All Three</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB-ExtraInput-Sum</td>
<td>4.16±2.37</td>
<td>4.27±2.93</td>
<td>6.33±2.10</td>
<td>4.09±1.61</td>
</tr>
<tr>
<td>SB-ExtraInput-Vote</td>
<td>4.57±2.84</td>
<td>4.99±2.47</td>
<td>6.87±2.99</td>
<td>4.67±1.99</td>
</tr>
<tr>
<td>SB-FeatureSelector-Sum</td>
<td>3.29±2.69</td>
<td>3.24±2.66</td>
<td>5.34±2.16</td>
<td>3.15±1.72</td>
</tr>
<tr>
<td>SB-FeatureSelector-Vote</td>
<td>3.91±3.61</td>
<td>3.93±2.18</td>
<td>6.07±2.34</td>
<td>3.89±1.89</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Sum</td>
<td>3.01±3.16</td>
<td>2.96±2.39</td>
<td>4.37±2.19</td>
<td>2.94±2.61</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Vote</td>
<td>3.66±3.41</td>
<td>3.47±2.67</td>
<td>5.92±2.13</td>
<td>3.66±3.10</td>
</tr>
<tr>
<td>No-SB-Sum</td>
<td>5.33±3.01</td>
<td>5.27±2.38</td>
<td>7.06±5.91</td>
<td>4.71±2.83</td>
</tr>
<tr>
<td>No-SB-Vote</td>
<td>5.87±2.99</td>
<td>5.33±2.91</td>
<td>7.24±5.78</td>
<td>4.99±2.36</td>
</tr>
</tbody>
</table>

Table 5.19: Error rates and standard deviations for the Multimodal MCS

It is interesting to consider the results obtained from experiments which aim to enhance the processing by incorporating soft biometrics, such as can be seen when we add in the age-based, handedness or gender information as additional identity evidence to the direct biometric data. The improvement in performance which this brings about suggests a very valuable further benefit of an approach which seeks to exploit the availability of soft biometrics as a means of enhancing performance.
Figure 5.29: Results for the unimodal and multimodal for both multiclassifier and multiagent systems
5.4. SOME EXPERIMENTAL RESULTS AND GENERAL REMARKS

Table 5.20: \( p \) – values when comparing the lowest error rate for the multiclassifier with the other ones in each databases combinations

<table>
<thead>
<tr>
<th>Pred-SB-Weighted-Sum vs</th>
<th>Sig + Fin</th>
<th>Sig + Han</th>
<th>Fin + Han</th>
<th>All Three</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB-ExtraInput-Sum</td>
<td>2.01E-003</td>
<td>3.25E-004</td>
<td>3.98E-010</td>
<td>1.16E-004</td>
</tr>
<tr>
<td>SB-ExtraInput-Vote</td>
<td>1.55E-004</td>
<td>7.51E-009</td>
<td>8.20E-011</td>
<td>1.77E-007</td>
</tr>
<tr>
<td>SB-FeatureSelector-Sum</td>
<td>0.250</td>
<td>0.217</td>
<td>9.32E-004</td>
<td>0.251</td>
</tr>
<tr>
<td>SB-FeatureSelector-Vote</td>
<td>0.031</td>
<td>1.53E-003</td>
<td>1.51E-007</td>
<td>1.79E-003</td>
</tr>
<tr>
<td>Pred-SB-Weighted-Vote</td>
<td>0.082</td>
<td>0.078</td>
<td>4.48E-007</td>
<td>0.039</td>
</tr>
<tr>
<td>No-SB-Sum</td>
<td>1.44E-007</td>
<td>4.59E-011</td>
<td>1.53E-005</td>
<td>3.80E-006</td>
</tr>
<tr>
<td>No-SB-Vote</td>
<td>2.12E-010</td>
<td>9.77E-010</td>
<td>3.12E-006</td>
<td>1.11E-008</td>
</tr>
<tr>
<td>Best UMCS signature</td>
<td>0.706</td>
<td>0.760</td>
<td>0.007</td>
<td>0.767</td>
</tr>
</tbody>
</table>

Table 5.21: Error rates and standard deviations for the Multimodal MAS

<table>
<thead>
<tr>
<th>Sensitivity-SB vs</th>
<th>Sig + Fin</th>
<th>Sig + Han</th>
<th>Fin + Han</th>
<th>All Three</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auction</td>
<td>3.34±2.81</td>
<td>3.25±2.53</td>
<td>4.99±5.81</td>
<td>3.40±2.12</td>
</tr>
<tr>
<td>Game Theory</td>
<td>2.99±2.69</td>
<td>2.84±5.83</td>
<td>4.66±5.34</td>
<td>3.18±2.31</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>2.14±3.69</td>
<td>2.06±5.75</td>
<td>3.97±3.01</td>
<td>2.30±2.26</td>
</tr>
<tr>
<td>Sensitivity-SB</td>
<td>1.81±2.54</td>
<td>1.56±5.33</td>
<td>2.70±3.10</td>
<td>1.45±2.28</td>
</tr>
</tbody>
</table>

Table 5.22: \( p \) – values when comparing the lowest error rate for the multiagent with the other ones in each databases combinations

5.4.3 Multiagent multimodal system results

Finally, this section will compare the results of the traditional multimodal system configurations with the multimodal systems including soft-biometrics and multimodal multiagent systems (both including and not including soft-biometrics). Figure 5.29 shows all the results for the different multimodal configurations and combinations of the three databases (which was calculated using the data of Tables 4.16 and 5.21).
Figure 5.30: Results for the unimodal and multimodal for both multiclassifier and multiagent systems
Again, the addition of the handwritten signature produced better results than when fingerprint and hand geometry were the two modalities combined together. Moreover, the multimodal system which adopted a configuration based on three modalities performed nearly as well as the multimodal system with signature and fingerprint and signature and hand geometry.

When comparing the traditional multimodal systems (traditional vote and sum) results of each modality with multimodal multiagent systems, it can be seen that the difference in performance is very accentuated. Nevertheless, in order to confirm this statement, the statistical t-test was applied and demonstrates that all the multimodal multiagent systems are statistically better than all the traditional multimodal fusion techniques (as can be seen in Table 5.22).

As a summary, Figure 5.30 shows all the Unimodal and Multimodal results for both Multiclassifier and Multiagent Systems.

It is very important to note that even when using different system structures, the signature modality still presents very encouraging results. These final results presented give more support to the view that to the use of handwritten signature in a multimodal system can offer real benefits, and the results provide some very important insights into how these might be realised. Likewise, developing a better understanding of how demographic information (which can be related with the characteristics of handwritten signature) can be utilised in conjunction with identity prediction and the different modalities is essential to maximise the system performance in all senses.

5.5 Chapter conclusions

The results presented here have both confirmed some observations which have been previously reported, but also, importantly, have shed new light on some significant issues surrounding the choice and specific configuration and implementation of processing platforms for optimising biometric system performance. With respect to the former, a number of important conclusions may be noted:

- Even though these results are very much dependent on the database used, it is still possible to find applications where the identification results are generally more reliable with the signature dataset than with the fingerprint or hand geometry datasets.
- The degree of sophistication of the processing algorithm is generally (and unsurprisingly) directly related to its attainable performance.
- Based on the results produced using this specific database, MMCS configurations generate better results than those attainable with individual classifiers operating on UMCS.
- Most of the MMCS configurations generate better results than UMCS configurations and individual classifiers, but this is directly related to the modalities adopted.
In terms of new empirical insights, some important conclusions can be drawn, such as the following:

- Again, based on the results using this specific database, it can be said that the MMCS performance generally represents an improvement compared with UMCS, but the improvement is typically modest and sometimes non-existent when comparing the UMCS based on the signature.

- Choosing an appropriate combination method in the implementation of a multimodal system can make a significant difference, and the results have provided some quantitative performance data on this subject.

- The inclusion of non-biometric information, even if available in a limited form, can make an impact on performance. The biggest impacts shown by the results presented has been observed when the signature database was used.

- The use of multiagent solutions can make a big impact in all the different databases used either in multimodal or unimodal configurations. But especially, the $p$-values for the signature database, when compared with any other configuration can be said to the strong statistically.

Of most significance, however, is that quantitative and qualitative information has been presented which allows a system designer to consider a range of options in implementing an optimised biometric recognition system. Specifically, it may not be the case that a solution based on multiple biometric modalities will always be a first choice platform for delivery of high performance solutions, and in many cases a multiclassifier approach, based on single modality biometric samples, will be a better choice, especially where particular usability factors are paramount.

Also, when the inclusiveness factor is the most important requirement of the system and a multimodal solution is essential, modalities which would not normally be considered because are generally perceived as being unstable or insufficiently powerful for general use (such as handwritten signature, for instance) have been shown to offer other advantages which should not be overlooked. What is most important here is that the empirical study reported increases an awareness of the importance of adopting a flexible and task-related strategy for developing an optimal solution in specific circumstances.
This chapter will present a summary of all the issues addressed in this thesis as well as all the contributions given. An analysis of the potential impact of the new ideas in the biometrics area will be discussed and possible future related contributions will be discussed.
6.1 Introduction

This thesis has presented a new foundation for how to design biometric-based systems. This new approach takes into account what possible sources of identity evidence, in the widest sense, the system designer has available as well as the basic requirements of the system itself. The new work reported can be divided into three areas corresponding to three different ways of dealing with the biometric data. We have referred to these as multcategory, multiclassifier and multimodal approaches.

In relation to these three possible approaches, issues were identified and possible solutions were proposed, leading to new contributions in each of these three approaches. Also, a system basic architecture were proposed based on components which can be used as an universal way of designing biometric-based systems.

Generally, we have provided some empirical data, both qualitative and quantitative, which demonstrate the wide variability in identification performance in relation to classifier selection, fusion technique, modality selection, addition of non-biometric (soft-biometric) information and so on. This is seen to be the case both when the principal index of performance is absolute overall error rate and, perhaps most significantly, also when the analysis of the population characteristics is considered.

More specifically, each chapter from this thesis has made a potentially very important contribution from the point of view of dealing with specific problems in biometrics system design. Issues dealt in each of the five chapters can be listed as follows:

Chapter 1: Challenges in biometrics system design

This chapter presented an overall introduction to the field and a discussion of some particular problems of designing a biometric-based system. The division into three approaches is discussed as well as the issues specific to each of them.

Chapter 2: Experimental methodology

This chapter presented the new components-based system architecture which makes the managing of designing a biometrics system a much reliable task.

Chapter 3: Multicategory approach

This chapter discussed the use of soft-biometric information for enhancing biometrics system performance as a contribution for the multicategory approach.

Chapter 4: Multiclassifier approach

This chapter introduced the use of multiagent system solutions replacing the more conventional, non-interactive centralised fusion techniques which have been traditionally reported in the literature.
Chapter 5: Multimodal approach

This chapter provided a more detailed investigation of the importance of the correct choice of the modalities to be used in a multimodal system. As a case study, the use of handwritten signature data in multimodal solutions, providing some new analysis and pointing to some new ways of thinking about modalities which have sometimes not been well represented in practical solutions, presenting some very interesting results and analysis to support the argument.

The main contributions made by this thesis in the biometrics field will be listed and discussed in more detail in Section 6.2. Section 6.3 will present a list of possible future research which can be derived from the work and results reported. And finally, Section 6.4 will present some final conclusions arising from, and some concluding remarks about this work.

6.2 Impact of the contributions in the biometrics field

From the most general perspective, some very important issues were addressed. The conclusions which can be raised from the contributions made in this work are listed as follows:

- Although caution is advisable when pointing to any individual classifier as representing a "best" choice, our experiments do reveal some general trends concerning the relative merits of different classification approaches which, while not absolute, may be useful pointers to selection strategies (Chapter 2).

- It is apparent that productive possibilities exist for integrating biometric and soft-biometric information in the specification of task-specific optimal solutions (Chapter 3).

- Knowledge of lower-level information about population characteristics in relation to classification technique can offer a whole new approach to issues about user-system interaction (Chapter 3).

- The prediction of soft-biometrics is extremely useful in specific scenarios when the user often does not want to provide enough information or is not cooperative with the data collection protocol (Chapter 3).

- In relation to the signature modality, for example, even our basic analysis of different age profiles within a population reveals important information about changing patterns of vulnerability with respect to system performance indicators across the age spectrum. This could be very significant in system optimisation in a number of application scenarios (Chapter 3).
- Multiclassifier solutions to single modality configurations are rather under represented in the literature, and yet the multiclassifier methodology is widespread and often very effective in many application domains. Our empirical study provides relevant information to inform further investigation of this approach to enhancing identification performance (Chapter 4).

- Despite the fact that multiclassifier systems can combine the benefits of many classifiers, they do not necessarily provide entirely "intelligent" solutions. It may be advantageous for the classifiers to be more interactive, taking fuller account of their individual strengths and weaknesses. Multiagent systems offer such a possibility, and our results provide a new approach to designing a novel solution based on such an operating principle (Chapter 4).

- The independence and individuality of each agent taking part in the identification process gives a whole new dimension to the philosophy of biometric processing. Thus, this type of system relates very well with the specialist discussion scenario (Chapter 4).

- The results also point to the potential benefits, especially using the negotiation strategy, of allowing the agents to carry the configuration process further, for example to the point of determining the most reliable modalities to adopt in different task domains (Chapter 4).

- Multibiometric solutions are now widely recognised to offer advantages not only in enhancing overall system performance, but also, significantly, in offering greater flexibility and user choice in system configuration. This study provides some initial insights into how to match classifiers and modality-specific data in determining an optimal configuration (Chapter 5).

- In large volume applications, for example, the level of performance improvement achieved using the multiagent multimodal approach might make a significant impact, and provides options too in choosing an appropriate method to deal with the number of modalities available (Chapter 5).

- A finer-grained analysis of performance within a specific modality can also generate useful practical insights into the relation between lower-level factors and performance returned using different classification approaches (Chapter 5).

- Although there is now an extensive literature on modality combination, adopting the signature as one of the target modalities is a relatively little used option, and our benchmark performance characterisation can provide a starting point for a productive study of optimal modality selection (Chapter 5).

The implications of these findings are very exciting. These results therefore point to a very interesting strand of investigation which, until now, has received
relatively modest attention, but which clearly offers opportunities to develop better, more robust and more flexible practical biometric identification systems in the future.

6.3 Future work

The research presented in this thesis has aimed to maximise the performance of biometric-based systems by focusing on the designing of the system in general, not only in specific parts of it. In the context of the very interesting contributions represented in this thesis, naturally, some new ideas have emerged from the results presented.

Sections 6.3.1, 6.3.2 and 6.3.3 will propose some suggestions for future work in relation to each of the three approaches.

6.3.1 Further research in multicategory approach

A more detailed investigation should be made using different soft-biometrics apart from age, gender and handedness and their relation with other biometrics modalities in addition to handwritten signature, fingerprint and hand geometry.

Also, the issue of subject age is in itself a starting point for a whole new area of investigation. Effects of age in different modalities as well as the template age are among many ideas which can be explored in this particular area.

New, more sophisticated, fusion techniques will need to be proposed using soft-biometric information. The four techniques proposed in this area, although producing very encouraging results, are in fact relatively simple and straightforward.

The prediction of soft-biometric information from biometric data is another very interesting area of research that must be investigated in more detail.

6.3.2 Further research in multiclassifier approach

The use of multiagent technology is still under-explored when applied to biometrics applications. The main future work which is suggested in this sense, is to explore the negotiation techniques to provide more detailed insights into their future use.

Also, the exploration of the use of the agents in different levels of the system is also an interesting new contribution (i.e. using agents for feature selection and extraction or using agents to choose which classifiers are more suitable to different users and/or modalities).

6.3.3 Further research in multimodal approach

The investigation of the use of the handwritten signature in multimodal applications can still provide some new contributions. A more detailed investigation using a bigger and more statistically significant database is still necessary.
A deeper analysis of different population characteristics in a handwritten signature is also an interesting and important contribution to be made.

6.4 Chapter conclusions

This thesis has presented significant contributions in the biometrics field, most specifically in relation to how to best design a biometric-based system. We have introduced a new approach to the process of improving the accuracy of biometric identification systems.

The use of both biometric and soft-biometric information was one of the main contributions in an effort to enhance performance, robustness and reliability. We have proposed substantial modifications to some established methods, principally seeking to integrate soft-biometric information sources into an enhanced identity prediction system.

Also, a major contribution has been the integration of different sources of identification data, in a very general way, and the design of an implementation structure built around an approach embodying more intelligent and flexibly entities (intelligent agents), which are invoked in reaching a decision about the identity of a user. This approach has a number of advantages, since it provides a significant enhancement to the reliability of decision-making compared to other approaches but, importantly, it also provides long-term extendability, since it is relatively easy to see how multiple different sources of identity evidence can be incorporated within the general structure proposed in order to support further enhancements.

Finally, a discussion of the benefits of the correct modality choices in a multi-modal application was also an aim of this thesis. Here, instead of focusing entirely on well accepted modalities, a significant analysis of what are the advantages of using handwritten signature, in a high performance level, as well as in a low level were discussed.

These contributions appear to be well suited to the nature of the generalised biometric identification problem, and can be readily used to incorporate additional sources of information (biometrics or not) and to decide the best structure to be used.

In summary, the work reported in this thesis has provided an opportunity to learn a great deal about the specification, implementation, optimisation and deployment of biometric systems, and to contribute some new ideas to how this very important and emerging area of technology can be enhanced and developed in a positive way in the future. Increasing performance, flexibility, inclusiveness and optimality into the ways in which biometric systems will develop in the future are seen as very important factors in encouraging their uptake, and it is hoped that the work reported here will make some impact in these areas.
Bibliography


