CIHSPS 2005 – IEEE International Conference on
Computational Intelligence for Homeland Security and Personal Safety
Orlando, FL, USA, 31 March – 1 April 2005

A Multi-Modal Multi-Paradigm Agent-Based Approach to Design Scalable Distributed Biometric Systems

Marco Gamassi, Vincenzo Piuri, Daniele Sana, Fabio Scotti, Olga Scotti
University of Milan - Department of Information Technology
Via Bramante 65 – 26013 Crema (CR) – ITALY
{gamassi, piuri, sana, fscotti, oscotti}@dti.unimi.it

Abstract *– This paper presents an innovative approach to design advanced biometric systems for person identification, recognition and monitoring, with high level of privacy.*
The original aspect consists of a modular, structured design approach at system level, based on the use of distributed systems, multi-agent architectures, multiple computing paradigms, and adaptable/evolvable techniques, which allow for achieving a scalable structure in terms of biometric algorithms, identification quality, sensors, database complexity, database integration, and component heterogeneity.
Our goal is to face the specific application by using a flexible design strategy based on a systematic comprehensive view, by focusing on global optimization, adaptivity and evolvability.
Advantages of the proposed approach are accuracy, confidence, scalability, opportunities for parallel processing, high performance, interoperability, fault tolerance, service continuity, biometric techniques updating, usability, and components privacy.
These characteristics can be very useful for governmental agencies, enterprises, banks and all other organizations that need to protect people or control access to critical resources.

Keywords *– identification, recognition, monitoring, security, modular design, system approach, multi-agent architecture, distributed systems, multi-paradigm computing, adaptable and evolvable techniques.*

I. INTRODUCTION

Safety of critical places (e.g., airports, public buildings, banks, court houses, ministry offices) is increasingly perceived as a very critical requirement by citizens. Guaranteeing safety becomes important to avoid criminal actions and make the towns and the countryside more livable. Besides, the access to sensible information (e.g., personal, sanitary, bank, commercial trading) is very frequent in economy and all modern public and private services. In these cases guaranteeing the privacy becomes a mandatory requirement.

The use of advanced techniques for person recognition and identification acquires therefore today a central role in the society and in the economy. Identification and recognition are directed to verify if a person belongs or not to a prefixed group, denying or granting him/her the access to places, information, and services. Even though specific suspicions persons do not need to be identified or recognized, early detection of suspicious behaviors are interesting to recognize malicious intentions in advance and to prevent dangerous acts. Studying people movements, monitoring human behavior, and detecting anomalous scenes can therefore become valuable to avoid dangers.

On the other hand, to guarantee safety and privacy of citizens, institutions and enterprises are interested nowadays in using solutions based on biometric techniques to develop innovative services. For institutions, the adoption of these approaches is finalized to improve services and to be closer to the citizens and their feelings. For enterprises, these solutions are extremely useful to maintain and increase the presence and the competitiveness on domestic and worldwide markets.

The relationship between the biometric features and the person identifier (template) should be non-reversible, i.e. it should not be possible to reconstruct the original biometric features from the template. This is fundamental to ensure privacy and usability with the end users (people are in fact very concerned with the "big brother" security syndrome, i.e., for example the association of fingerprint to crime and criminality).

Many methods for identification and recognition have been studied. Most important researches have developed very efficient algorithm to identify or recognize person by using biometric information. Actually best results in identification can be obtained starting from iris comparison and finger print analysis. For recognition, good rates have been reached with face analysis [1]. Other techniques (like voice and signature [2]) are still to be improved.

Limits of current solutions and research projects are that the problem is addressed from specific points of view; without systematic and comprehensive approach. They do not introduce adaptivity and evolvability; no global optimization; there is not attention to specific and integrated consideration for system-level issues (e.g., multiplicity of databases, databases privacy and security, algorithms privacy, scalability, integrability, interoperability, maintenance, usability, service continuity).

A very large quantity of heterogeneous biometric databases exists. Each institution or big enterprise memorized, according to their own necessities, one or more biometric data, by following rules useful for their needs and by using various sensors and collection procedures.

Our goal is to design a comprehensive system having the opportunity of querying, in parallel, all available databases with various feature extraction approaches, so as to permit a wider check. Advanced devices will be used to collect

0-7803-9175-6/05/$20.00 ©2005 IEEE

biometric data and code them before transmission. Coded data will be compared with data stored in all selected databases to contribute to identification or recognition.

This paper is a preliminary report of a research activity which is under development at the Biometric Laboratory of the University of Milan.

II. OBJECTIVES

Our approach to the system design is directed to deal with different situations concerning the real application scenarios:

- Person identification by comparison of the code generated by biometric measurements with the one stored in the passport (one-to-one).
- Person verification by code data base searching (one-to-N search), including negative search (i.e., non-matching approach). This approach demands for interoperability of data streams incoming by terminals and heterogeneous data stored in different, multinational data bases.
- Person identification by generating a non-reversible biometric code also from incomplete data base with heterogeneous/incomplete data base.

The project here reported and the proposed approach aim to study, experiment, and evaluate the use of a modular, structured design approach at system level, based on the use of distributed systems, multi-agent architectures, multiple computing paradigms, and adaptable/evolvable techniques. Cooperative and integrated use of these technologies is necessary and fundamental to reach our comprehensive target for designing and implementing the new generation of integrated biometric security systems. This constitutes the innovation proposed by our system-level design methodology.

III. MULTI-MODAL APPROACH

The effectiveness of each method for identification is dependent on the quantity of available information, the operating conditions, and the intrinsic characteristics of each technique. This consideration suggests not limiting the use to only one biometric technique. When one method fails, or is not sufficiently adequate for accuracy and confidence, other techniques or other biometrics modalities might offer better results.

The multi-modal approach, based on the use of more than one biometric characteristic to carry out identification, recognition or monitoring, allows for increasing the probability of correct identification and recognition by using different biometric information. Abilities of each biometric feature for person identification/recognition are in fact not exactly overlapping and, therefore, the union of all abilities becomes wider of the individual solutions, thus providing overall better performances [3] [4].

In order to always provide the more accurate and reliable performance, the use of a variety both of techniques and biometrics modalities becomes appealing to overcome the limits of each of them: the final answer will be created by fusing the partial results achieved by each of them. Solutions will also have to be adapted evolutionarily to the changing environmental conditions and to the quality of the analyzed information in order to overcome the limits of solutions tailored on specific conditions.

IV. MULTI-PARADIGMATIC APPROACH

The use of more techniques for the analysis of one biometric characteristic constitutes the multi-paradigmatic approach to system design.

Each technique operating on one biometric characteristic has specific limits and points of force. The multi-paradigmatic approach allows analyzing the same biometric information from various points of view, possibly overcoming the limitations and the problems that are intrinsic in the individual technique [5] [6].

The multi-paradigmatic approach allows for exploiting the characteristics of each alternative technique to process the same biometric information and for dealing with different characteristics of the information stored in the various databases (also due to the various sensors and collection procedures used during biometric information acquisition). For example finger prints can be coded by looking at local or global features. The method used depends from the kind of image available, the sensor, the algorithm, and so on, but the match with all databases can be possible only if each database receive data which are comparable with the ones stored in the database itself.

On the other hand, this approach allows for supporting natively the inclusion and deployment of more advanced algorithms and new solutions as soon as the research and the industry make them available without changing the overall biometric system structure and services.

V. ADAPTIVE AND EVOLVING TECHNIQUES

The changeable or not completely specified system characteristics and desired features make difficult to implement solutions that are optimum, able to evolve by following the environmental and information changes, and remain optimum even after the evolution of the application environment.

The use of adaptive and evolutionary techniques (in particular based on computational intelligence, i.e., neural networks, fuzzy systems, evolutionary computing, and granular computing) allows for incorporating adaptivity and flexibility in the security system by means of continuous learning [7].

This concurs to create intelligent biometric systems by defining their objectives by means of an appropriate set of examples, by allowing for their self-adaptation to changing or not completely defined operating conditions. The system will

exploit in fact his generalization abilities to interpolate very well the desired behaviors and extrapolate them from the known cases.

VI. DISTRIBUTED SYSTEMS

The various entities holding biometric databases (e.g., national and international polices, security services, ministries of interior, banks) are usually eager and very firm in protecting their own biometric information, for security and privacy reasons and to reassure the public opinion. Usually sharing of information is perceived as necessary to increase the protection, but is feared with horror for possible information leakage or database intrusion and manipulation.

Besides, centralizing all information could result in loss of quality and ownership, as well as in reduced responsibility. On the other hand, heterogeneity of sources and collection procedures and sensors make difficult to integrate different databases into a single environment by exploiting only the conventional database technologies.

Distributed systems constitute a technological solution that easily allows for integrating the biometric resources available in the various existing databases without the need of physically merging the databases themselves. Biometric integrability is in fact a relevant issue in advanced system design.

The parallel use of various biometric modalities and various analysis paradigms make feasible to exploit the possible parallelisms offered by the hardware architecture of the distributed information processing system [8]. In particular, it is possible to physically execute the computation of single tasks in parallel on different processors whenever these tasks are sufficiently independent each other, thus reducing the total elapsed processing time for a better real time response. To this aim we can exploit multiprocessor structures, distributed architectures in local or geographic networks, GRID structures, local clusters, or systems based on blade processors. The exploitation of the parallelism based on the concurrent execution of the various paradigms for the various biometric modalities is much easier and natural to be introduced since it is not related to the parallelization of a single algorithm. Besides, it allows for a dynamic computation allocation and, thus, for a better balancing of workloads and use of resources.

Parallelism can also be exploited to deal with the performance limits imposed by the size of the databases and, thus, to ensure high scalability to biometric databases. In particular, database partitioning can be used to limit the size of the archive in which search must be performed; distribution of the partitions on various processing systems allows for search parallelization, while limiting the size of each portion of global database to be managed by the security system.

Modeling the biometric information processing on a distributed system allows for introducing an intrinsic mobility in the operations and, consequently, in supporting service continuity and fault tolerance in a native way. Suited replication of the databases allows for designing strategies that prevent the lack of accessibility due to network or processing nodes failures: the application will search for an available copy of the desired database in the accessible network.

Distributed systems allow for querying various databases by ensuring their individual privacy, security, integrity, and ownership, without actually sharing their information within the whole security system. At the same time, the distributed systems allow for using private algorithms for feature extraction and matching, by ensuring their secrecy even within the security system. In particular, databases and biometric analysis algorithms can be made available remotely, without actually sharing them publicly within the security system. The system can in fact access to remote processing systems with the biometric information obtained from the sensors to be completely processed and to perform the database search remotely or the concise biometric features extracted locally to perform only the database search remotely. This will avoid publication of algorithms and database information within the security system, thus allowing for supporting high privacy.

Distributed structures allow also for easily supporting the scalable increase of available database information and the integration of heterogeneous systems and legacy systems. Scalability can be achieved, for example, by expanding the individual database, by restructuring the database allocation by means of splitting on various host computers, by merging various databases, or by connecting new separate databases.

Interoperability of heterogeneous databases can be also supported since individual databases are connected into the integrated environment.

VII. MULTI-AGENT ARCHITECTURE

Organizing the biometric systems as multi-agent systems allows for efficiently constructing software architectures flexible, adaptable, and modularly scalable. An agent will carry out the analysis of a specific biometric modality with a specific technique on a specific database.

The multi-agent architecture allows for natively supporting the use of all of the above characteristics for advanced biometric information processing, namely distributed information sources, multi-modal approaches, and multi-paradigmatic techniques, by encapsulating the various sources and the various queries in a homogeneous framework.

The use of multiple paradigms will be made transparent by merging the results of the various processing before using the achieved comprehensive result.

The use of multiple modalities will be encapsulated by spawning parallel searches on the collected biometric features and, then, by fusing the various partial results, possibly obtained with various paradigms for each modality.

The intrinsically parallel structure of the computation based on multiple agents allows moreover for taking advantage, in a natural way, of the possible parallelisms

offered by the hardware architecture of the information processing system. The use of various databases containing biometric information in the same modality will be hidden by running separate agents querying the various databases in parallel and, then, by merging the retrieved partial results. In particular, it is possible to physically execute the computation of single agents in parallel on different processors, thus reducing the total elapsed processing time. This allows also for exploiting possible parallelisms in the analysis of biometric information and in database searching, thus reducing the overall processing time.

The agent-based approach makes also easier to transparently interrogate several information sources thus increasing the system usability and usage, as well as reducing the overall response time for a better real-time operation of the whole biometric system.

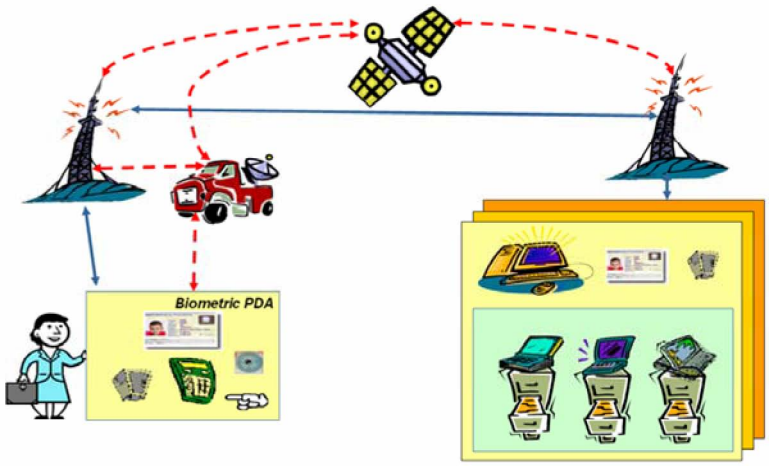

Fig. 1. The overall structure of a biometric system

Modeling the biometric information processing as a multi-agent system allows for introducing an intrinsic mobility in the operations and, consequently, in supporting service continuity and fault tolerance in a native way. Agents will search for an available copy of the desired database in the accessible network. This allows for natively ensuring fault tolerance and continuity of service through automatic redistribution of the queries.

The intrinsically parallelism of the computation in multi-agent systems allows for natively supporting the distribution of information and services, thus guaranteeing also high levels of security, protection, and privacy of information and processing algorithms.

The multi-agent architecture allows also for easily supporting the scalable increase of databases and the integration of heterogeneous systems and legacy systems by encapsulation in suited agents.

The synergic cooperation of agents allows for finding the optimal solution by compensating possible deficiencies and limits of individual paradigms, modalities, and databases, by logically operating in parallel.

The use of multi-agent systems will in particular be very useful to address the interoperability of biometric databases and biometric sensors outputs. The various differences among them can be encapsulated in the agent-based framework and appropriate analysis algorithms can be devised to take into account the differences between the quality and the characteristics of the collected biometric information. The multi-agent structure can hide the various heterogeneous components by providing the interconnection glue and the homogenization infrastructure for database access.

On the other hand, the availability of efficient interoperability support will be highly valuable to realize multi-national security systems since it will natively and easily allow for querying in the databases of the various cooperating nations without the actual need of sharing the real biometric information and analysis algorithms.

VIII. THE SYSTEM-LEVEL DESIGN APPROACH

The construction of a biometric system with high abilities of integrating existing components and information databases, preserving ownership and privacy, scalability, and interoperability as well as the native ability of supporting multi-modal and multi-paradigmatic methodologies is a challenging goal, which has an inestimable value for advanced biometric systems and their effective and efficient use in a heterogeneous distributed environment.

To achieve effective usability of biometric technologies in institutions and enterprises, it is in fact fundamental to adopt solutions that can be easily integrated in the usual operating processes and products.

They must have good effectiveness, reasonable cost, small managerial impact, good integrability, good scalability, good interoperability, and good adaptability to changeable conditions.

In summary, biometric solutions need to be studied and implemented with a system-level perspective and not only as a technological add-on to existing services and products.

The cooperative coordinated use of multiple modality, multiple paradigms, distributed systems, and multi-agent frameworks allows for supporting such an integrated perspective in system design.

IX. EXAMPLE

The overall structure of a biometric system designed by using the proposed comprehensive system-level methodology is shown in Fig. 1.

Each security agent, assigned to identities control, will be supplied of an object, similar to a palmtop (hand held device), in which are inserted multiple single-biometry sensors for collecting biometrics data (finger prints, iris, signature, other), a camera, a lodging for smart card and a CPU [9].

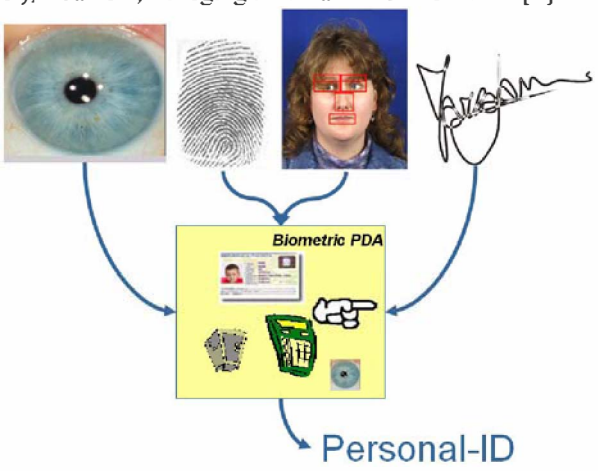

Fig. 2. Generation of the personal identifier

After collection biometrics data of the person to identify are codified using all techniques loaded on the palmtop at the moment (techniques can be dawned, or increased of number, following technological developments).

Multiple biometric data are integrated from the intelligent terminals in a sort of biological fiscal code (Non Reversible Coding, NRC), a unique identifier for each person. The unique identifier is based on the combination of data from the sensors so that it may not be traced back to any of the biometrics and/or sensors used to generate it. Generation of the personal identifier is shown in Fig. 2.

The Non Reversible Code can be generated form multiple biometric measurements and also from heterogeneous incomplete data bases.

Development of algorithms to generate biometric code (NRC) from existing limited data bases allows both to exploit data already stored and to manage the transition phase.

Coded data can be transmitted without violate privacy of the individual, since also the union of all the possible coding of the same type of biometric information does not concur to go back to original data.

Mechanism of communications is, anyway, based on secure channels [9]. If conventional channels are interrupted, backup procedure using satellite communication is started.

Implementing agent systems, based on information technologies and advanced hardware platforms (i.e., parallel computing, clustering), allows for managing the complexity of heterogeneous data bases and for performing all data base operations (queries, new data introduction from multiple sources) by satisfying stringent time requirements. The multi-agent structure supporting all features described in the previous sections is shown in Fig. 3.

X. CONCLUSIONS

The use of a comprehensive, integrated approach to system-level design of biometric systems for security applications is fundamental to implement optimized and flexible systems, able to evolve and adapt themselves to changing scenarios and technologies. The main and innovative goal consists of the specific focus on the system-level design, directed to create a structure with high characteristics of accuracy, modularity, expandability, adaptability, evolvability, maintainability, scalability, integrability, interoperability, optimizability, usability, privacy, reliability, and service continuity.

To achieve these goal we studied, experimented and evaluated the technologies and the design methodologies suited to realize an intelligent distributed system for person identification, recognition, and monitoring, based on multi-modal, multi-paradigmatic, multi-agents, and adaptive-evolutionary technologies in order to take synergically advantage of the opportunities offered by every technology.

Since the main focus is on the system-level perspective, the proposed methodological approach is open to the possible enhancement of the single components that are used in the security system, namely, the sensors, the portable devices for collecting the biometric features, the biometric feature extraction algorithms, the biometric identification, recognition, and monitoring algorithms, the database structure and query processing, the communication technologies, the information and communication security.

Future research will study the issues of optimum application of this comprehensive system-level design approach to satisfy the specific requirements of real applications. In particular, optimization will consider accuracy, confidence, reliability, performances, security, and cost.

REFERENCES

[1] Image-based multimodal face authentication Pigeon, Stéphane; Vandendorpe, Luc; Signal Processing Volume: 69, Issue: 1, August 31, 1998, pp. 59-79

[2] On-line signature verification with hidden markov models. J. J. van Oosterhout, H. Dolfing, and E. Aarts; in ICPR, 1998

[3] Accuracy and Performance of Biometric Systems M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, F. Scotti; IEEE Instrumentation and Measurement Technology Conference, Como, Italy, 18-20 Maggio 2004

[4] Design of a vision system for identity verification Tistarelli, M.; Lagorio, A.; Jentile, M.; Grosso, E.; System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on , Volume: Track3 , 5-8 Jan. 1999 Pages:9 pp.

[5] A High-level Optimum Design Methodology for Multimodal Biometric Systems
M. Gamassi, V. Piuri, D. Sana, F. Scotti; Proc. International Conference on Computational Intelligence for Homeland Security and Personal Safety CIHSPS, Venice, Italy, 21-22 Luglio 2004

[6] Fusing face and ECG for personal identification Israel, S.A.; Scruggs, W.T.; Worek, W.J.; Irvine, J.M.; Applied Imagery Pattern Recognition Workshop, 2003. Proceedings. 32nd , 15-17 Oct. 2003 Pages:226 – 231

[7] Multiple query evaluation based on an enhanced genetic algorithm Tamine, Lynda; Chrisment, Claude; Boughanem, Mohand pp. 215-231 Information Processing and Management Volume: 39, Issue: 2 March, 2003

[8] Parallel biometrics computing using mobile agents You, J.; Zhang, D.; Cao, J.; Minyi Guo; Parallel Processing, 2003. Proceedings. 2003 International Conference on , 6-9 Oct. 2003 Pages:305 - 312

[9] Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body Cherukuri, S.; Venkatasubramanian, K.K.; Gupta, S.K.S.; Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on , 6-9 Oct. 2003 Pages:432 – 439

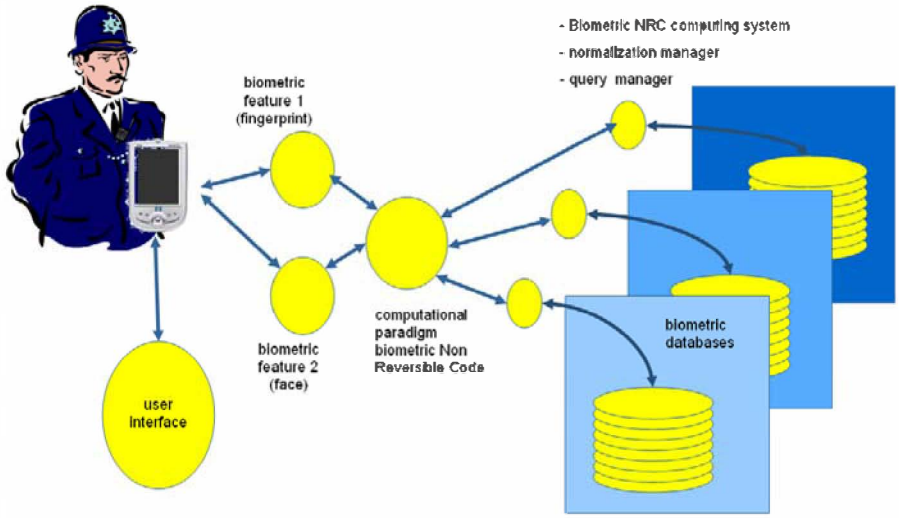

Fig. 3. The multi-agent structure supports all features