Applied Surveillance using Biometrics on Agents Infrastructures

Manolis Sardis, Vasilis Anagnostopoulos, Nikos Doulamis

National Technical University of Athens, Department of Telecommunications & Software Engineering, 15773 Zografou Campus, Athens, Greece,
WWW home page: http://www.ece.ntua.gr
emails: {sardis, vanag}@telecom.ntua.gr, ndoulam@cs.ntua.gr

Abstract. The biometric identification of individuals has many safety and security applications in several fields of major interest. This can range from healthcare to commerce and from defense to banking systems. Current biometric technologies are hardly suitable for remote online massive use. This paper presents an innovative approach to design advanced biometric systems for personal identification, recognition and monitoring, with high level of privacy and scalability. The proposed system consists of a modular design using distributed systems, multi agent technologies, adaptable techniques that allow the creation of a surveillance infrastructure based on biometrics sensors. The proposed infrastructure is characterized by scalability and adaptability on sensors (cameras) number and signal manipulation through the multi agent infrastructure. System results can be extended to link more enterprises and application domains that need person identification and related events for access control on critical resources.

1 Introduction

Safety and security airports, public buildings, and private domain areas, like corporate buildings, is of paramount importance nowadays. Consequently we need secure ways to identify human actions. The starting point of unpredictable unsecured actions is usually the entrance on the specific sensitive place, where we need surveillance. In order to avoid such conditions we propose through this work an agent infrastructure that achieves practical human surveillance using camera sensors and biometrics technologies.

The application of advanced techniques for person recognition and identification is directed to verify if a person belongs or not to a prefixed group, denying or granting the access to places, information and services. Even though specific suspicious persons do not need to be identified or recognized, early detection of suspicious behaviors is applied to recognize malicious intentions in advance and to

prevent dangerous acts. Authentication is testing if an individual has access to proceed.

In the last years using biometric techniques to develop services for surveillance was the common approach [1]. Biometrics is the science and technology of measuring and analyzing human body characteristics. Systems based on this technology are pattern recognition systems that acquire biometric data, a set of characteristics, and a mechanism to compare these features against a collection of previously acquired templates. There is evidence that this procedure can be automated by the use of Haar wavelets in a supervised learning manner [11] and this is one of the motivations behind this paper.

Authentication is a simple one-to-one verification process where an acquired pattern is compared against a single stored template in order to determine whether the user is the individual who claims to be. Identification is a one to many process where the pattern at hand is compared against a database of multiple stored templates in order to establish the identity. Most of the biometric devices are operating in *authentication mode* using the following two steps: (a) an identity is requested from a database where participants templates have been previously stored, (b) then by presenting a live biometric sample for comparison the intelligent system provides or not the related labels and outputs.

The *identification mode* is working directly by doing a search in the database based on the acquired biometric sample. In general the biometric framework should be practical in terms of performance and acceptability and circumvention. Data fusion techniques should be incorporated in order to eliminate the biometric system errors [2]. Face analysis techniques [3] present the best results for identification and recognition. The system examines the faces and attempts to find visually similar matches in its stored database visitors. The agent technology controls the related events from the GUI to the external systems connected on the infrastructure or the end users/operators. The operator is able to provide feedback to the infrastructure in the case of misclassified visitors. The face recognizer is working online and is able to learn online. Face recognition under unconstrained conditions is very challenging. The purpose of the visitor identification infrastructure is to provide not only access control but a whole adaptive solution for security using surveillance and biometrics techniques. These solutions are extremely useful for enterprises to increase the domestic and worldwide markets.

The paper is structured as follows: Section 2 analyzes the design considerations of the proposed infrastructure. Section 3 proposes multi-agent technology combined with biometrics sensors as a solution. In Sections 4 and 5 we present the system design and related use cases for the system evaluation. Finally, in section 6 conclusions and remarks close the paper structure giving future research topics.

2 Design considerations

To design ambient intelligence environments, many methodologies and techniques have to be merged together originating many approaches present in recent literature [4]. From the wide range of the possible solutions any ambient intelligent environment is characterized by the following goals and technologies.

- Adaptability, the infrastructure is reactive to new habits, behaviors and needs from the operators and the working environment.
- Context awareness, the infrastructure has the ability to recognize people and the situational context.
- Flexibility, for the operators to customize the control outputs from the infrastructure to other systems connected on it.
- Extensibility, for the surveillance objects and their attributes that can be implemented and controlled by the infrastructure.

The above characteristics are achieved by the use of the artificial intelligence and the proposed multi agent platform. System independence and transparency is achieved by the use of the biometrics sensors that bring the face recognition signals into the infrastructure and are able to verify the correspondence between people requesting access and authorized accounts, which have been stored during the learning procedures from the infrastructure, in system storage module.

Finally, the automatic validation and recognition allows the infrastructure to adapt related services and the according environmental parameters to the system operators' requests and preferences of the recognized objects/persons, during the surveillance. The following paragraphs are analyzing the above infrastructure in more details.

3 Biometrics and multi agents

The proposed infrastructure has been implemented using a distributed collection of agents [6]. The number sensors /cameras provides adaptability to different conditions and environments as biometric characteristics that characterize the identification, recognition and monitoring of the surveillance objects, allow the increase of identification and recognition probability percentage. Biometric integraability is a relevant issue in advanced system design. Also system adaptability is supported by allowing the participation of different agents, which manipulate different algorithms and techniques for surveillance, in the proposed infrastructure allowing the inclusion and deployment of more advanced and new solutions, without changing the overall system architecture and structure. Based on "Fig. 1" the *Surveillance Input* agent represents the biometric sensor that is used for the surveillance. In our case study the system is based on cameras. The *Agent for recognition* uses algorithms for the processing of the data input. With the help of

Evaluator Agent and *Agent for Event creation* the system does the recognition and identification of the objects/humans and prepares the related *events* that will trigger the graphical user interface of the infrastructure. The role of the *Output controller* is to manipulate the output data to other external systems that have been integrated in the proposed infrastructure, either as an extension or as an integrated part of the system. The agent community needs a coordinator of all agents, and this is performed by the *Agent Network Controller*.

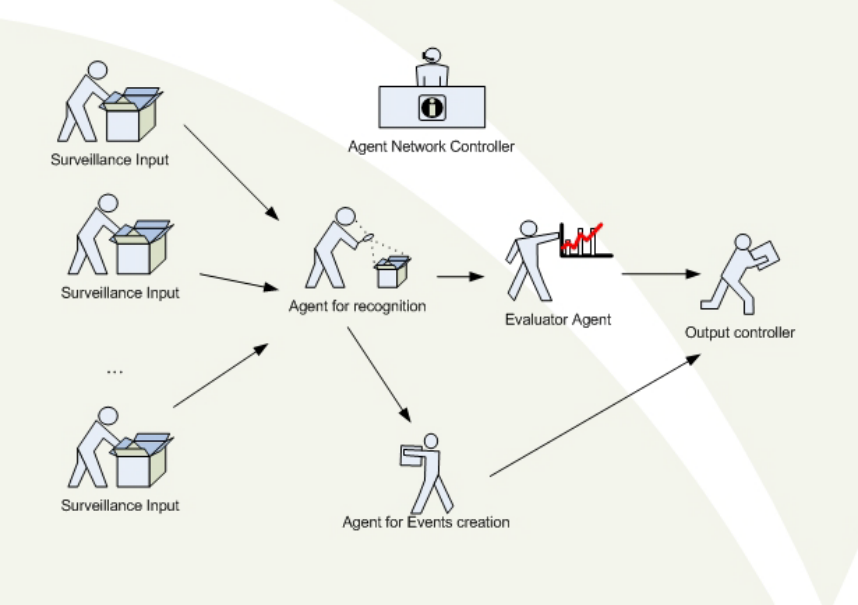

Fig. 1, Multi Agent Infrastructure

The parallel use of biometric sensors and algorithms using agents to control them provides distributed information processing [5] through a modularly scalable software architecture. This architecture supports the integration of heterogeneous and legacy systems by encapsulation in related agents.

The face detection scope is to examine a camera image and extract regions containing a face. In this infrastructure the face detector described in [8] by Viola and Jones has been employed. This detector scans square regions at various scales in the image and extracts features in the form of Haar wavelets to determine whether the region contains a human face. The selection of this detector from a number of other published detectors, like [9] and [10] pool of detectors (references), was based on acceptable detection accuracy requirements, its readily available implementation in the OpenCV library and finally its suitability for real-time processing. Different camera positions generate images for various face orientations for increasing accuracy. However, in this specific application there are physical constraints as to the distance of the human from the camera and to the orienta-

tion of the face. Two cameras suffice to have acceptable performance. Moreover the feedback from the system, guides the user to correct his placing with respect to the camera.

The face recognition procedures rely on a previously acquired collection of several images per visitor, in a controlled environment, and fast modeling of a variety of illumination conditions in the form of normalized color spaces. The output from the multi-agent recognition module will trigger the graphical user interface, giving the possibility to the infrastructure operators to provide feedback to the user and fine tuning of the system.

4 System Architecture

The proposed infrastructure has been implemented using a distributed collection of agents based on the architecture of "Fig. 2".

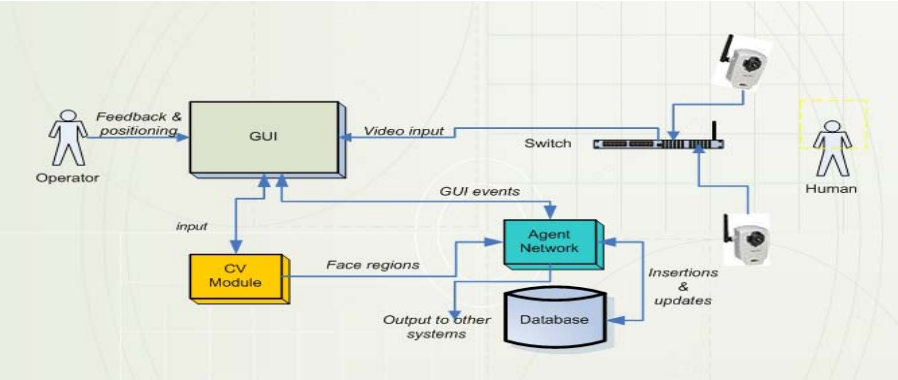

Fig. 2, System Architecture

The architecture we adopted for the problem at hand is comprised by various modules which we will analyze now. We have implemented a module for the Axis 207w cameras which grabs the provided JPEG pictures. The video input is controlled by the GUI which also presents the frames to the operator. This GUI also sends the frames to the computer vision module, for face region detection and extraction. In order to speed up the procedure, the regions are sent directly to the multi-agent infrastructure module for recognition. In addition to the mentioned role this module also controls database access. Successful recognitions are fed back to the GUI in the form of a series of matches ordered by decreasing probability via an event mechanism.

In order to optimize the interaction diagram for performance we exploit the hierarchical nature of the Haar wavelets in our setup. We didn't choose a complex methodology like in [7], since our problem is simpler. By their definition each newer level detects details in half the previous level. For this reason, since our im-

ages are rectangular each new level generates four new sub images. Our network is a graph of identical peers. These peers take as input two images of power of 2 side lengths, wavelet-tranform them and compute inner products. An inner product is also performed in order to detect similarity between the two transforms. If they are greater than a threshold, an agent forwards the four equally sized parts of the image (SouthEast, SouthWest, NorthEast and NorthWest) to its neighbors ("Fig. 3"). We define neighbors as the agents having number with residual equal to the initiator minus one mod 4. We design our system around 16 agents and our algorithm works in depth 4 per side. For this reason, the Evaluator expects 16 messages at depth 4 per stored image. The percentage of them that arrives at the evaluator is the probability of success.

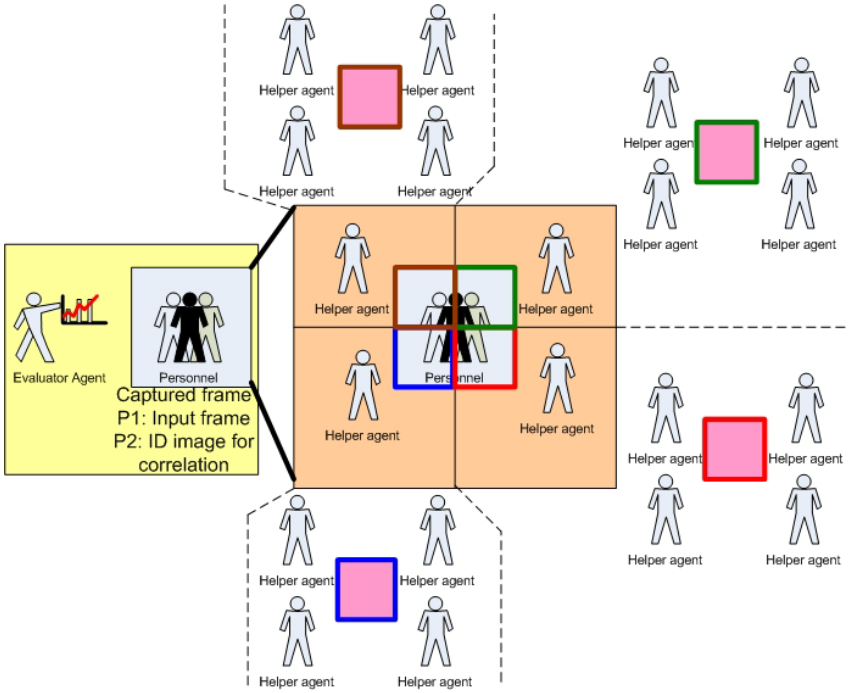

Fig. 3, Agents subsystem decomposition

For speedier calculations the corresponding transforms of the images can be pre-computed and retrieved by the orientation and depth pair of the region in the images. In our case, we do not scan the whole image via translations because this step is already done by the face detector. Moreover we make our images normalized to 64x64 resolution which is clearly a power of 2. There is over completeness in our design because the transforms of the lower levels are used in the higher levels too. But this redundancy is unavoidable in order not to drop information and have well defined inner products. We also achieve a nesting of subspaces from coarser to finer information.

5 System design and case studies

The proposed infrastructure has been implemented using a Java-based system implemented on the JADE platform. The prototype design is presented in "Fig. 4". "Fig. 4" shows a typical example of the application of our system on real-world data. The captured images have size 640x480 pixels with zero compression. They are resized to half their size for presentation purposes. The frame grabber is implemented in C++ and the GUI in TCL/TK 8.5.6. For the agent-based system we selected the well-documented JADE platform and for face detection we used the stock implementation of the OpenCV library. The communication between the GUI and JADE was accomplished with SOAP messaging. The database stores the Haar features and the normalized 64x64 sized images. We used the mingw/msys compiler system and jdk 1.6.11.

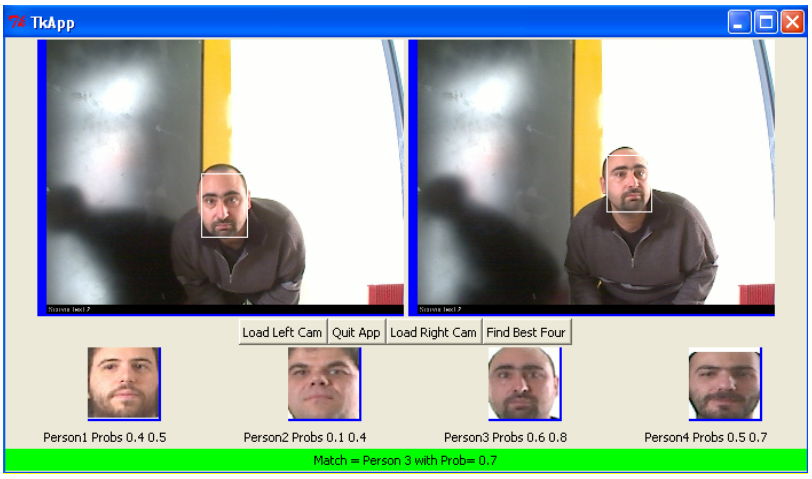

Fig. 4, Prototype system

The functionality is the following: two buttons load images from the two-camera system. The button *Find Best Four* initiates the procedure of face detection and recognition and finds the four best matches in the database by resizing to 64x64, extracting features and using a Euclidean distance. In order to reduce false positives, we select face detected regions that have high matching in the database. In this way, we eliminate spurious face regions that have negligible resemblance to the already stored data due to noise. This is a typical problem with the above mentioned Haar detector. The existing data were extracted manually from the operator after the recording of 18 persons in 4 poses with 100 copies for the same person-pose pair. We also stored some negative results from the entrance without any humans to increase robustness. In a latter version we should try to automate this procedure possibly by selecting another face detection algorithm or exploiting further real biometric information. We used the already trained detector of OpenCV but the cascade was run as a pipeline on different agents.

6 Conclusions

This paper proposes an infrastructure for intelligent environments and biometrics. The surveillance tasks are distributed on multi agents and resources are shared between heterogeneous services. Our intent is to further extend our prototype and experimentation by considering as future goals the integration of new services mediated by other categories of adaptive agents and to perform an evaluation between different surveillance algorithms implemented by the proposed infrastructure.

References

[1] Delac, K., Grgic, M., "A Survey of Biometric Recognition Methods", *46-th International Symposium Electronics in Marine*, ELMAR-2004, ISBN 953-7044-02-5, Zadar, Croatia, 16-18 June 2004, pp. 184-193, (2004)

[2] Ross, A., Jain, A., "Information fusion in biometrics", *Pattern Recognition Letters*, No. 24, Elsevier Science, pp. 2115-2125, (2003)

[3] Pigeon, S., Vandendorpe, L., "Image-based multimodal face authentication", *Signal Processing* Volume:69, issue: 1, August 31, pp. 59-79, (1998)

[4] Leca, R. Groza, V., "Online Personal Identification Agent", *IEEE International Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Security*, Orlando, FL, USA, 29-30 March, IMS 2005, (2005)

[5] You, J., Zhang, D., Cao, J., Minyi, G., "Parallel biometrics computing using mobile agents", *Parallel Processing, 2003. Proceedings. 2003 International Conference on*, 6-9 Oct., pp. 305-312, (2003)

[6] Sterritt, R., Garity, G., Hanna, E., O'Hagan, P., "Autonomic Agents for Survivable Security Systems", 1st *IFIP Workshop on Trusted and Autonomic Ubiquitous and Embedded Systems (TAUES 2005)*, at EUC'05, Nagasaki, Japan, 6-9th December, in "LNCS 3823", (2005)

[7] Swiniarski, W. R., "An Application of Rough Sets and Haar Wavelets to Face Recognition", in *Revised Papers from the Second International Conference on Rough Sets and Current Trends in Computing,* Springer-Verlag,, pp. 561-568, http://portal.acm.org/citation.cfm?id=646472.692649, (2001)

[8] Belhumeur, N.P., Hespanha, P.J., Kriegman, J.D., "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," IEEE Transactions on *Pattern Analysis and Machine Intelligence*, 19, no. 7, pp. 711-720, (1997)

[9] Rowley A. H., Baluja, S., Kanade, T., "Neural Network-Based Face Detection," *IEEE Transactions On Pattern Analysis and Machine intelligence 20*, pp. 23--38, doi:10.1.1.110.5546, (1998)

[10] Viola, P., Jones, M., "Robust Real-time Object Detection", *International Journal of Computer Vision*, doi:10.1.1.23.2751, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.2751, (2001)

[11] Papageorgiou C,, Poggio T. "A trainable system for object detection", *International Journal of Computer Vision,* vol 38, No. 1, June 2000, pp. 15-33.