Access Control to Security Areas Based on Facial Classification

Aitor Moreno Fdz. de Leceta\textsuperscript{1,*} and Mariano Rincón\textsuperscript{2}

\textsuperscript{1} Intelligent Systems of Control and Management Department, Ibermática
Parque Tecnológico de Álava, c/Leonardo Da Vinci, 9 2ª Planta - Edificio E-5
01510 Miñano, Álava, Spain
ai.moreno@ibermatica.com

\textsuperscript{2} Departamento de Inteligencia Artificial, Escuela Técnica Superior de Ingeniería Informática, Universidad Nacional de Educación a Distancia,
c/ Juan del Rosal 16, 28040 Madrid, Spain

Abstract. The methods of biometric access control are currently booming due to increased security checks at business and organizational areas. Belong to this area applications based on fingerprints and iris of the eye, among others. However, although there are many papers related to facial recognition, in fact it is difficult to apply to real-world applications because of variations in lighting, position and changing expressions and appearance. In addition, systems proposed in the laboratory do not usually contain a large volume of samples, or the test variations not may be used in applications in real environments. Works include the issue of recognition of the individual, but not the access control based only on facial detect, although there are applications that combine cards with facial recognition, working more on the verification that identification. This paper proposes a robust system of classification based on a multi-layer neural network, whose input will be samples of facial photographs with different variations of lighting, position and even time, with a volume of samples that simulates a real environment. Output is not the recognition of the individual, but the class to which it belongs. Through the experiments, it is demonstrated that this relatively simple structure is enough to select the main characteristics of the individuals, and, in the same process, enable the network to correctly classify individuals before entering the restricted area.

1 Introduction

Face recognition is one of the problems that most challenges are proposing to technical computing nowadays, especially in security systems. Face is the most frequently used way to identify another individual. For this, the brain begins to establish the physical aspects of a face, and then determines whether these factions are known or not, and finally gives a name to what he sees \cite{11}. This process seems so simple for us, but it can be very difficult for a machine. Therefore,

\* Corresponding author.
before developing a biometric system, scientists have been dedicated to analyze the mental processes of facial recognition. So, they have found, for example, that there is a region in the back of the brain that responds preferentially when faces are detected in contrast with other parts of the anatomy or objects [6]. There is also evidence that the face gesture interpretation processes are independent of face identification [13], so a good system for facial recognition should be invariant to facial expression. A final challenge to overcome is the process speed: systems must operate in real time, with a very fast response time, and with the possibility of learning from failures.

This paper presents a part of a prototype for a logistics company access control, in which a winch or a door is connected to a camcorder, detecting a person who is going to enter into the lathe and approve or deny his access. In the case of denied access, an operator will record the identity of the individual, reclassified to next visit, if competent. The information is contained in the weights of a neural network. The use of the network can discriminate whether a record belongs to the set of authorized people or not, but can not retrieve the record. With this restriction, the network achieves a much higher ratio of capacity of discrimination compared to other models. The system requirements are an acceptable response time to a particular discrimination, easy deployment, and a robust and flexible learning process with unknown individuals and misclassification errors. The proposed solution offers some advantages over other methods of access control as a cheap solution, since it requires no expensive hardware and a non-intrusive architecture, with the advantage that the user should not do anything to access into the control area.

2 Prototype Description

The solution developed in this project is based on a grayscale image as input, linked to a classifier built on a multilayer neural network with backpropagation. The novel aspects incorporated are:

- **Use of neural networks for facial classification, not only as final classifier but also as feature detector:** As is clear from the state of the art [10], neural networks have been used in facial recognition systems to classify the characteristics of an individual. This characteristics or features are previously obtained by another processes and usually reduced with some feature reduction methods. This paper demonstrates that a single neural network is sufficient to make a correct classification of images of individuals without a prior extraction of key features. In other words, the network is capable of extracting intrinsic features before making the final classification.

- **Classification of individuals, without identifying them individually:** Another new aspect of this work is the classification of individuals into groups, forgetting the identification of each individual, looking for a technique that combines efficiency, adaptation, very short response times even with general purpose hardware (cameras and computers) and easy configuration.