PCA Face Verification System Using Smart Cards

Alejandro Lara, Gualberto Aguilar, Gina Gallegos
Mechanical and Electrical Engineering School of National Polytechnic Institute of Mexico. Mexico, Mexico D.F.

Abstract - This paper proposes a three factor verification system based on PCA face recognition for smart cards implementation to address some possible vulnerability on smart cards that would allow identity theft. The proposal aims to combine the robustness provided by smart cards and face recognition via PCA approach using ANN. The limited storage capacity on smart cards was a prior consideration on the system design. The results were obtained using the Faces94 database that includes sequence photographs of 153 subjects (20 females and 133 males) with facial expression changes. The proposed method tests showed that the system given an appropriate threshold value provides a good recognition rate and a low false acceptance.

Keywords: Biometrics, Smart cards, Face recognition, PCA, Eigenfaces

1 Introduction

Secure authentication and verification systems for many application domains: transaction protection, access control, computer and network security are becoming increasingly important for organizations and individuals. Providing mechanisms that guaranty security regarding the identity of individuals in an efficient way has become one of the main challenges that the IT community faces.

One alternative that is widely used in industry to authenticate individuals, their transactions and access control mechanisms are based on secret keys and tokens such as smart cards. Smart cards are advanced embedded systems consisting of pocket-sized cards with integrated circuits plastic with storage capacity and that allow the execution of some programmable logic. These types of cards have advantages such as comfort, ease of use, portability, processing and safe storage. [1] However, several vulnerabilities and concerns have arisen toward their use regarding the safety of the stored data which can lead to counterfeiting and identity theft [2].

For these reasons, even though smart card contribute to access control, they do not guarantee by themselves, the identity of the person who is using them, it is possible to strengthen the use of smart card using biometrics recognition. Biometrics refers to the automatic identification of individuals based on physical or behavioral traits associated with the person under the premise that each of these characteristics is unique such as fingerprints, iris, face, retina, and hand geometry [3].

Biometrics is an active research area; particularly face recognition is of great interest due to its non-intrusive recognition and straightforward method for recognizing people. In order to provide the highest degree of confidence in identity verification, biometric technology is considered to be essential in a secure identification system design. [4]

The general structure of biometric system basically consists of an enrollment stage and matching or test stage [5]. In the enrollment the biometric sample of the individual is captured to create the user’s biometric template and it is stored in a database or on a machine-readable ID card for later use. This process is shown on Figure 1.

Figure 1: Enrollment stage of a biometric system

In the matching or test process, a biometric sample is again captured to create a live biometric which will be compared with the previously stored and a numeric matching score is generated on templates similarity. This process is shown in Figure 2.

Figure 2: Test stage of a biometric system
Combining smart card technology with biometrics provides the means to create a positive binding of the smart card to the cardholder thereby enabling strong verification and authentication of the cardholder’s identity [5]. However, due to the limited capacity of storage of smart cards, face recognition and other biometric verification algorithms cannot be applied straight forward [6].

In this research, we present an alternative to solve the problem by the creation of a verification system that combines the robustness provided by smart cards and a PCA approach for face recognition patterns and ANN. The paper is organized in 5 sections, in section 1 an introduction and a brief description of the problem is presented. In section 2 we describe the PCA analysis. Section 3 presents the proposed system, in section 4 the most important results are shown and finally in section 5 some conclusions are drawn.

2 PCA Analysis

The principal component analysis (PCA) for face recognition, also called Eigenfaces proposed by Turk and Pentland in 1991[7], is a well-known statistical technique for dimensionality reduction. This multivariate analysis method aims to project faces onto a feature space that spans the significant variation among a set of known faces.

In other words, it obtains an optimum linear subspace form a covariance matrix of a set of samples[8]. The Eigenface approach is considered an appearance base method since it uses the whole face region as a raw input to a recognition system. The main advantage of PCA is that it allows compressing patterns in data, without much loss of information.

The PCA can be divided in two main processes: the eigenfaces generation which belongs to the training stage and the projection of the test image projection part of the verification stage.

Figure 3 summarizes the process for training images. Firstly the matrix $X$ is created by converting the training images into column vectors, the $\Psi$ average face is computed, and this average face is subtracted from each of the training images, then the co-variance matrix $C$ is computed and finally the eigenvectors and its corresponding values are calculated storing just $K$ eigenvectors with corresponding highest eigenvalues.

On the other hand, Figure 4 shows the process for test images. To project the image, initially the image is converted to column vector, and then the average face $\Psi$ from the training process is subtracted, subsequently it is projected into the eigenspace resulting in a projected test image.

3 Proposed system

Since the proposed system is based on a biometric system, it is structured in two main stages: the enrollment or learning phase and the test or verification phase. The enrolling phase objective is to generate a PCA reference model from a set of training images, while the test phase’s objective is to use this model to verify unknown captures of an individual face. In Figure 5 a high level scheme of the system is depicted.
3.1 Enrolling phase

The enrolling phase comprises the following modules: a) image acquisition, b) PCA feature extraction, c) ANN training, d) neuron weights encryption and e) storage of encrypted weights on smart card. In this phase, a smart card is customized to authenticate the card holder’s identity on a three-factor basis: a token (the cards physical possession), the knowledge of an eight digit Personal Identification Number (PIN) and biometric feature (face image capture).

For the implementation of this proposal, a 32kb smart card with JavaCard technology was used, a pc with a webcam and a smart card reader. The use of a JavaCard was mainly motivated by its ease of use and capability to deploy applications for smart cards more quickly[1]. It is important to note that JavaCards are compliant with ISO e 7816 standard.

In this phase, instead of storing directly the template in the smart card for latter comparison to a live capture stored in the smart card as discussed in section I in a traditional biometric systems using smart cards [5], in this proposed system the trained weights of a backpropagation neural network are stored in the card. Following this approach, it is possible to provide an additional security layer in case the data of the card or the database.

Considering one of the characteristic of neural networks are exposed is that are seen as black boxes [9] leading to less information for a malicious entity even though the information of the card could be retrieved for known vulnerabilities such as differential power analysis, timing attacks, flaws in design or implementation, among others [2].

A set of images are collected from the user to train the ANN. These images are transformed into feature vectors and are used in conjunction with other users training set image feature vectors to train the ANN for verifying that individual’s identity. Once the training and test images have been projected to a lower dimensional space using the Eigenfaces PCA approach, the resulting set of m-size vectors is used to train back-propagation neural network.

Back-propagation learning algorithm was selected for the proposed system for its linearity and powerful mapping of network. Another important consideration of the network’s architecture was its level of complexity. Due to storage constraints that smart cards present, the network architecture was designed to be as simple as possible trying to reduce the number of neurons and hidden layers without compromising the verification capabilities of the network.

The back-propagation network is trained in such a way that for a feature vector that corresponds to the subject of interest, the network will output 1 and 0 otherwise. When the training stage is over (the training error has reached a specified threshold), the weight vectors are encrypted using the AES cipher by a user specified key and stored into the smart card for later use in the test stage. In Figure 6, an example of an ANN used in the proposed system is shown.

![Fig. 6. Example neural network](image)
3.2 Test phase

Once the enrolling phase is concluded and a smart card is issued for an individual it can be used to test the card holder’s identity. In the test phase, the smart card is inserted in a Card Acceptance Device (CAD) and the PIN is solicited to the user. In case this secret key matches the one established in the enrolling phase, the decryption of the stored weights in the cards proceeds, a test image of the card holder’s face is taken, projected to the PCA space, and given as an input to a reconstructed neural network with weights \( w \). Finally the neural network outputs “1” if the card holder authenticates correctly, and outputs “0”.

4 Results

The proposed system for face recognition using smartcards was tested on the Faces94 database [10]. This database contains images from 153 individuals (20 women, 133 male), which were taken under controlled conditions such as lighting, background uniformity, head turn, tilt and salt and expression variation. Sequences of 20 photographs per individual were taken at a fixed distance from the subject while speaking to introduce facial expression variation. A sample of face images from the Faces94 database is shown in Figure 7.

![Fig. 7 Sample images from Faces94 database](image)

In order to validate the proposed system two main tests were made. On the first test, 1740 face images belonging to 50 individuals were processed. Fourteen images per individual were used in the training phase for generating a template per individual calculating the PCA. An ANN was trained with these PCA vectors considering a training error of 0.01%. Once the ANN train process concluded, the 6 remaining images of the individuals (from the 20 sequence per individual) were presented as input to the trained system. Considering these outputs a threshold of 0.15 was found efficient to reach a 100% recognition rate from individuals belonging to the training set.

On the second experiment, given the threshold obtained on the previous test, the system was presented with a set of 750 fully unknown face images (individuals not contained in the training set) to observe the system response to reject newly unauthorized subjects. In this test given a 0.15 threshold only 4 false acceptances were obtained.

5 Conclusion

In this paper, a novel system for identity verification using PCA face recognition techniques in conjunction with smart cards technology was presented. The proposed approach used PCA for face image extraction and the trained weights of an ANN to customize a smart card for verifying an individual’s identity. Experimental results showed that the system given an appropriate threshold value provides a good recognition rate and a low false acceptance. Moreover, the size of training weights is suitable for implementation in the limited storage space of smart cards. The security layer provided by face biometrics in addition to a two factor authentication system of smart cards (possession and knowledge of a secret PIN) widely used in industry creates a three factor authentication system that we believe is a good candidate for enhancing security in access control systems, especially in scenarios where smart cards are already used for this purpose.
6 References


