

# How to deceive a face recognizer?

B. Gökberk, L. Akarun, B. Aksan  
Computer Engineering Dept., Boğaziçi University  
{gokberk, akarun, aksan}@boun.edu.tr

## Abstract

*Many security systems depend upon face recognizers to identify a person. Many of these systems are passive and are deployed at places such as airline terminals. However, face recognizers are sensitive to deception attacks. Previous studies suggest that hair regions are very crucial in face recognition and the success of a recognizer depends on the success of a pre-segmentation stage which extracts the face region from the hair and the background. Deception attacks which would change the hairstyle, apply make-up or occluding objects to the face would cause many systems to fail. In this study, we study the effects of deception attacks on two basic face recognition systems: a PCA-based system and a Gabor wavelet-based recognizer. We study the performance of the recognizers under different attacks and focus on the selection of features so as to maximize performance under attacks.*

## 1. Introduction

Over the past two decades significant progress has been made in the automatic human face recognition research. Although many successful face recognition systems have been proposed in the literature, the problem is still not considered to be fully solved, especially in real-life applications. The main obstacle can be simply stated as follows: intra-personal variations between human faces is large when compared to inter-personal variations. These variations can be broadly classified into two groups: *external variations* and *internal variations*. Variations due to illumination, head pose, scale and translation are considered to be external variations. However, variations due to hair color, hair style, moustache, beard and eyeglasses as well as facial variations which stem from the subject itself are considered to be internal variations.

One of the studies dealing with internal variations such as expression changes and occlusion is [1], where the AR face database is used to illustrate the superior performance of a local probabilistic approach. The local component

based approach has also been studied to deal with external variations in face recognition [2, 3]. When occlusions such as beards and glasses are present, a different approach is to try to remove them [4, 5].

In this paper, our aim is to examine how an impostor can deceive a face recognizer by taking the advantage of internal variations; specifically hair color change, occlusions, and expression variations. After analyzing the effects of such variations aiming to deceive a recognizer, we propose a robust technique that increases the performance of PCA and Gabor-based face recognizers.

## 2. Face Representation

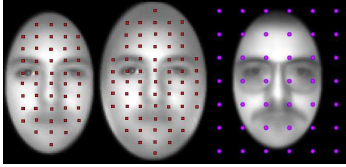
### 2.1. PCA-based Method

In PCA, faces are expressed as linear combinations of the eigenvectors of faces. Then, for recognition, the PCA coefficients can be used to denote a face. In its original form, PCA is found to be rather sensitive to image intensity variations, local perturbations, and needs almost perfect correspondence. Image variations which are not present in the training phase generally cause a poor recognition performance. A possible solution to improve the PCA method is to divide the whole face region into subregions and do modular PCA analysis. In a modular PCA analysis, each subregion is handled in isolation, and for each subregion, a different subspace is found. Then local features are extracted and merged to represent a face. An important advantage of modular PCA analysis is that local perturbations can only affect the local coefficients, not the whole face. Figure 1.c shows subregions that we have used in our experiments.

### 2.2. 2D Gabor Wavelet-based Method

A biologically motivated representation of face images is to code them using convolutions with multi-frequency multi-orientation 2D Gabor-like filters. In order to represent face images using Gabor filters, the intensity image is convolved by Gabor kernels. The set of convolution coefficients for kernels of different orientations and frequencies

at one image pixel constitutes local feature vectors. Local feature vectors are then merged to represent whole face. In this work, we employ Gabor filters as in [6], and use uniform grid-based sparse representation (see Figure 1).



**Figure 1. Gabor sampling grid points: (a) Small ellipse, (b) Large ellipse (c) Local PCA regions**

### 3. Similarity Measure and Classifier

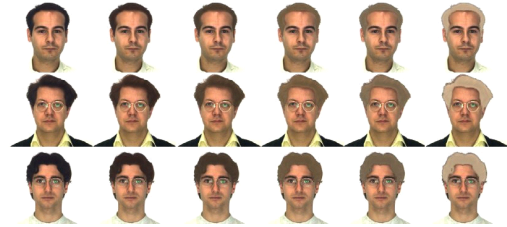
In both original PCA-based and Gabor wavelet-based recognition methods,  $L_2$ -norm similarity measure is used where classification is done via 1-nearest neighbor algorithm. Although comparing two faces in modular PCA-based approach can be simply done by  $\|I_i - I_j\|$  where  $\|\cdot\|$  denotes  $L_2$ -norm, a more robust distance measure can be used by taking advantage of the locality principle. Let  $I_i = \{V_1^i, V_2^i, \dots, V_p^i\}$ , and  $I_j = \{V_1^j, V_2^j, \dots, V_p^j\}$  be two global feature vectors for two different images, and let  $d = \{\|V_1^i - V_1^j\|, \|V_2^i - V_2^j\|, \dots, \|V_p^i - V_p^j\|\}$  be local Euclidean distance vector between corresponding local feature vectors. Here, each component in the  $d$  denotes how similar the local regions are in two images. For robustness against outlier regions, one can simply discard some subregions having smallest similarities, and select  $t$  subregions having greatest similarities, and then calculate the overall  $L_2$ -norm of this selected subregions. In this paper, we call this technique as asymmetric trimmed distance measure (ATDM). ATDM can also be applied to the Gabor wavelet-based representation technique by selecting most similar  $t$  local features among the global feature vectors.

## 4. Experimental Results

### 4.1. The Effect of Hair Color Change

In our experiments, we have used a subset of AR face database. For hair color experiments, we have selected four neutral images from 20 males and 20 females where the first two images are from the first session and the other two are from the second session. For each image, we have automatically generated six synthetic face images in increasing order of hair color change from darker color to lighter

color. Faces are normalized and rotated according to eye coordinates. After normalization, faces are cropped by an ellipse mask. In hair color experiments, two different ellipse masks are employed. The small mask covers the face outline whereas the large mask covers a wider region that includes the chin and the ears. Samples of original images and six synthetic images for three subjects are shown in Figure 2. Small and large ellipse masks are shown in Figure 1.

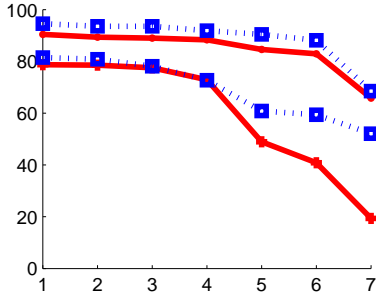


**Figure 2. Sample images from hair dataset**

In order to see the effect of hair color change, we have designed seven experimental setups. We have four original images per person, and six differently colored synthetic sets where each set contains four images that are modified from original images. Let  $S_0 = \{I_0^1, I_0^2, I_0^3, I_0^4\}$  be the original set of images of a person and  $S_i = \{I_i^1, I_i^2, I_i^3, I_i^4\}$ ,  $i = 1 \dots 6$  be the synthetic image sets of a person. In the first experiment, denoted by  $H_1$ , we put two images from  $S_0$  to the training set, and the remaining two images of  $S_0$  to the test set. Since there are six possible configurations for training set image selection,  $H_1$  has six training-test set configurations. Similarly in  $H_2$ , six different training sets are formed from  $S_0$  (original images) containing two images per person, and test sets are formed from  $S_1$ . So in each one of the six different configurations in  $H_2$ , we ask our algorithm to recognize synthetically modified two test images where the training set contains two original images. In such a setup, the first experiment,  $H_1$  determines the baseline classification accuracy of our recognizers, whereas experiments  $H_2 \dots H_7$  determine how much the increasingly modified hair color affects the recognition performance.

In the PCA method, we represent each face image using the first  $k = 40$  PCA coefficients. In the Gabor method, we identify uniform grid-like regions in ellipse masks (see Figure 1). The number of grid points is  $g = 47$  for the small ellipse mask, and  $g = 65$  for the large ellipse mask. At each grid point, local features of dimensionality  $5 \times 8 = 40$  are extracted, and then global feature vector is formed by concatenating these. Table 1 displays the classification performances of PCA and Gabor methods on seven experiments. Figure 3 plots the results on Table 1. It is clear from Figure 3 that as the hair color change increases the recognition performances of both PCA and Gabor methods decreases.

However, Gabor method outperforms PCA in all experiments, and its performance is more resistant than PCA. This behavior is especially clear when going from  $H_4$  to  $H_5$ . We also see that larger ellipse is better when hair color change is minimal.



**Figure 3. PCA and Gabor performances on small ellipse hair dataset for Euclidean (red lines) and robust ATDM (blue dotted lines)**

In the previous section, we saw that intensity variations around the hair region cause the deterioration of both PCA and Gabor-based classifier accuracies. This is an expected result especially for the PCA method because it is known that PCA runs into problems when it is required to code an unknown test image having variations which are not adequately present in the training set. PCA can not generalize well if the learning set (training images) does not cover all possible variations. In our experiments, training images are selected from original faces, and hair color variations are not present in training sets. This explains the poor generalization. For the Gabor method, the local features extracted from hair regions will be different, and this explains the performance drop. The reason why Gabor method performs better than PCA is that Gabor filters are less sensitive to intensity changes, and respond edge-like features in these regions.

After training the PCA and Gabor techniques against internal variations, we applied the robust similarity measure defined in Section 3. Since the PCA technique has shown inferior results, we use modular PCA in combination with the robust distance measure. The recognition accuracies of modular PCA and Gabor wavelet-based robust ATDM are shown in Table 1. Figure 3 depicts these results. In Figure 3, we see that ATDM outperforms the baseline PCA and Gabor methods especially in the difficult experiments, e.g.  $H_5, H_6, H_7$ . This is an important observation: ATDM improves the performance when there are highly variable subregions.

We have also performed additional experiments where some synthetically modified images are put into the train-

ing set in order to better reflect the variations. The results have shown that adding the synthetic images to the training set, especially the ones with more variation from the original hair color, generally increased the recognition accuracy of the PCA-based representation, as expected. However, the Gabor-based classifier and PCA-based classifier with ATDM did not have a considerable amount of increase in performance.

## 4.2. Eyeglasses and Moustache

Among internal variations besides hair color change, eyeglasses and moustache differences may be used for deception attacks. To analyze the effects of such variations, a different subset of the AR face database is used. 40 males are selected from the dataset where each male has two neutral images, two images having slight expression variations, and two images with dark eyeglasses. Let  $S_n$ ,  $S_e$ , and  $S_g$  denote these image sets respectively. Each set contains two images. We automatically generate synthetic sets from these images by adding moustache to each individual set, and obtain synthetically generated sets:  $S_{nm}$ ,  $S_{em}$ ,  $S_{gm}$  respectively. Sample images from these sets are shown in Figure 4.



**Figure 4. Sample images from the eyeglasses/moustache dataset.**

We have designed five experiments to analyze how face recognizers behave under expression, eyeglass, and moustache variations. The training and test set configurations are as follows:  $E_1 = (\text{Tr}: \{S_n\}, \text{Ts}: \{S_e\})$ ,  $E_2 = (\text{Tr}: \{S_n, S_e\}, \text{Ts}: \{S_g\})$ ,  $E_3 = (\text{Tr}: \{S_n\}, \text{Ts}: \{S_{em}\})$ ,  $E_4 = (\text{Tr}: \{S_e\}, \text{Ts}: \{S_{nm}\})$ ,  $E_5 = (\text{Tr}: \{S_n, S_e\}, \text{Ts}: \{S_{gm}\})$

Table 2 shows the recognition accuracies for both standard PCA and Gabor methods and their robust versions on small and large ellipse masks. PCA results show that adding moustache does not cause significant performance degradation. This can be seen by comparing the accuracies in  $E_1$  experiments to the accuracies for experiments  $E_3$  and  $E_4$ . Although robust version has an improved accuracy in eyeglass experiments ( $E_2, E_5$ ), both PCA versions perform poorly. Note that ellipse size does not effect performance in PCA.

In Gabor results, the robust ATDM generally outperforms the standard version. Also, large ellipse mask has performed better than the small one. Moustache experiments

**Table 1. Classification accuracies of PCA and Gabor methods for hair dataset.**

	PCA				Gabor			
	Small Ellipse		Large Ellipse		Small Ellipse		Large Ellipse	
	Euc.	ATDM	Euc.	ATDM	Euc.	ATDM	Euc.	ATDM
$H_1$	78,75	81,46	78,54	86,25	90,42	94,58	88,13	93,13
$H_2$	78,54	80,83	77,92	85,83	89,38	93,54	86,25	91,67
$H_3$	77,50	78,13	77,71	82,71	88,96	93,54	85,83	91,46
$H_4$	72,92	72,71	72,29	76,04	88,33	91,88	84,58	90,83
$H_5$	48,96	60,83	44,79	63,33	84,58	90,42	82,92	90,00
$H_6$	40,83	59,38	36,04	56,88	82,92	88,13	82,71	90,00
$H_7$	19,38	52,08	17,92	54,38	65,83	68,54	76,04	83,54

**Table 2. Eyeglasses/Moustache Experiments**

	$E_1$	$E_2$	$E_3$	$E_4$	$E_5$
	PCA				
Euc. (S)	78.75	15.00	80.00	70.00	11.25
ATDM (S)	82.50	35.00	83.75	68.75	28.75
Euc. (L)	78.75	15.00	80.00	70.00	11.25
ATDM (L)	82.50	35.00	83.75	67.50	28.75
	Gabor				
Euc. (S)	71.25	21.25	78.75	76.25	16.25
ATDM (S)	78.75	28.75	81.25	85.00	20.00
Euc. (L)	85.00	48.75	87.50	83.75	50.00
ATDM (L)	85.00	70.00	86.25	91.25	60.00

( $E_3$ ,  $E_4$ ) show that both standard and improved robust Gabor method is superior to PCA. This situation is especially visible in eyeglasses experiments where robust ATDM improves from 35.00 percent (PCA) to 70.00 percent in  $E_2$ , and from 28.75 percent (PCA) to 60 percent in  $E_5$ . However, since dark eyeglasses cover most of the discriminative regions in the human face, small ellipse masks can not provide useful information enough for recognition. This explains poor accuracies in the Gabor method, i.e., 28.75 percent recognition accuracy in  $E_2$  using the robust ATDM method.

## 5. Conclusion

In this paper, we analyze several deception attacks which use internal facial variations such as hair color change, expression variations, and occlusions by moustache and eyeglasses. Results show that both PCA-based and Gabor wavelet-based face recognizers are sensitive to these variations, although the latter generally outperforms the first. In hair color experiments, we see that PCA performance deteriorates drastically, while Gabor-based classifier is more robust to color changes. In eyeglasses experiments, since

a large portion of a face is occluded, both approaches perform poorly. It is also shown that adding moustache does not effect the recognition rate significantly. After these observations, we propose a robust classifier which uses asymmetric trimmed distance measure. This distance measure is suitable for modular representations. Therefore, a modular PCA algorithm is used to represent local facial regions. Our experiments show that using asymmetric trimmed distance measure with modular PCA and Gabor methods significantly improves the recognition performance when test images have considerable variations such as hair color change and eyeglasses.

## References

- [1] A. M. Martinex. Recognizing imprecisely localized, partially occluded, and expression variant faces from a single sample per class. *IEEE Tran. on PAMI*, 24(6):748–763, 2002.
- [2] R. Gottumukkal and V. L. Asari. An improved face recognition technique based on modular pca approach. *Pattern Recognition Letters*, 25(4):429–436, 2004.
- [3] B. Heisele, P. Ho, J. Wu, and T. Poggio. Face recognition: Component-based versus global approaches. *Computer Vision and Image Understanding*, 91(1/2):6–21, 2003.
- [4] Bon-Woo Hwang and Seong-Whan Lee. Reconstruction of partially damaged face images based on a morphable face model. *IEEE Tran. on PAMI*, 25(3):365–372, 2003.
- [5] C. Wu, C. Liu, H.-Y. Shum, Y.-Q. Xu, and Z. Zhang. Automatic eyeglasses removal from face images. *IEEE Tran. on PAMI*, 26(3):322–336, 2004.
- [6] L. Wiskott, J. M. Fellous, N. Kruger, and C. Malsburg. Face recognition by elastic bunch graph matching. *IEEE Tran. on PAMI*, 19(7):775–779, 1997.