A robust feature-based technique for watermarking frontal face images

Athanasios Nikolaidis Ioannis Pitas
Department of Informatics
Aristotle University of Thessaloniki
Box 451, Thessaloniki 540 06, GREECE
E-mail: {nikola, pitas}@zeus.csd.auth.gr

1 Introduction

The vast progress of multimedia systems during the last years has offered many chances for malicious attacks on all types of electronic forms of data, such as images, audio and video. This addressed the need to develop robust techniques that provide copyright protection of multimedia information.

Many different watermarking methods for images have been proposed until now, that can be divided into two wide categories: those directly applied on the pixel intensities of the image (e.g. [1]), and those making use of a transform domain to exploit image frequency properties (e.g. [2]). All of these techniques have in common the fact that the image is treated as a single object and no special attention is paid on selecting certain features or areas of the image that would remain unchanged after some unexpected manipulation. This paper presents a technique for watermarking frontal face images based on extracting a finite set of features that are robust under such attacks. Experimentation is being done in the direction of finding ways to extract robust features for any class of images.

2 Salient feature extraction

Our attention throughout this paper is focused in finding certain facial features that will help us embed the watermark in a way that will be easy to retrieve even after some geometric manipulation such as rotation, scaling or cropping.

Several methods have been proposed during the past for extracting facial features as in [3] or [4]. However none of them impose any kind of constraint for the extracted features to be robust against any kind of intended manipulation, such as JPEG compression, lowpass filtering and geometric changes to the initial image.

In this paper we propose the embedding of a chaotic watermark [5] in a region of the image that is accurately defined by choosing salient face image features, notably the eyes and mouth.

First we find the representation of the image in the HSV colour space, and afterwards employ a color segmentation technique that recognizes skin-colour areas as ones having hue, saturation and luminance parameters falling inside certain ranges. The output is a binary map of the image containing skin-coloured and non skin-coloured pixels. A connected component algorithm detects all the skin-coloured compact regions and the largest of them is selected as the one representing the face region. By moments computation we can calculate the orientation of the face region with respect to the $z-$axis.

We choose to consider the eyes and the mouth as significant features that can be localized by employing a pattern matching technique. Specifically, we model each eye by a weighted sum of an ellipse function and a circle fuction that is centered inside the ellipse. The radial of the circle equals the minor semiaxis of the ellipse. Pixels inside the circle are expected to have low intensity values, whereas pixels outside the circle but inside the ellipse are expected to have high intensity values. We assume that the difference between the weighted sum of intensity values inside the circle and the weighted sum of intensity values outside the circle but inside the ellipse should be

minimal. The common center of both the circle and the ellipse that minimizes the output of the shape matching algorithm is selected as the potential eye position. The search is made after a normalization of the face region according to the orientation that was calculated in the segmentation step. Optimal values for the weights are computed by imposing the constraint that the difference of the weighted sums should be ideally equal to zero. The mouth is similarly modeled by two ellipse functions having the same center and similar sizes.

The output of the above mentioned process provides us with a set of features (eyes and mouth position) which, together with the orientation information, is used for embedding and detecting the watermark.

3 Watermark generation and embedding

Once the extracted features are available, the watermark is embedded in a rectangular region that is centered in the mass center of the feature points and has width and height that are defined so that watermark covers the entire facial region.

A chaotic watermark [5] is chosen to be embedded because of its good lowpass properties that make it robust against filtering and JPEG compression. A chaotic sequence is first produced according to a specific function and is afterwards traversed in a Peanno scan manner to preserve its lowpass properties in two dimensions. A prototype watermark of fixed size is produced in this way. The initial image is first rotated according to the face orientation and the watermark is scaled to the dimensions of the above mentioned facial region. The scaled watermark is then embedded in the rotated image, centered in the mass center of the salient features. The resulting image is rotated back to the original orientation, producing the desired watermarked image.

4 Watermark detection

In the detection stage, the watermarked image is again segmented and the desired salient features (eyes, mouth) as well as the face region orientation are extracted. The image is rotated and the rectangular region is defined based on the features. The prototype watermark is scaled to the same dimensions and finally a statistical correlator is employed in order to decide about the presense or absense of the specific watermark.

The process followed throughout both embedding and detection stages compensates for any geometric distortion of the watermarked image, such as scaling, rotation and cropping, as well as for any combination of them. The feature points show a significant robustness in localization to any of these geometric attacks as well as to lowpass filtering and JPEG compression as we have seen in our experiments. The detector response is thus retained even at high compression values (e.g. 1:50), as experimental results showed in a large frontal face image database.

References

[1] N. Nikolaidis and I. Pitas, "Copyright Protection of Images using Robust Digital Signatures", in *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing, ICASSP '96*, May 1996, Atlanta, Georgia, vol. 4, pp. 2168-2171.

[2] I. J. Cox, J. Killian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", in *IEEE Trans. on Image Processing*, **6**(12), pp. 1673-1687.

[3] K. Sobottka and I. Pitas, "A novel method for automatic face segmentation, facial feature extraction and tracking", *Signal Processing: Image Communication*, **12**(3), pp. 263-281.

[4] S. Tsekeridou and I. Pitas, "Facial feature extraction in frontal views using biometric analogies", in *Proc. of EUSIPCO '98*, September 1998, Rhodes, Greece, vol. 1, pp. 315-318.

[5] G. Voyatzis and I. Pitas, "Chaotic Watermarks for Embedding in the Spatial Digital Image Domain", in Proc. of ICIP '98, October 1998, Chicago, Illinois, vol. 2, pp. 432-436.