Combination of face recognition methods with watermarking technology for authentication of digital images

Wioletta WÓJTOWICZ
AGH University of Science and Technology,
Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering,
Department of Automatics and Biomedical Engineering
al. Mickiewicza 30, 30-059 Krakow, Poland
e-mail: wwojtowi@agh.edu.pl

Abstract. As the substantial challenge in providing security of digital images is owners authentication in many security schemes based on cryptography, steganography and watermarking technology, biometric recognition methods are introduced. In the sequel to these studies in presented methodology the combination of biometric recognition methods based on facial images with watermarking technology to perform automated authentication of digital images owners/users is elaborated. Presented approach involves computing reduced face image representation (feature vector) and embedding it in some cover image in a few watermarking schemes. The robustness of watermarking algorithms is measured by identification accuracy results obtained using neural networks (NN).

Keywords: watermarking technique, biometrics, face recognition, principal component analysis, neural networks (NN)

Introduction

As modern society relies on digitalized information, security technologies for protecting rights of data owners are required. Taking into account digital images, to ensure that they are transmitted from the correct sources to the claimed receivers (authentication), many security solutions including cryptography, encryption, steganography and watermarking have been elaborated (e.g., [3]). Increasingly such technologies are combined with biometrics ([1], [3], [5]). In the present study to increase the security of digital images biometric watermarking using face feature vectors as watermarks is proposed.

Proposed methodology

As face images serve a means to identify subjects they are used to construct personalized watermarks, that enable images owners identification. The entity of this approach is that instead raw face image (from AT&T database [6]) just feature vectors obtained using machine learning method, Eigenfeature Regularization and Extraction (ERE) ([5]), are inserted. Then these vectors undergo a few common watermarking schemes based on Discrete Fourier Transform, Discrete Cosine Transform and Discrete Wavelet Transform. Initially watermarking algorithms are studied with some arbitrary cover image and additionally the most robust algorithm is tested for different cover images of particular subjects (40 people). After watermark extraction, subject identification is performed using neural networks, that are frequently used classifier also in traditional face recognition problems.

Results

The experimental results show that in many elaborated watermarking scenarios, incorporating also some processing of watermarked images, users authentication was performed at considerable high level of accuracy (around level 90%). Furthermore, the watermarking algorithm in DCT domain was the most robust in terms of providing the highest identification accuracy, regardless of attacks performed on watermarked images. In general, combination of watermarking algorithm in DCT domain and face feature watermarks obtained using ERE reduction method provided the highest identification accuracy (around level 95%). The strong point of this paper is that to find relationship between original and extracted biometric data instead using most common and simple measures like correlation coefficients or distance metric, the neural networks (NN) were applied. Using them the subject identification was performed straightforward, as there was no need to reconstruct face images after watermark extraction, compute templates for particular subjects or seek an appropriate distance metric.

Conclusions

As face images provide a means of identifying subjects they are used to construct personalized watermarks, that makes it possible to identify the owners of images. In the presented approach, data projection methods were applied to obtain reduced vectorial representation of face images from the training and testing data sets. These face feature vectors underwent a few watermarking schemes, implemented according to the simplest approaches presented in the literature. Then the performance of these algorithms was evalu-
ated according to the identification accuracy obtained using NNs trained and tested on extracted face feature vectors. The experimental results showed that the proposed method enables authenticating images with a considerably high accuracy.

BIBLIOGRAPHY


Author(s): Wioletta Wójtowicz, MSc - is a PhD candidate at AGH University of Science and Technology, The Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering and an academic assistant at Institute of Applied Computer Science, Cracow University of Technology, Poland. She received her MSc in Mathematics from AGH University of Science and Technology in 2011. Her research interests include digital watermarking, image analysis, biometrics and machine learning methods.