Egyptian Informatics Journal xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Review

The detection of spoofing by 3D mask in a 2D identity recognition system

Bensenane Hamdan *, Keche Mokhtar

Laboratoire Signals and Images, Dept. of Electronique, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO-MB, BP 1505, 3100 Oran, Algeria

ARTICLE INFO

Article history:
Received 2 November 2016
Revised 29 July 2017
Accepted 4 October 2017
Available online xxxx

Keywords:
Anti-spoofing
Angular Radial Transformation (ART)
Linear Discriminant Analysis (LDA)
Support vector Machine (SVM)
Nearest Neighbor Classifier (NNC)

ABSTRACT

Nowadays face recognition systems are facing a new problem after having won the challenge of reliability. The problem is that these systems have become vulnerable to attacks by identity theft. In order to deceive the recognition systems hackers use several methods, such as the use of face images or videos of people belonging to the system database. Luckily, this type of attack is thwarted by the use of adapted systems. But unfortunately another type of attack that uses 3D face masks appeared. This type of attack is very efficient, since as will be shown, a high percentage of hackers who use 3D masks can mislead a good facial recognition system, like the one used in our investigation. In this paper, a new method is proposed for the detection of hackers that use 3D masks to deceive face recognition systems. This method uses the Angular Radial Transformation (ART) to extract pertinent features that are fed into a classifier to decide whether the captured image represents a face image. The performance of the proposed method was evaluated using a public 3D Mask Attack Database (3DMAD). The obtained results show the efficiency of the proposed method, since it can reduce the error rate in discriminating between a real face and a face mask down to 0.90%.

Contents

1. Introduction . . . 00
2. The recognition phase . . . 00
   2.1. Extraction of characteristics . . . 00
   2.2. Classification for recognition . . . 00
3. The verification phase . . . 00
   3.1. Extraction of facial features using the ART . . . 00
   3.2. The ART projection basis. . . . 00
   3.3. Classification in the verification step . . . 00
   3.4. Maximum likelihood classifier . . . 00
4. Experimentation . . . 00
   4.1. The 3DMAD database . . . 00
   4.2. Pretreatment of the images in the database . . . 00

* Corresponding author.
E-mail addresses: hamdan.bensenane@univ-usto.dz, bensenane1300@gmail.com (B. Hamdan), m_keche@yahoo.com (K. Mokhtar).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2017.10.001
1110-8665/

Please cite this article in press as: Hamdan B, Mokhtar K. The detection of spoofing by 3D mask in a 2D identity recognition system. Egyptian Informatics J (2017), https://doi.org/10.1016/j.eij.2017.10.001

4.3. Protocol . . . 00
4.3.1. The recognition phase . . . 00
4.3.2. The verification phase . . . 00
5. Results and discussion . . . 00
5.1. Recognition results . . . 00
5.2. The verification results . . . 00
6. Conclusion . . . 00
References . . . 00

1. Introduction

Today security has become an international concern. Among the fields where the security is a concern, one can cite, as examples: access control to computers, e-commerce, identification based banking, public transport, etc.

A biometric system is essentially a pattern recognition system that uses biometric data of individuals. Depending on the context of the application, a biometric system may operate in the learning mode, verification mode or identification mode. The choice of using facial recognition as a biometric modality is motivated by the fact that it is contactless, natural, well accepted and requires only a very inexpensive sensor (Webcam) that is virtually available on all electronic devices. Furthermore, it requires a small cooperation from the users during the acquisition phase of the facial features.

Automatic face recognition involves two main steps: extraction of facial features and classification. Unfortunately, all the advantages of facial recognition systems have fallen into the water with easy pirating of facial characteristics. The experiments showed that hackers can easily fool facial recognition systems in the acquisition phase of facial features with a simple photo or video recording of the face.

In the case of identity theft by a picture, liveliness detection (eye blinking, facial micro movements...) can distinguish a real face from a picture and thus definitely neutralize this type of hacking.

For video based hacking, the usual approach to detect the attack is to analyze the motion in the scene by examining how objects move in front of the sensor. The movements of the planar objects like screens differ greatly from those of a true face.

Another method, proposed by Bai et al. [1], consists of finding printing artifacts and/or blurring of the texture of the face image to distinguish between a real face and a stroke. For the same purpose, Li et al. [2] proposed a technique based on the analysis of 2-D Fourier spectra. All these attack detection methods have failed to deal with identity usurpation with 3D mask. Indeed, blink detection of eyes and lips movements can be overcome simply by using high resolution printing masks of the eyes and regions of the mouth.

Several research works were carried out to distinguish between a real face and a face mask. The most commonly used approaches rely on distinguishing between the human skin and the facial mask material, thanks to the difference between their light reflecting factors. To this end, the reflectance disparity based on the albedo between facial skin and face mask materials (silicon, latex, etc.) is exploited.

In [3], a 2D characteristic vector composed of 2 radiance measurements under beams of light (685–850) nm is used to detect a fake face, through Linear Discriminant Analysis (LDA). An accuracy of 97.78% was reported. The fact that for mask detection, the measurements of radiation should be acquired at 30 cm on the forehead region, in addition the possibility of occlusion in the forehead and light range limitations, make this method impractical.

Similarly, Zhang et al. [4] proposed a multi-spectral analysis for fake face detection. After measuring the skin albedo curves of the face and mask materials with varying distances, two discriminating wavelengths (850–1450-nm) were selected to train a Support vector Machine (SVM) classifier for discriminating between genuine and false attempts. The experiments were performed on a base of 20 masks of different materials: 4 plastic, 6 silica gel, 4 pulp, 4 plaster and 2 sponge. The results show that the correct classification can attain 89.18% accuracy.

The authors of this experiment did not do their studies with masks that are replicas of real subjects. On the contrary, Kose and Dugelay [5] carried out their work with a database of printed masks of about 16 real subjects. The analyses of the facial features were carried out by a 3D scanner after the masks were realized by means of a 3D printing service. In addition to the texture images, the database also comprises the two samples with real face and face mask for each person. The authors propose a method based on various linear binary pattern (LBP) techniques, for feature extraction using two image types (color and depth) and they claim 88.12% and 86% accuracy both types of images.

In this article we propose a face recognition system that includes a new approach to distinguish between a real face and a face with mask. As shown in Fig. 1, the proposed system consists of two step, a recognition step followed by a verification step, to detect impostors with mask 3D.

The advantage of the proposed approach is that it can be used by any system of recognition that uses RGB images from a simple webcam, unlike other approaches, such as the ones proposed in [3] and [5] that uses special sensors for the acquisition.

The approaches proposed by Kim et al., [3] and Zhang et al., [4] measure the reflected light by probing light waves on the face, which can be damaging and harmful to users' health.

On the contrary, our technique can be used without any risk to the user's health. For the verification stage, Kose and Dugelay [5] use two types of images, a depth one and a RGB one, captured with an adequate acquisition camera. In contrast, our method uses only RGB images that could be acquired by a simple Webcam.

The ART has been widely used in several algorithms, such as logo recognition [8], video surveillance systems [9], face detection [10] and Region-based descriptor in MPEG-7 [11]. It has also been

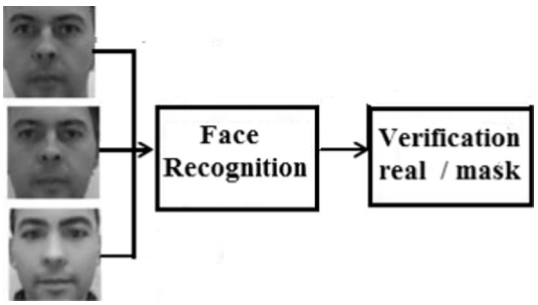

Fig. 1. The principle of detecting impostors in a face recognition system.

Please cite this article in press as: Hamdan B, Mokhtar K. The detection of spoofing by 3D mask in a 2D identity recognition system. Egyptian Informatics J (2017), https://doi.org/10.1016/j.eij.2017.10.001