Information Sciences 268 (2014) 103–121

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A novel hand reconstruction approach and its application to vulnerability assessment

Marta Gomez-Barrero [a,*], Javier Galbally [a], Aythami Morales [b], Miguel A. Ferrer [b], Julian Fierrez [a], Javier Ortega-Garcia [a]

[a] Biometric Recognition Group – ATVS, EPS, Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente 11, 28049 Madrid, Spain
[b] Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC), Universidad de Las Palmas de Gran Canaria, Campus de Tafira s/n, E35017 Las Palmas de Gran Canaria, Spain

ARTICLE INFO

Article history:
Available online 20 June 2013

Keywords:
Biometric system
Hand recognition
Hand reconstruction
Security
Vulnerability

ABSTRACT

The present work proposes a novel probabilistic method to reconstruct a hand shape image from its template. We analyse the degree of similarity between the reconstructed images and the original samples in order to determine whether the synthetic hands are able to deceive hand recognition systems. This analysis is made through the estimation of the success chances of an attack carried out with the synthetic samples against an independent system. The experimental results show that there is a high chance of breaking a hand recognition system using this approach. Furthermore, since it is a probabilistic method, several synthetic images can be generated from each original sample, which increases the success chances of the attack.

1. Introduction

Biometrics are nowadays being introduced into many applications as an alternative to traditional security mechanisms [38,75]. The main advantage of biometric systems is that you no longer need to carry a key or remember a PIN code: you are your own key.

One of the most popular biometric traits deployed by these systems is the hand [61,77]. In the last 30 years, hand recognition devices have been installed in airports, nuclear plants or hotels [49,79]. These systems offer a reliable [30,41,73], low-cost (acquisition can be made by means of commercial low-resolution scanners or cameras) and user-friendly [32,42] solution for a wide range of access control applications.

However, as any other security device, these systems are also vulnerable to external attacks that may compromise their security [62]. Therefore, it is of the utmost importance to understand and analyse these eventual threats in order to increase the security offered by biometric systems.

One of the areas that is more directly related to the vulnerabilities evaluation of biometric systems and that presents a high potential impact in their security, is the reconstruction of a biometric trait starting from the original user template, or *inverse biometrics*. If such an inverse engineering process is possible, an eventual attacker that manages to obtain a template belonging to a certain user (e.g. the iriscode or minutiae template) would be able to reconstruct the original biometric sample and could use it to illegally access the system.

* Corresponding author. Tel.: +34 914973363.
E-mail addresses: marta.barrero@uam.es (M. Gomez-Barrero), javier.galbally@uam.es (J. Galbally), amorales@gi.ulpgc.es (A. Morales), mferrer@dsc.ulpgc.es (M.A. Ferrer), julian.fierrez@uam.es (J. Fierrez), javier.ortega@uam.es (J. Ortega-Garcia).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.06.015

In this context, the ultimate question is: are we able to generate synthetic images whose templates are similar enough to those of the original user? That would mean that given just a template, we are able to reconstruct an image with which we can deceive a recognition system or even steal someone's identity.

In the past, it has been a common belief that templates do not comprise enough information in order to reconstruct the original sample from them [35]. However, recent studies have arisen several concerns regarding the soundness of this widely spread belief for traits such as the fingerprint [12], the iris [67] or the face [26].

In this work, we address for the first time these questions and concerns for the hand trait. For this purpose, we present a novel probabilistic approach based on the Uphill Simplex algorithm and a hand-shape generator for the reconstruction of hand shape images from their templates. Three main objectives are pursued in the present work:

- Analyse the feasibility of such a reverse engineering process for the hand geometry trait.
- Study whether the reconstructed images obtained with the proposed method are able to deceive state-of-the-art hand recognition systems. This will also serve as validation for the new reconstruction technique.
- Determine if it is possible to generate not just one, but several different synthetic images which yield templates very similar to the genuine one.

In this new scenario, the results presented in this contribution show the necessity to include in hand-shape applications efficient countermeasures to repel the studied attacks [19,21].

In order to follow a fully reproducible experimental protocol which permits the comparison of the results with future studies, experiments are carried out on three publicly available databases. Furthermore, the hand recognition systems used for development and testing are well known and state-of-the-art systems which may be easily obtained by any interested party.

The article is structured as follows. After the introduction, a selection of the most important related works may be found in Section 2. Hand recognition is briefly summarized in Section 3. The novel probabilistic hand reconstruction algorithm is presented in Section 4. Then, the experimental protocol together with the databases and hand recognition systems used are described in Section 5. In Section 6 the development and validation results, as well as a quality assessment of the real and the synthetic samples, are presented. Conclusions are finally drawn in Section 7.

2. Related works

A growing interest has arisen in the biometric community over the last decade for the generation of synthetic biometric traits such as voice [18], fingerprints [11], iris [80], handwriting [47], face [57] or signature [58].

One of the first research lines in this field was the generation of the so-called *duplicated samples*. In these methods the generation algorithm starts from one or more real samples of a given person and, through different transformations, produces different synthetic (or duplicated) samples corresponding to the same subject. This type of algorithms is useful to increase the amount of already acquired biometric data which can be helpful, for instance, to synthetically augment the size of the enrolment set of data in identification and verification systems, a critical parameter for instance in signature biometrics [22]. This approach has been applied to signature [52,55], handwriting [51,69] or face synthesis [57,68,70].

Based on those initial works, researchers have also focused their efforts on a second and more complex problem: the generation of *fully synthetic biometric individuals*. In this case, some kind of a priori knowledge about a certain biometric trait (e.g., minutiae distribution, iris structure, signature length, etc.) is used to create a model that characterizes that biometric trait for a population of subjects. New synthetic individuals can then be generated sampling the constructed model. In a subsequent stage of the algorithm, multiple samples of the synthetic users can be generated by any of the procedures for creating duplicated samples. Different model-based algorithms have been presented in the literature to generate synthetic individuals for biometric traits such as iris [15,64,80], fingerprint [11], or speech [40,56].

All the previous works have been mainly focused on the generation of new synthetic data, intended in general to overcome the limitation of assembling large biometric databases for performance assessment purposes. However, none of these very valuable efforts addresses directly the main objective raised in the present work referred to as *inverse biometrics*, that is, the reconstruction of a synthetic biometric sample from a genuine template and the evaluation of the ensuing security implications.

One of the first works that addressed the problem posed by inverse biometrics was carried out by Hill [31]. This work, focused on fingerprint recognition, proves that the information stored in the minutiae template allows the reconstruction of images similar to the original fingerprint. After him, other researches have generated fingerprint images [12,59] or gummy fingers [25] given only the minutiae template. However, not only fingerprints have been successfully reconstructed: in [1,2,26] face images are recovered from their templates, and in [67] iris images are generated starting from the iriscodes.

In our particular case study, hand shape recognition, to our knowledge, only our previous work [28] addresses the inverse biometrics problem, proposing the first reconstruction approach to recover hand geometry samples from their templates. In that work, only the theoretical framework was proposed and some preliminary experiments were carried out. In the present contribution we significantly extend that initial work with: (i) a more thorough and comprehensive description of the