Pattern Recognition Letters 36 (2014) 243–253

Contents lists available at SciVerse ScienceDirect

Pattern Recognition Letters

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

Efficient software attack to multimodal biometric systems and its application to face and iris fusion

Marta Gomez-Barrero *,[1], Javier Galbally [1], Julian Fierrez [1]

Biometric Recognition Group – ATVS, EPS, Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente 11, 28049 Madrid, Spain

ARTICLE INFO

Article history:
Available online 10 May 2013

Communicated by Luis Gomez Deniz

Keywords:
Multimodal system
Security
Vulnerabilities
Hill-climbing
Countermeasures

ABSTRACT

In certain applications based on multimodal interaction it may be crucial to determine not only *what* the user is doing (commands), but *who* is doing it, in order to prevent fraudulent use of the system. The biometric technology, and particularly the multimodal biometric systems, represent a highly efficient automatic recognition solution for this type of applications.

Although multimodal biometric systems have been traditionally regarded as more secure than unimodal systems, their vulnerabilities to spoofing attacks have been recently shown. New fusion techniques have been proposed and their performance thoroughly analysed in an attempt to increase the robustness of multimodal systems to these spoofing attacks. However, the vulnerabilities of multimodal approaches to software-based attacks still remain unexplored. In this work we present the first software attack against multimodal biometric systems. Its performance is tested against a multimodal system based on face and iris, showing the vulnerabilities of the system to this new type of threat. Score quantization is afterwards studied as a possible countermeasure, managing to cancel the effects of the proposed attacking methodology under certain scenarios.

1. Introduction

Multimodal systems represent a new direction for computing that embraces users' natural behaviour as the center of human–computer interaction (Oviatt and Cohen, 2000). As with any other novel discipline, the research community is just beginning to understand how to design robust and well integrated multimodal systems. But only trough multidisciplinary cooperation among those with expertise in individual component technologies can multimodal systems reach its final aim: building more general and robust systems that will reshape daily computing tasks and have significant commercial impact (Oviatt, 1999).

One of the main areas of research in multimodal interaction, where specific expertise is needed, is *recognition*, generally regarded as a form of processing users' commands. However, for certain applications based on multimodal interaction, a second form of recognition is crucial: it is not only necessary to distinguish *what* the user is doing, but *who* is doing it, so that non-authorized individuals cannot use the system. For these cases, a robust personal automatic recognition solution such as the one provided by *biometrics* is required. Although being relatively young compared to other mature and long-used security technologies, biometrics have emerged in the last decade as a pushing alternative for applications where automatic recognition of people is needed. Certainly, biometrics are very attractive and useful for the final user: forget about PINs and passwords, you are your own key (Jain et al., 2006; Wayman et al., 2005). However, we cannot forget that as any technology aimed to provide a security service, biometric systems are exposed to external attacks which could compromise their integrity (Schneier, 1999). Thus, it is of special relevance to understand the threats to which they are subjected and to analyse their vulnerabilities in order to prevent possible attacks and increase their benefits for the users.

External attacks to biometric systems are commonly divided into: *direct attacks* (also known as *spoofing attacks*), carried out against the sensor, and *indirect attacks*, directed to some of the inner modules of the system. In the last recent years important research efforts have been conducted to study the vulnerabilities of biometric systems to both direct and indirect attacks (Galbally et al., 2010, 2011; Matsumoto, 2004; Uludag and Jain, 2004).

This new concern which has arisen in the biometric community regarding the security of biometric systems has led to the appearance of several international projects, like the European Tabula Rasa (2010), which base their research on the security through transparency principle (Schneier, 2000; Kerckhoffs, 1883): in order to make biometric systems more secure and reliable, their vulnerabilities need to be analysed and useful countermeasures need to be developed.

* Corresponding author. Tel.: +34 91 497 33 63.
E-mail addresses: marta.barrero@uam.es (M. Gomez-Barrero), javier.galbally@uam.es (J. Galbally), julian.fierrez@uam.es (J. Fierrez).

[1] This work has been partially supported by projects Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) and Bio-Shield (TEC2012-34881) from Spanish MINECO, TABULA RASA (FP7-ICT-257289) and BEAT (FP7-SEC-284989) from EU, and *Cátedra UAM-Telefónica*.

0167-8655/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.patrec.2013.04.029

In this scenario, biometric multimodality has been regarded as an effective way of increasing the robustness of biometric-based security systems to external attacks. Combining the information offered by several traits would force an eventual intruder to successfully break several unimodal modules instead of just one. However, it has already been proven that this is not necessary in spoofing attacks: breaking into the module based on the most accurate biometric trait grants access to the multimodal system in many occasions (Akhtar et al., 2011; Chetty and Wagner, 2005; Rodrigues et al., 2009).

In addition to research works which address the vulnerabilities of multimodal systems to spoofing attacks (Akhtar et al., 2011; Chetty and Wagner, 2005; Rodrigues et al., 2009, 2010; Akhtar and Alfarid, 2011; Hämmerle-Uhl et al., 2011; Johnson et al., 2010; Marasco, 2010), different studies may be found in the literature regarding the analysis of indirect attacks against unimodal systems (Galbally et al., 2010; Uludag and Jain, 2004; Martinez-Diaz et al., 2011). However, the problem of whether multimodal approaches are vulnerable or not to software-based attacking methodologies still remains unexplored.

In the present work we propose and analyse a general multimodal indirect attack, which can be used to study the vulnerabilities of biometric systems based on different number of traits, different fusion strategies and different types of templates (e.g., real valued, binary). Without loss of generality, the attack is applied to the particular case of a face- and iris-based recognition system. This trait combination is regarded as one of the most popular and user-friendly, since the acquisition of both traits can be transparent to the user (Wang et al., 2003; Zhang et al., 2010; Gan and Liu, 2009; Gan and Liang, 2006). This provides a straight-forward integration of both modalities, a complex topic on multimodal computation (Oviatt et al., 2003). Furthermore, the experimental protocol used is fully replicable, so that the results obtained can be fairly compared.

Score quantization is studied afterwards as a possible countermeasure against the proposed attack. Two different approaches are analysed: quantizing the score before and after the fusion of the partial face and iris scores. While the second scheme barely reduces the success rate and efficiency of the attack, the first one succeeds in preventing an intruder from breaking into the system.

Thus, following the same transparency principle which is starting to prevail in the biometric community through European Projects such as Tabula Rasa (Schneier, 2000; Kerckhoffs, 1883), the main objectives and contributions of the present work are: (*i*) proposal of a fully novel software-based attacking methodology against multimodal systems, (*ii*) study of the vulnerabilities of a realistic multimodal system to the previous attack under a replicable scenario, (*iii*) comparison of the performance of the attack to that obtained against the unimodal modules in order to determine if the multimodal approach increases the security of the system against this type of threat, and (*iv*) study of some biometric-based countermeasures which may prevent such an attack.

The paper is structured as follows. Related works are summarised in Section 2. The novel multimodal attacking algorithm used to evaluate the system is presented in Section 3. Then the multimodal verification system evaluated is described in Section 4. The database and experimental protocol followed are presented in Section 5. In Section 6 we describe and analyse the results obtained. Score quantization is studied as a possible countermeasure in Section 7. Conclusions are finally drawn in Section 8.

2. Related works

In 2001, Ratha et al. identified and classified in a biometric recognition system eight possible points of attack (Ratha et al., 2001). These vulnerable points can be broadly divided into direct and indirect attacks.

2.1. Direct attacks

Also known as spoofing-attacks, these are attacks at the sensor level, carried out with synthetic biometric traits, such as gummy fingers or high quality printed iris images, and thus requiring no knowledge for the attacker of the inner parts of the system (matching algorithm used, feature extraction method, template format, etc.) Some research regarding the vulnerabilities of multimodal systems to these attacks has been carried out over the last recent years: in 2005, Chetty and Wagner (2005) tested the performance of spoofing attacks against a novel multimodal system based on face and voice; in 2009, Tan (2009) investigated methods for increasing the security of multimodal systems based on face and voice against spoofing attacks; in 2010, Rodrigues et al. (2010) and 2011, Rodrigues et al. (2009), evaluated the vulnerabilities of a multimodal system based on face and fingerprint, using different fusion techniques and proposing new ones; in Johnson et al. (2010) analysed the effect of spoofing attacks against a multimodal system based on face and iris, proposing a method for the vulnerabilities assessment of these systems; later in 2010, Marasco (2010) analysed the security risks in multimodal biometric systems based on face and fingerprint coming from spoofing attacks; in 2011, Akhtar et al. (2011) and Akhtar and Alfarid (2011) used real rather than simulated spoof samples for the evaluation of the vulnerabilities of a multimodal system based on fingerprint, face and iris, proposing a new learning algorithm able to improve the security offered by the system against spoofing attacks. All these works have proven that combining several traits in one system for person authentication does not necessarily increment the security offered against spoofing attacks, since the system can be bypassed by breaking only one of the unimodal traits.

2.2. Indirect attacks

These attacks are directed to the inner modules of the system and can be further divided into three groups, namely: (*i*) attacks to the communication channels between modules of the system, extracting, adding or changing information; (*ii*) attacks to the feature extractor and the matcher may be carried out using a Trojan Horse that bypasses the corresponding module; and (*iii*) attacks to the system database which manipulate it in order to gain access to the application, by changing, adding or deleting a template. While for direct attacks the intruder needed no knowledge about the inner modules of the system, this knowledge is a main requisite here, together with access to some of the system components (database, feature extractor, matcher, etc.). Most of these indirect attacks are based on some variation of a hill-climbing algorithm, consisting on iteratively changing some synthetically generated templates until access to the system is granted. Even though some research has been done in this area using unimodal systems (Galbally et al., 2010; Uludag and Jain, 2004; Martinez-Diaz et al., 2011; Adler, 2004), to the best of our knowledge there is no previous analysis of the vulnerabilities of multimodal biometric systems to this kind of attacks.

3. Proposed attack

Until now, only the vulnerabilities of unimodal systems to indirect attacks have been analysed. In this section we present the first algorithm for the evaluation of the vulnerabilities of multimodal systems to this type of threat. As can be observed in Fig. 1 (top),