Tiago de Freitas Pereira

X A Comparative Study of Countermeasures to Detect Spoofing Attacks in Face Authentication Systems

Campinas
2013

Universidade Estadual de Campinas
Faculdade de Engenharia Elétrica e de Computação

Tiago de Freitas Pereira

A Comparative Study of Countermeasures to Detect Spoofing Attacks in Face Authentication Systems

Qualificação de Mestrado apresentada na Faculdade de Engenharia Elétrica e de Computação como parte dos requisitos exigidos para a obtenção do título de Mestre em Engenharia Elétrica. Área de concentração: Computação

Orientador: Professor Doutor José Mario De Martino

Este exemplar corresponde a versão final do exame de qualificação apresentado pelo aluno, e orientado pelo Prof. Dr. José Mario De Martino

Campinas
2013

Faça aqui sua dedicatória.

Acknowledgment

Text

A maravilhosa disposição e harmonia do universo só pode ter tido origem segundo o plano de um Ser que tudo sabe e tudo pode. Isto fica sendo a minha última e mais elevada descoberta.

Isaac Newton

Abstract

User authentication is an important step to protect information and in this field face biometrics is advantageous. Face biometrics is natural, easy to use and less human-invasive. Unfortunately, recent work has revealed that face biometrics is vulnerable to spoofing attacks using low-tech equipments. Countermeasures have been proposed in order to mitigate this vulnerabilities. However several works in the literature present evaluations using different metrics and in private database making the comparison of countermeasures a difficult task. The main goal of this masters project is to provide a comparative study of countermeasures against face *spoofing* attacks.

Key-words: Antispoofing, Liveness detection, Countermeasure, Face Recognition, Biometrics

List of Figures

List of Tables

Acronyms

Contents

Chapter 1

Introduction

1.1 Scope and Contributions

1.2 Organization of the Thesis

Chapter 2

Biometrics

Some text.

2.1 Introduction to Biometric Systems

Biometrics is the science of recognizing the identity of a person based on their physical attributes and / or behavior, such as face, fingerprints, hand veins, voice or iris (**?**). The use of biometrics as authentication factor has some advantages. Naturally, is not possible to forget or transfer a biometric trait and it hardly disappears (perhaps in case of a seriously accidents). Biometrics has some disadvantages. As an example, our voice vary drastically when we get sick or when we are under stress. Unfortunately our facial trait change when we get old. It is important to remark that authentication based on biometrics is probabilistic, which means that errors can happen (????).

To use a biometric trait in a biometric system, the candidate must satisfy the following requirements.

- Universality (every person must have it);
- Uniqueness (must distinguish people);
- Stability (must be stable along the time);
- Coletability (must be measure);
- Performance;
- Acceptance;
- Circunvention (low risk of frauds).

Table 2.1 shows a comparative between the most used biometric traits (**?**). It can be observed that none of the presented biometric traits fulfil all the listed requirements and the selection of a trait depends on the application (??????) (**?**).

Table 2.1: Comparison of the most used biometric traits (**?**)

Biometric trait	**Universality**	**Uniqueness**	**Stability**	**Coletability**	**Performance**	**Acceptance**	**Circunvention**
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	Medium
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Palm vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice	Medium	Low	Low	Medium	Low	High	Low

A regular biometric authentication system can be represented with the simple flow chart in Figure X.

FIGURE X

Firstly the biometric trait is captured using some sensor. Secondly the captured biometric trait is processed in order to extract the biometric features. When it is in an enrolment procedure, these features will generate a biometric reference, and it will be stored in a database. In an authentication procedure, these features will be used in a comparison with the stored biometric reference. It is possible to observe in the Figure Y, attacks can be done in any point of the architecture (**?**). The next subsections will be discussed about each one of the possible point of attacks and how to mitigate it.

FIGURE Y

2.2 Attacks in Biometric Systems

2.2.1 Replay attack

The replay attack is performed by injecting a biometric data previously sent, of the target identity, in order to have a non authorised access. This data can be obtained sniffing the biometric software in one of the points of the Figure X. To mitigate these kind of attacks, the biometric system should ensure that the provided data was not injected artificially (**?**). The most popular way of protect this kind of attack is to associate a timestamp to the data. As it is improbable to have the exactly the same biometric data in different times, this method is effective.

2.2.2 Biometric reference attack

The attack in the biometric reference is performed where the biometrics are stored. This kind of attacks include actions such as the inclusion, removing, modifying and steal a biometric template. Among this actions, the possibility to steal a biometric reference is the most dangerous treat, since it is possible to work in a reverse engineering processes to regenerate the biometric trait. (**?**) shown that is possible to generate synthetic fingerprints applying reverse engineering in a biometric references based on minutia. With this fake fingers was possible to deceive a fingerprint authentication system. To mitigate the risk of this kind of attack is recommended to encrypt the biometric reference and increase the policy to access the biometric references.

2.2.3 Man-in-the-midle attack

The man i

2.2.4 Ataque de Spoofing

The spoofing attack in biometric system is a direct attack to the biometric sensor; a forged biometric is presented to the biometric sensor. The goal is to pretend to be someone else in order to get some forbidden privileges.

Best practices in security recommends to use cryptography or the creation of security channels in order to mitigate most of the problems aforementioned. But in case of a spoofing attack, the target is the biometric sensor, and in the chart presented in Figure X, is not possible to apply any of the security tools to prevent attacks, becoming the most fragile point of attack. This kind of attacks is the main point of this thesis.

Chapter 3

Spoofing Attacks

As aforementioned, spoofing attacks in biometrics are direct attacks to the biometric sensor. Spoofing techniques vary from different biometrics. This chapter discusses the spoofing attacks in different biometric traits focusing in face recognition.

3.1 Spoofing Attacks in Biometrics

It is always possible to create a spoofing attack to a biometric system. This sections discusses the occurrences of spoofing attacks in different biometric systems.

3.1.1 Fingerprint

In fingerprints based systems the attacker can forge a fingerprint with different materials (gummy, silicone, etc) in order spoof the system as can be observed. (**?**) and (**?**) discusses how to generate fake fingerprints using materials that is possible easily to find in a supermarket. Figure X shows how easy is to create a mold from a live finger and to reproduce its fingerprint with gummy. This fake fingers can be used to spoof a fingerprint biometric systems.

Figure X.

Recently in Brazil (2013), was reported that doctors in Sao Paulo were arrested after being caught in the act of using fake fingers made of silicone and imprinted with real finger prints to defraud a hospital's biometric punch-in clock[1].

A more sophisticated attack were discussed in (**?**). This paper uses a hill climbing procedure to optimise the position and the orientation of the minutia in a minutia based fingerprint verification system. This optimized minutia can be used to generate a fake finger.

3.1.2 Speaker

Finally (**?**) e (**?**) address speaker based biometric systems.

[1] http://www.foxnews.com/us/2013/03/13/brazilian-doctors-use-fake-silicone-fingers-to-defraud-hospital-punch-in-clock/

3.1.3 Iris

(**?**), (**?**) and (**?**) are works addressing spoofing attacks in iris biometric system.

3.2 Spoofing Attacks in Face Recognition

Because of its natural and non-intrusive interaction, identity verification and recognition using facial information are among the most active and challenging areas in computer vision research. Despite the significant progress of face recognition technology in the recent decades, wide range of viewpoints, ageing of subjects and complex outdoor lighting are still research challenges. Advances in the area were extensively reported in (**?**) and (**?**).

Unfortunately, the issue of verifying if the face presented to a camera is indeed a face from a real person and not an attempt to deceive (spoof) the system has mostly been overlooked. It was not until very recently that the problem of spoofing attacks against face biometric system gained attention of the research community. This can be attested by the gradually increasing number of publicly available databases (**?**, **?**, **?**, **?**) and the recently organized IJCB 2011 competition on counter measures to 2D facial spoofing attacks (**?**) which was the first competition conducted for studying best practices for non-intrusive spoofing detection.

In authentication systems based on face biometrics, spoofing attacks are usually perpetrated using photographs, videos or forged masks. While one can also use make-up or plastic surgery as mean of spoofing, photographs and videos are probably the most common sources of spoofing attacks. Moreover, due to the increasing popularity of social network websites (facebook, flickr, youtube, instagram and others), a great deal of multimedia content - especially videos and photographs - is available on the web that can be used to spoof a face authentication system. In order to mitigate the vulnerability of face authentication systems, effective countermeasures against face spoofing have to be deployed.

DEPENDENTE E INDEPENDENTE DA COLABORACAO.

3.2.1 Presence of vitality (liveness)

Presence of vitality or liveness detection consists of search for features that only live faces can possess. The eye blinking is an activity that humans do constantly. A regular human blinks once every 2 or 4 seconds in order to maintain the eyes clean and wet. This frequency can vary in stress conditions and/or in a high concentration task. In that situations the interval can extend to $\sim$ 20 seconds. However, does not matter in what condition, in some point the eye blink will occur. Following that fact, (**?**) propose a countermeasure measuring the eye blinking using hidden markov (HMM ???) mapping the state of eyes open and closed. Experiments carried out using a database created by the authors and freely available for download[2], shown an accuracy of 95.7% .

EULERIAN.

[2]http://www.cs.zju.edu.cn/ gpan/database/db_blink.html

3.2.2 Scene

3.2.3 Differences in image quality assessment

3.3 Face Spoofing Databases

Discuss permeability of the databases.

Chapter 4

Developed Countermeasures

Chapter 5

The Comparative Study

5.1 Databases Permeability

5.2 Evaluation Protocol

5.2.1 Intra Database Test Protocol

5.2.2 Inter Database Test Protocol

5.2.3 Evaluation Metrics

Chapter 6

Experiments and Results

Chapter 7

Conclusion

Chapter 8

Future Work

Appendix A

Related Publications

Bibliografia