Iris Recognition: Threat Analysis at the User Interface Level

Inmaculada Tomeo-Reyes, Judith Liu-Jimenez,
Belen Fernandez-Saavedra, Raul Sanchez-Reillo

University Group for Identification Technologies (GUTI)
Carlos III University of Madrid
Tlf.: +34 91 624 40 35   Fax: +34 91 624 94 30
{itomeo,jliu,mbfernan,rsreillo}@ing.uc3m.es

Outline

Introduction

Main target

Biometric systems threats

Iris database development

Attacks at the user interface level: iris

Countermeasures

Conclusions

Outline

- Introduction
- Main target
- Biometric systems threats
  - Threats according to Common Criteria
  - Attacks at the user interface level
- Iris database development
- Threat analysis at the user interface level in iris recognition systems
  - Impersonation
  - Obfuscation
  - Spoofing
- Countermeasures
- Conclusions

Outline

Introduction

Main target

Biometric systems threats

Iris database development

Attacks at the user interface level: iris

Countermeasures

Conclusions

Introduction

- Security threats ⚠
  - When working with biometric systems, it is very important to keep in mind the potential security threads, as they can lead to security failures. Such failures can occur due to:
    - Intrinsic limitations of the system
    - Explicit attacks
      - Carried out by insiders (e.g. administrators and legitimate users)
      - Carried out by external attackers
- Iris recognition
  - Iris pattern is unique, stable and non-invasive ✓
    - Suitable for individual recognition purposes
    - Low error rates
  - It has inherent weaknesses that can compromise security ✗
    - Susceptibility to certain attacks

Outline

Introduction

Main target

Biometric systems threats

Iris database development

Attacks at the user interface level: iris

Countermeasures

Conclusions

Main target

- Identify potential threats at the user interface level in iris recognition systems
  - Distance analysis of different types of potentially threatening input images
    - Cases under study: impersonation, obfuscation, spoofing
    - Database: specially developed for this purpose
    - Distance calculation: Hamming distance obtained from an iris recognition system inspired by Daugman works
- Apply later the knowledge to the development of robust, threat-resistant algorithms that correctly work in non-collaborative/unsupervised environments

Outline

Introduction

Main target

Biometric systems threats

Iris database development

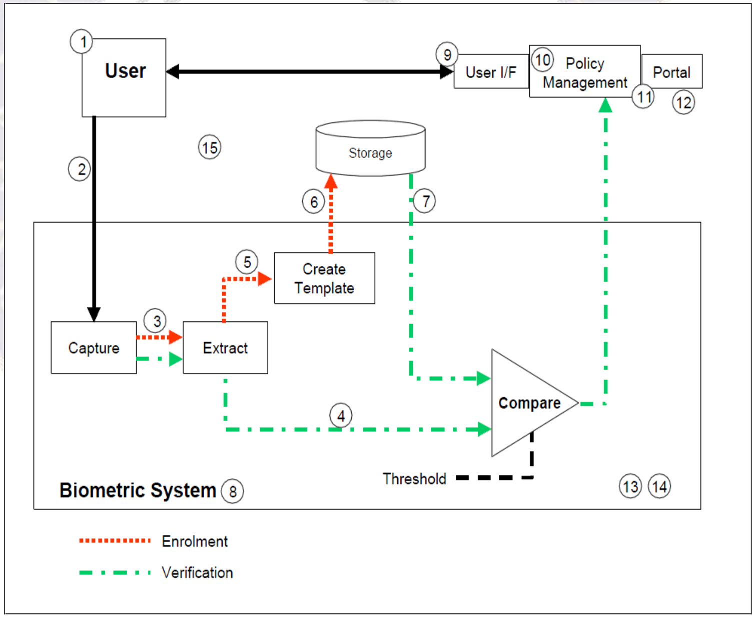
Attacks at the user interface level: iris

Countermeasures

Conclusions

Biometric systems threats

- Any biometric system, regardless of the trait, is basically composed of four different subsystems:
  - Data acquisition, pre-processing, feature extraction and comparison
  - Data storage and administrative subsystems can be added to the general biometric schema
- Each subsystem may have different points of attack, and for each point of attack, there may be one or more potential exploits. According to Common Criteria (Biometric Evaluation Methodology Supplement, BEM):



1	User Threats.
2	User/Capture Threats
3	Capture/Extraction Threats
4	Extraction/Comparison Threats during Verification
5	Extraction/Template Storage Threats during Enrolment
6	Template Storage Threats
7	Template Retrieval Threats
8	Administrator/Resource Manager Threats
9	User/Policy Management Threats
10	Policy Management Threats
11	Threats to Policy Management/Portal
12	Portal Threats
13	Threats to all hardware components
14	Threats to all software/firmware components
15	Threats to all connections (including network threats)

Outline
Introduction
Main target
Biometric systems threats
Iris database development
Attacks at the user interface level: iris
Countermeasures
Conclusions

Biometric systems threats

- We will focus on user/capture threats (type 2), which can be considered, as well, threats at the user interface level
  - Any attempt by an attacker to break into the system by presenting a biometric sample can be considered an attack at the user interface level
- Three main types of attacks are possible at the user interface level:
  - Impersonation
    - Impostor attempts to intrude the system by posing himself as another authorized user.
    - E.g. Modify his/her own behaviour (e.g. voice, signature or gait) or physiology (e.g. face or hand) in an attempt to match the identity under attack.
  - Obfuscation/disguise
    - Attacker deliberately changes his/her biometric characteristic in order to avoid being recognized by the biometric system.
    - E.g. Use of disguises or plastic surgery in the case of face, or applying techniques to obliterate fingerprints (e.g. abrasion, cutting or burning).
  - Spoofing
    - Impostor presents a spoof biometric trait (counterfeit biometric that is not obtained from a live person).
    - E.g. Presentation of fake or artificial traits such as gummy finger, photograph of a face, recorded voice, etc.

Outline

Introduction

Main target

Biometric systems threats

Iris database development

Attacks at the user interface level: iris

Countermeasures

Conclusions

Iris database development

- Difficult to find public databases of noisy, artificial or fake iris images
  - 4000 images
    - Noisy, artificial and fake iris images
  - 60 subjects
    - Ages between 16 and 70 years old
  - Non-collaborative environment
    - Different scenarios, under several different lighting conditions
    - No image has been rejected, except those with an extremely poor quality

Outline

Introduction

Main target

Biometric systems threats

Iris database development

Attacks at the user interface level: iris

Countermeasures

Conclusions

Attacks at the user interface level: iris

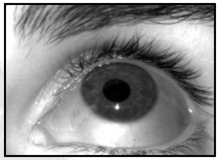
- Impersonation
  - Potential threats
    - Casual impersonation
      - The identity to attack is randomly chosen and the impostor does not modify his/her biometric characteristic
    - Targeted impersonation
      - Impostor attacks a specific identity enrolled in the system, which is known to be easier to impersonate (e.g. weak iris template).
      - Impostor may also target an identity whose biometric characteristics are known to be similar to his/her traits (e.g. twin).
      - Impostor may modify his/her own physiology (iris) in an attempt to match the identity under attack.

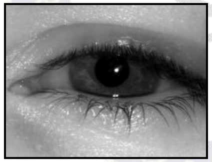
Attacks at the user interface level: iris

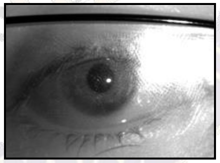
- Impersonation
  - Threat analysis
    - Impersonation attacks in the case of iris can be considered impossible
      - Extremely high unicity of the iris → Some studies state that the probability of finding 2 exact irides is 1 in 10^{78} ✓
      - Irides of twins are different → Although the coloration and structure of the irides is genetically linked, the details of the patterns are not ✓
      - Given the anatomic characteristics of the iris, there is no possible way to modify it in an attempt to match a specific identity ✓

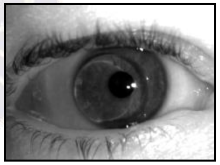
Attacks at the user interface level: iris

- Obfuscation/disguise
  - Potential threats
    - Intentionally presenting a noisy or poor-quality biometric sample
      - Gaze deviation
      - Eyelid obstruction
      - Dirty glasses
      - Hard contact lenses

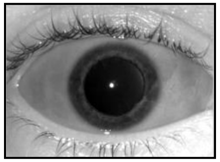

Up gaze deviation

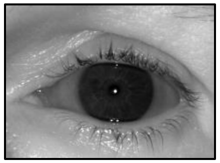

Severe eyelid obstruction


Dirty glasses (poor quality sample)

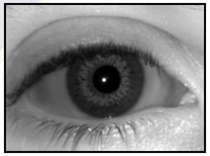

Hard contact lens

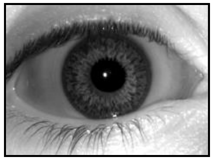
    - Artificially provoking iris alterations
      - Mydriasis (excessive pupil dilation)
      - Miosis (excessive pupil constriction)

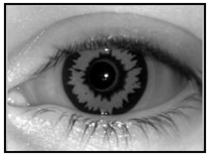

Mydriasis

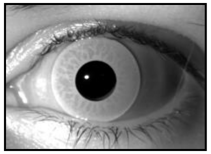

Miosis

    - Occluding the iris by using cosmetic lenses
      - Colour contact lenses
      - Fantasy contact lenses


Green lens


Blue lens


Fantasy lens
Model *Wolf Black*


Fantasy lens
Model *Blood Shot*

Attacks at the user interface level: iris

Outline

Introduction

Main target

Biometric systems threats

Attacks at the user interface level: iris

Countermeasures

Conclusions

- Obfuscation/disguise
  - Threat analysis
    - Noisy/poor-quality biometric sample
      - Severe gaze deviation and severe eyelid obstruction can be dangerous.
        - Distances over the threshold
      - Poor-quality samples can be easily discarded
      - Attacker **may succeed** ⚠
        - It will depend on the system robustness
    - Iris alterations
      - Final stage mydriasis can be dangerous.
        - Distances over the threshold
      - Attacker **may succeed** ⚠
        - It will depend on the system robustness
    - Occlusion by using cosmetic lenses
      - Iris is totally occluded, so no recognition is possible
      - Attacker **will succeed** ✖
        - Unless systems is supervised

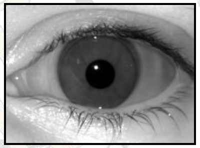
Mean intraclass distance = 0.185
Mean interclass distance = 0.320
} → Threshold = 0.26

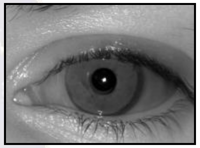
Case	*Scenario*	*Case under analysis*	*Mean Hamming distance*
Noise or Poor Quality	Gaze Deviation	Up	0.320
		Down	0.345
		Left	0.340
		Right	0.315
	Eyelid Obstruction	Slight	0.190
		Medium	0.195
		Severe	0.275
	Glasses	Conventional	0.185
		Dirty	0.255
	Contact Lenses	Soft	0.190
		Hard	0.215
Iris alteration	Mydriasis	Initial Stage	0.220
		Medium Stage	0.245
		Final Stage	0.280
	Miosis	Initial Stage	0.195
		Medium Stage	0.240
		Final Stage	0.255
Occlusion	Colour Lenses	Green	0.330
		Blue	0.315
	Fantasy Lenses	*Wolf Black*	0.410
		Blood Shot	0.350

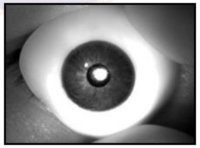
Outline
Introduction
Main target
Biometric systems threats
Iris database development
Attacks at the user interface level: iris
Countermeasures
Conclusions

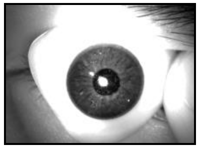
Attacks at the user interface level: iris

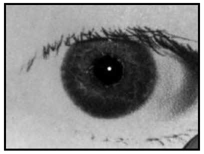
- Spoofing
  - Potential threats
    - Prosthetic lenses
      - Hand-painted. Try to reproduce all details of a healthy eye
      - Prosthetic lenses can be hard or soft
      - Can be made with black or transparent pupil
      - Reproductions from images in visible and IR range considered
    - Prosthetic eyes
      - Hand-painted. Try to reproduce all details of a healthy eye
        - Painted in one layer
        - Painted in three layers (sense of depth)
      - Take the shape of a convex shell
      - Reproductions from images in visible and IR range considered
    - Printed photographs
      - Result of taking a high resolution photograph of a genuine eye and printing it

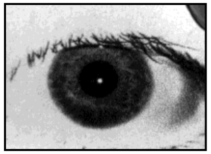

Prosthetic lens with black pupil


Prosthetic lens with transparent pupil


1-layer prosthetic eye


3-layers prosthetic eye


Printed photo with cut-out pupil


Printed photo with non-cut-out pupil

Attacks at the user interface level: iris

- Spoofing
  - Threat analysis
    - Prosthetic lenses
      - Distances far from the threshold
        - Hand-painted reproductions
      - Attacker **will not succeed** ✓
        - What would happen if we print the iris instead of painting it? !
    - Prosthetic eyes
      - Distances far from the threshold
        - Hand-painted reproductions
      - Attacker **will not succeed** ✓
        - What would happen if we print the iris instead of painting it? !
    - Printed photographs
      - Distances near the threshold
      - Attacker **may succeed** !
        - It will depend on the system robustness

Mean intraclass distance = 0.185
Mean interclass distance = 0.320
→ Threshold = 0.26

Scenario	*Case under analysis*	*Mean Hamming distance*
Prosthetic lenses	Black pupil visible	0.375
	Black pupil IR	0.370
	Transparent pupil visible	0.365
	Transparent pupil IR	0.310
Prosthetic eyes	1-layer visible	0.370
	1-layer IR	0.335
	3-layers visible	0.390
	3-layers IR	0.330
Printed photographs	Cut-out pupil	0.285
	Non-cut-out-pupil	0.270

Countermeasures

- According to Common Criteria there are 15 different points of attacks in a biometric system
  - ➢ For each point of attack, there may be one or more potential exploits
- In each case, we need to consider the appropriate defensive measure
  - ➢ One possible high level classification of defensive measures could be:

	Input device protection	Input data Protection	System data protection	Data Storage	System tamper resistance	Secure communications
Challenge/response	✓	✓	✓	✓	✓	✓
Randomising input biometric data		✓	✓		✓	
Liveness detection		✓	✓		✓	
Multiple or multi-modal biometrics		✓	✓		✓	
Multi-factor authentication		✓	✓		✓	
Use of ''soft'' biometrics			✓		✓	
Signal and data integrity and identity		✓	✓	✓	✓	✓
Encryption and digital signatures		✓	✓	✓	✓	✓
Template integrity			✓	✓	✓	
Cancellable biometrics			✓	✓	✓	
Hardware integrity	✓	✓	✓	✓	✓	
Network hygiene	✓	✓	✓	✓	✓	✓
Physical security	✓	✓	✓	✓	✓	✓
Activity logging, policy and compliance checking	✓	✓	✓	✓	✓	✓

Countermeasures

- Multimodal biometrics:
  - Combination of several biometric modalities into one biometric system
    - Multi-modal biometric systems are more difficult to attack
      - Necessary to circumvent all biometric traits involved in the system
    - Computational overhead and more complexity
  - Regarding iris recognition systems
    - Impersonation
      - Not really useful considering impersonation minimum success probability ❌
    - Obfuscation
      - More difficult to circumvent the global system, but iris system threaten level do not decrease ⚠
      - It could motivate obfuscation attacks ❌
        - Attacker may attempt to bypass the main biometric system (iris), and then exploit the loopholes in the fall-back mechanism, which may be easier to circumvent.
    - Spoofing
      - More difficult to circumvent the global system, but iris system threaten level do not decrease ⚠

- Outline
- Introduction
- Main target
- Biometric systems threats
- Attacks at the user interface level: iris
- **Countermeasures**
- Conclusions

Countermeasures

- Liveness detection
  - Aimed at recognizing human physiological signs of life
  - Regarding iris recognition systems
    - Impersonation
      - Not really useful considering impersonation minimum success probability ✗
    - Obfuscation
      - Only prevents certain types of obfuscation attacks
        - Useful when cosmetic lenses are used ✓
          - If lenses are detected the potential attack is detected
        - Potentially useful to detect artificially provoked iris alterations ✓
          - As pupil size variations are more difficult to notice, it would be possible to detect anomalous samples of this type
        - Not useful in the case of noisy or poor-quality images ✗
    - Spoofing
      - Prevents most of the spoofing attacks ✓

Outline
Introduction
Main target
Biometric systems threats
Attacks at the user interface level: iris
Countermeasures
Conclusions

Conclusions

- Security threats are a major issue when working with automatic iris recognition systems
  - They can compromise the system security
- In this presentation, threats at the user interface level have been analyzed in the case of iris recognition systems
  - Impersonation attacks can be considered impossible
  - Obfuscation attacks are easy to perform, so special care must be taken
  - Spoofing attacks are difficult to perform, but given the fast technological development, we cannot forget about them
- In order to prevent such threats...
  - Multimodal systems can be considered
    - More difficult to circumvent the global system, but iris system threaten level do not decrease
  - Liveness detection mechanisms can be considered
    - Liveness detection mechanisms are quite useful to prevent threats at the user interface level, specially in the case of spoofing attacks

Thank you for your attention
Any question?

Inmaculada Tomeo-Reyes, Judith Liu-Jimenez,
Belen Fernandez-Saavedra, Raul Sanchez-Reillo

University Group for Identification Technologies (GUTI)
Carlos III University of Madrid
Tlf.: +34 91 624 40 35 Fax: +34 91 624 94 30
{itomeo,jliu,mbfernan,rsreillo}@ing.uc3m.es