From the Iriscode to the Iris: A New Vulnerability Of Iris Recognition Systems

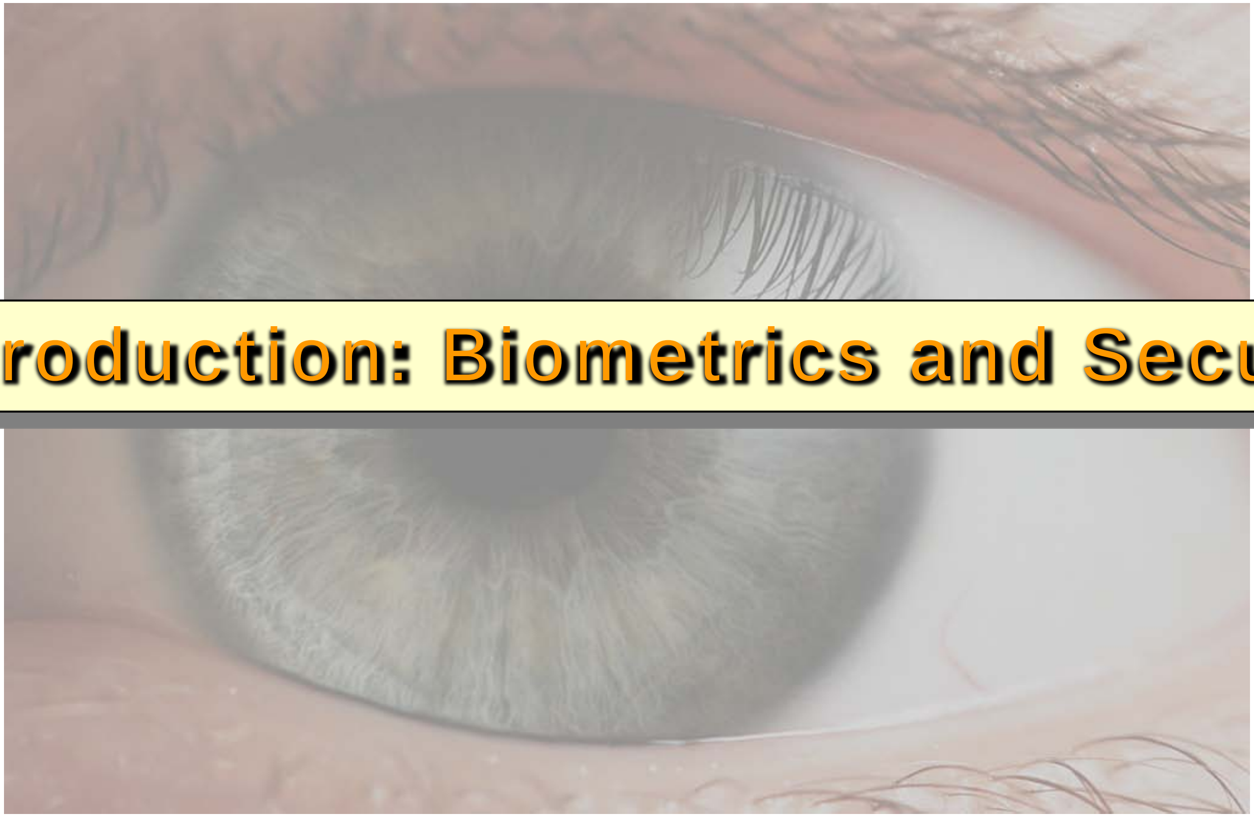
Javier Galbally

Biometrics Recognition Group - ATVS
Escuela Politécnica Superior
Universidad Autónoma de Madrid, SPAIN

http:/ /atvs.ii.uam.es

Outline

1. Introduction: Biometrics and Security
2. Biometrics
3. Iris Recognition
4. The Reconstruction Method
5. Experimental Protocol
6. Results: Performance
7. Results: Appearance
8. Conclusions



1. Introduction: Biometrics and Security

Security Evaluation

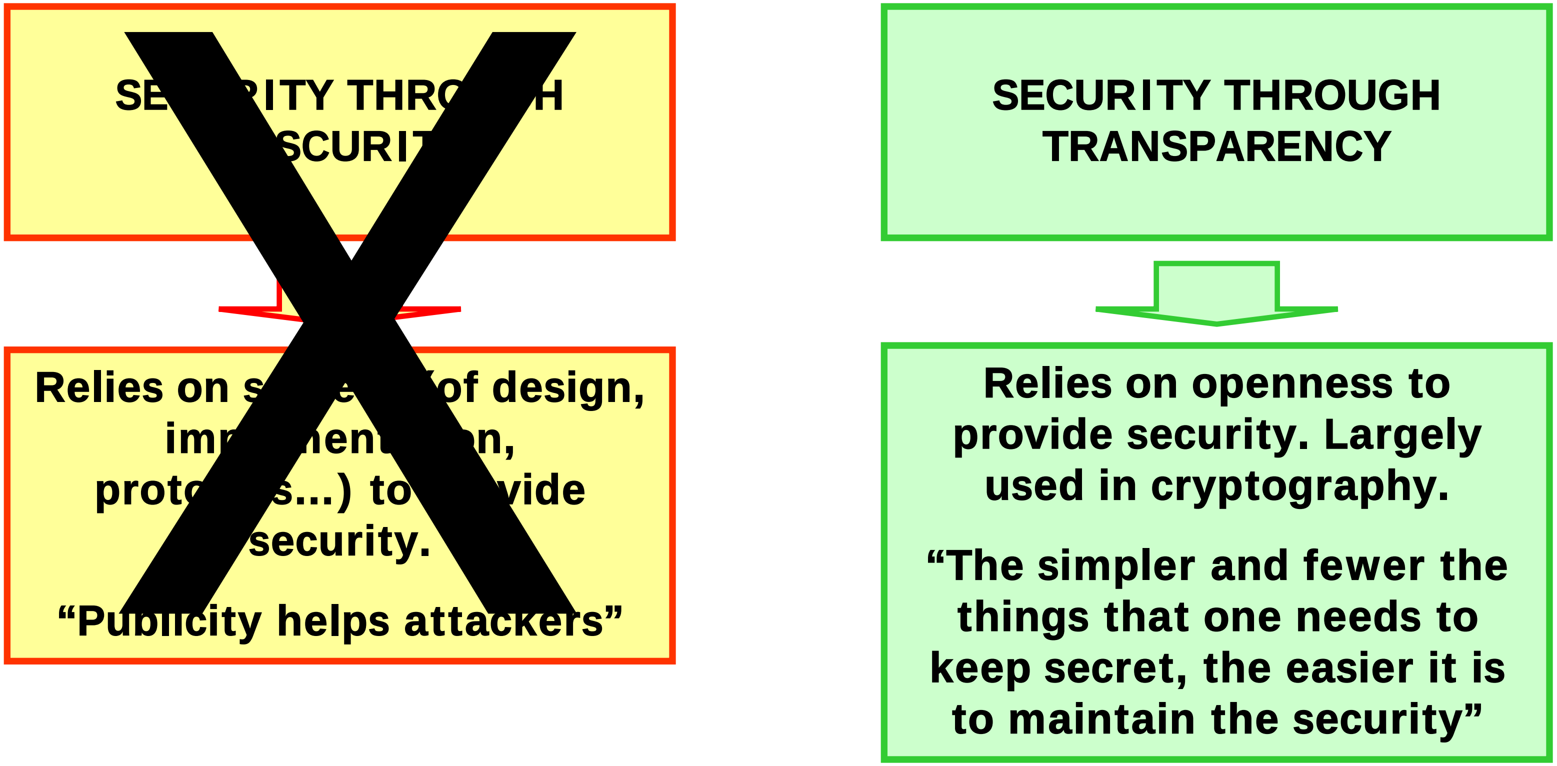
- FAQ when dealing with IT solutions for security applications:
  - How secure is this technology?
  - Why should I trust it?
  - Who assures the level of security offered by this system?
  - …

INDEPENDENT SECURITY EVALUATION

How is this being implemented in BIOMETRICS?

Security Perspective

- There are two ways of addressing the security problem:



~~SECURITY THROUGH OBSCURITY~~

~~Relies on secrecy (of design, implementation, protocols...) to provide security.~~

~~“Publicity helps attackers”~~

SECURITY THROUGH TRANSPARENCY

Relies on openness to provide security. Largely used in cryptography.

“The simpler and fewer the things that one needs to keep secret, the easier it is to maintain the security”

Let’s face the problems and find solutions for them (controlled risk), before somebody else finds the way to take advantage of our secrets (unpredictable consequences)

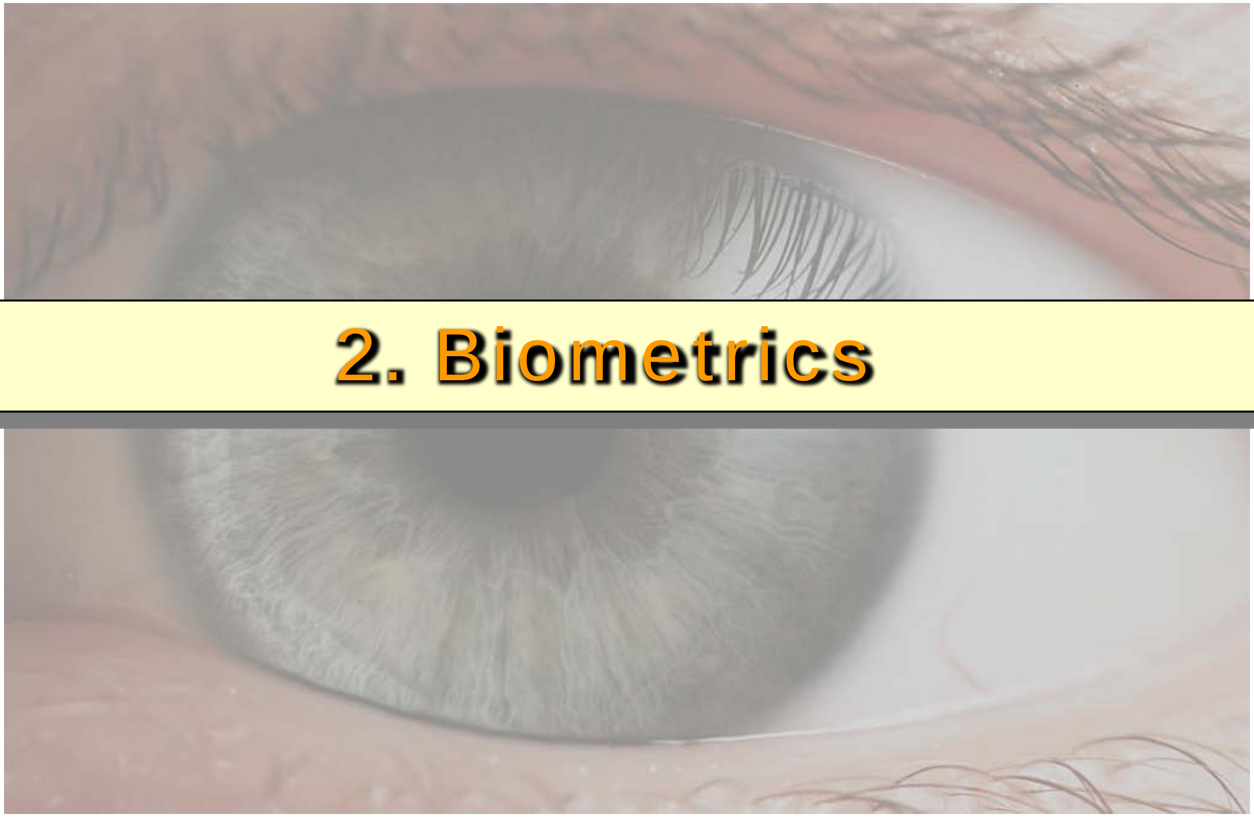
Security Evaluation in Biometrics

- Projects:

- Competitions:

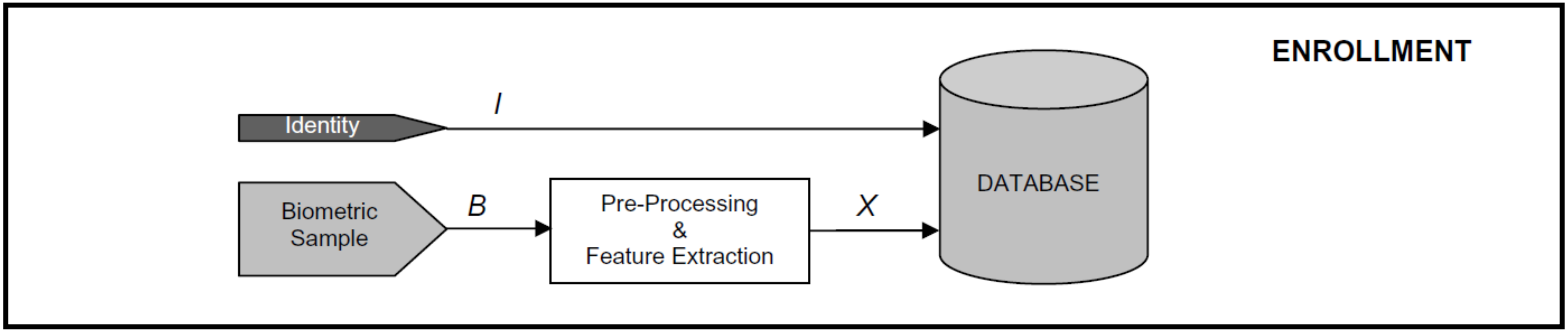
- Standards:

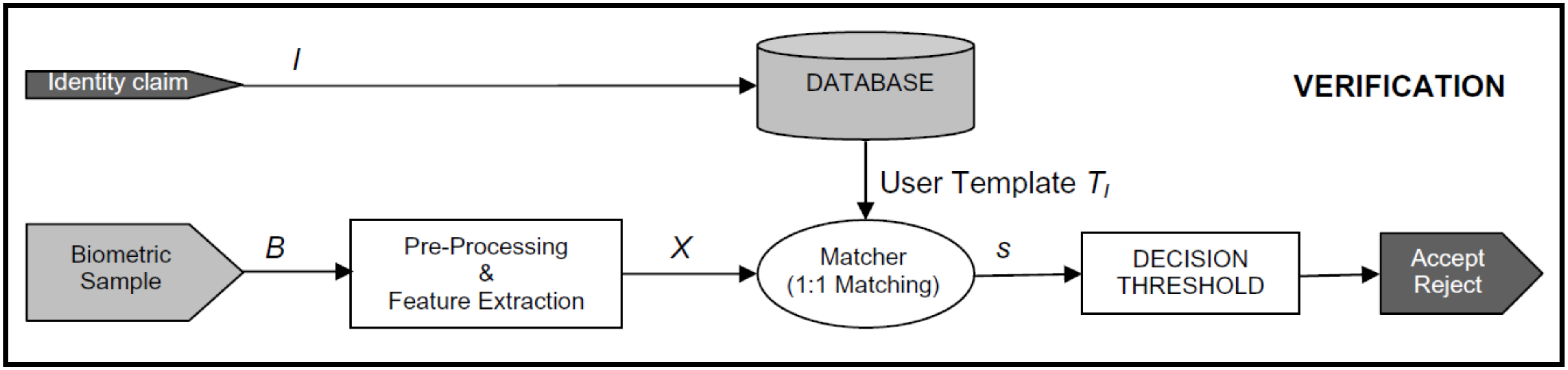
Constant need to search for new vulnerabilities



2. Biometrics

Biometric systems

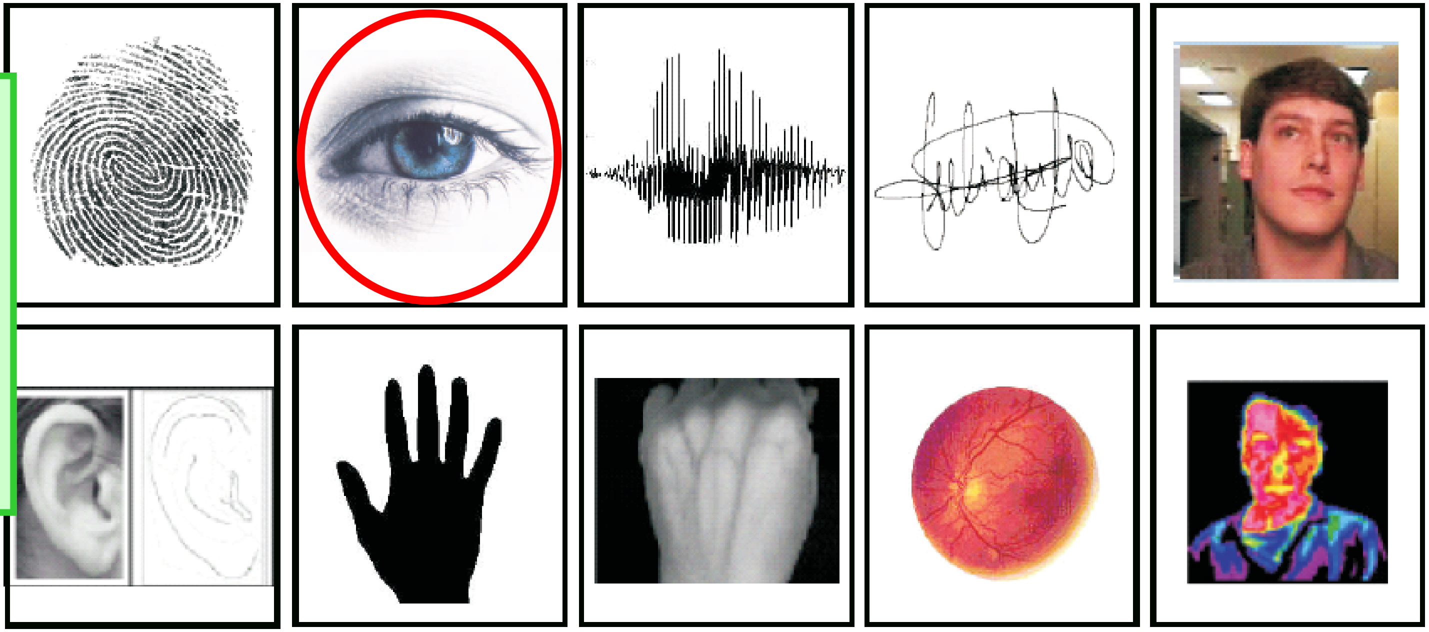




Biometric modalities

BEHAVIOURAL
(signature, voice, gait...)

PHYSIOLOGICAL
(fingerprints, iris, face, hand geometry...)



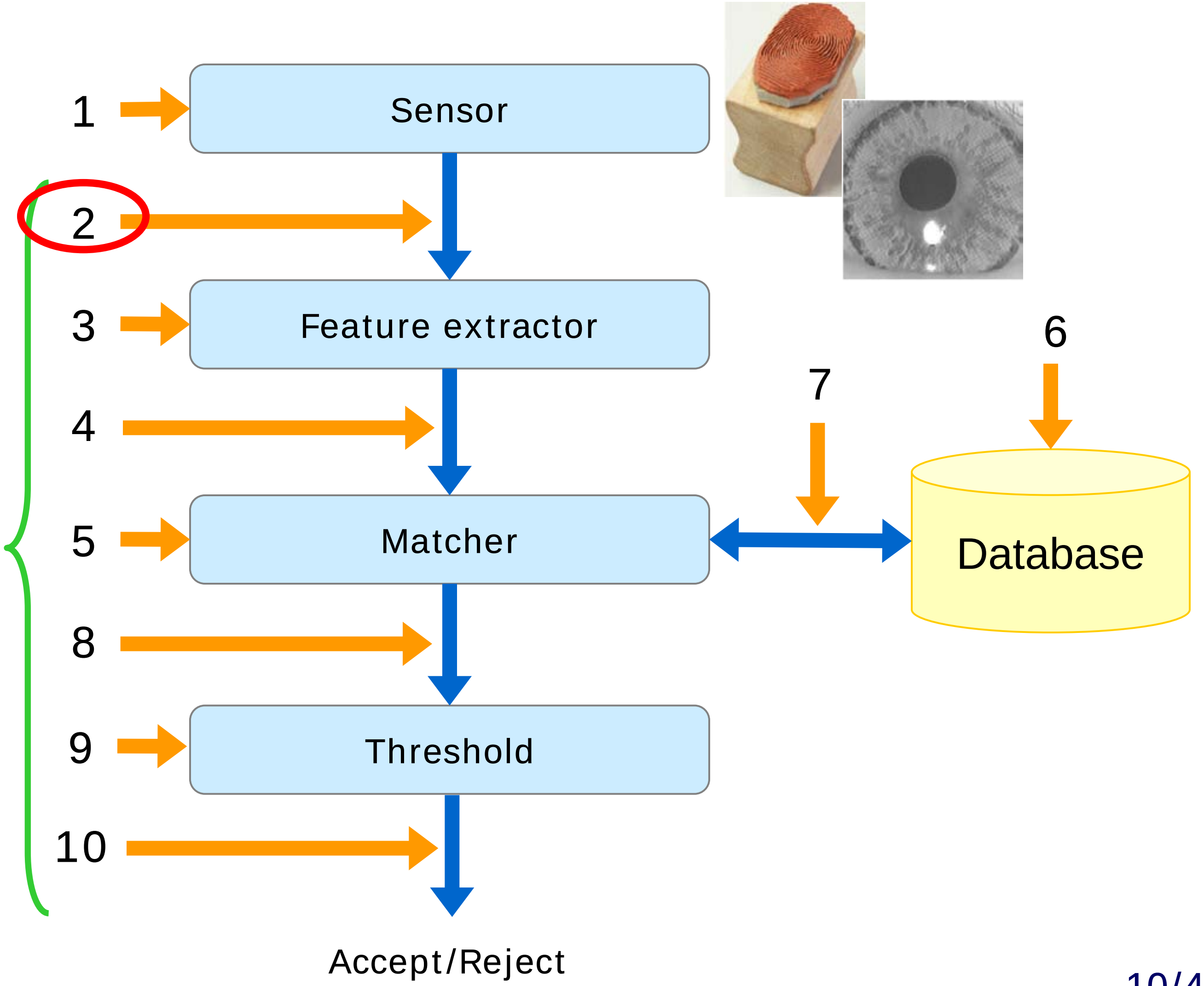
- Characteristics:
  - **Universality**: everybody should possess it
  - **Distinctiveness**: should have enough intervariability
  - **Permanence**: should not vary through time
  - **Collectability**: should be easy to acquire
  - **Performance**: should have good error rates
  - **Acceptability**: user should not be reluctant to use it
  - **Circumvention**: difficult to bypass

Attacks to Biometric Systems

- Possible points of attack to a biometric system.

DIRECT ATTACKS
(Spoofing, mimicry)

INDIRECT ATTACKS
(Trojan Horse, Hill Climbing, Brute Force, channel interception, replay attacks, masquerade attacks...)

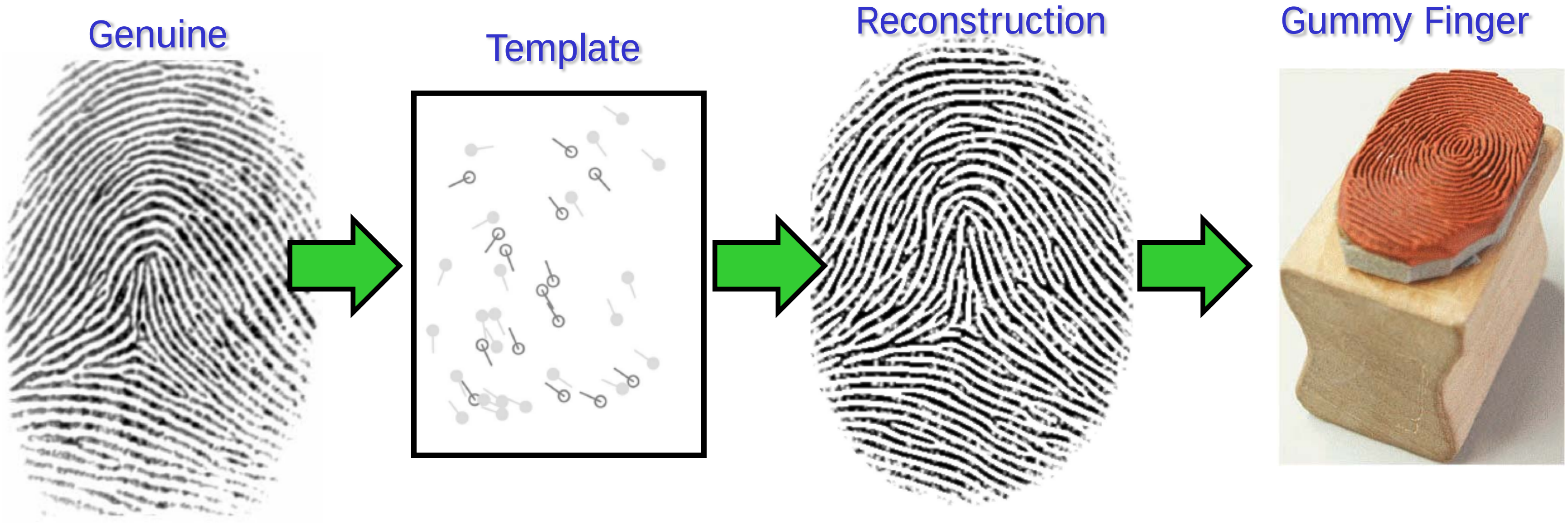


Objective: Inverse Biometrics

- Inverse Biometrics:

Can we reconstruct the sample from the template?

- Traditional answer → NO!
- However...


Genuine

Template

Reconstruction

Gummy Finger

IS THIS POSSIBLE FOR THE IRIS?

3. Iris Recognition

Iris Recognition

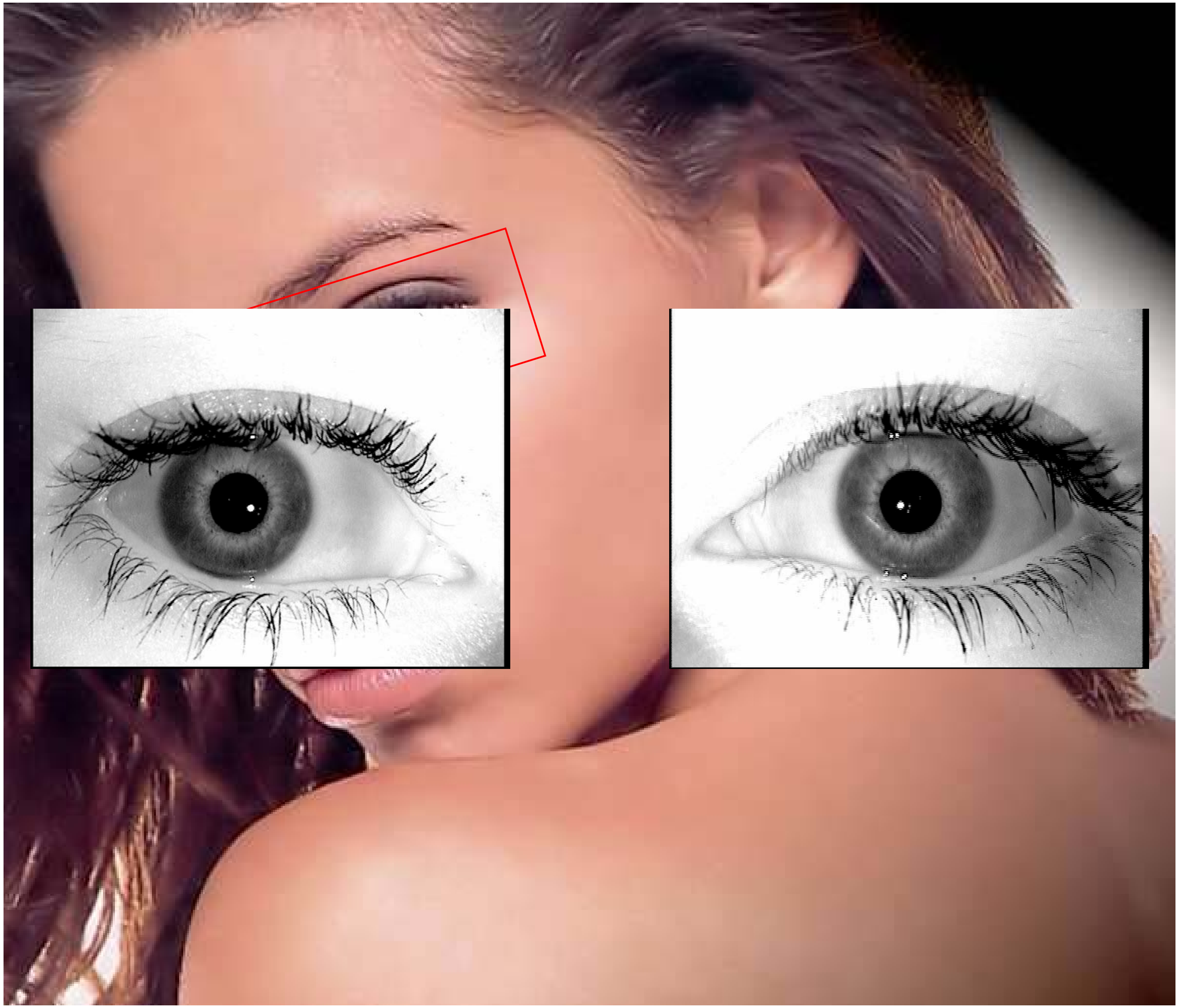
- Very low error rates
- Long-term permanence
- Many commercial solutions
- ...
- Vulnerabilities?

Iris Recognition: How does it work?

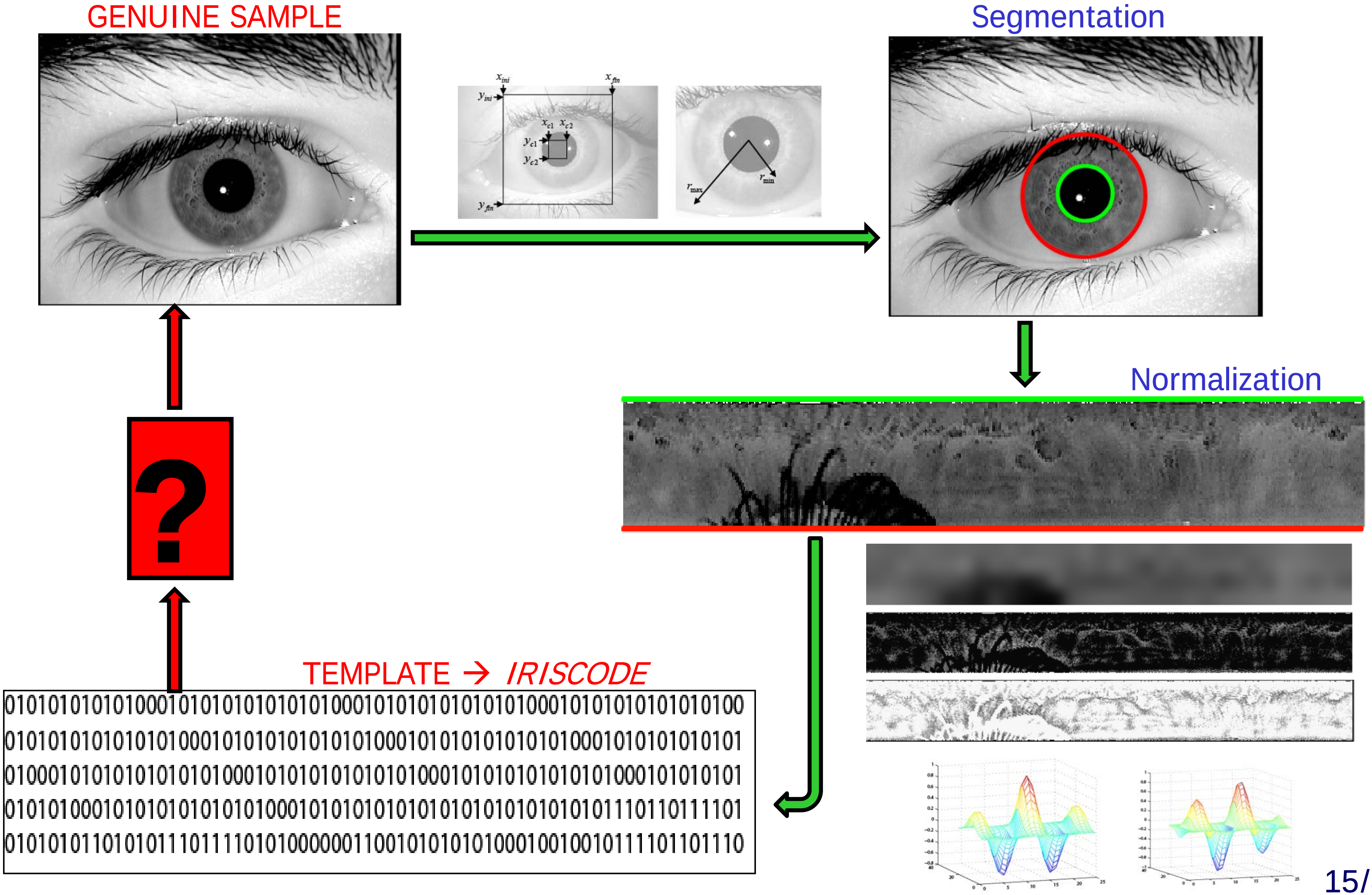
Acquisition

+

Detection



Iris Recognition: How does it work?



GENUINE SAMPLE

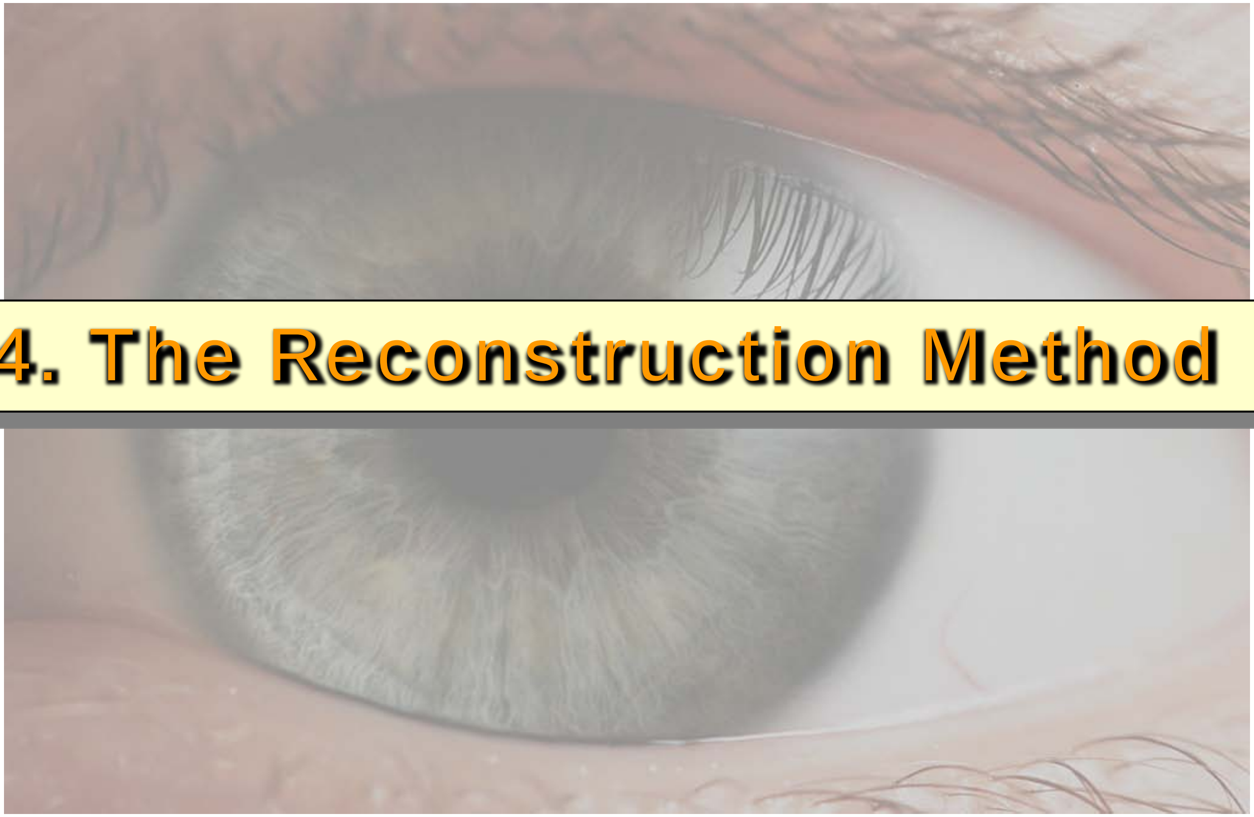
Segmentation

Normalization

?

TEMPLATE → *IRISCODE*

```
01010101010100010101010101010100010101010101010100010101010101010100
01010101010101010001010101010101010001010101010101010001010101010101
01000101010101010101000101010101010101000101010101010101000101010101
01010100010101010101010100010101010101010101010101010101110110111101
01010101101010111011110101000000110010101010100010010010111101101110
```



4. The Reconstruction Method

The Problem (I)

How do we know that an iris image is the reconstruction of a given template?

Because it is positively matched to the genuine template by iris recognition systems

- Find an iris image: *IR*
  - Any iris image? → NO!
- Such that:
  - It´s associated template *BR*
  - When compared to the known template *B* (the one being reconstructed)
  - Using a matching function *J*
  - Gives a score higher than a certain threshold δ

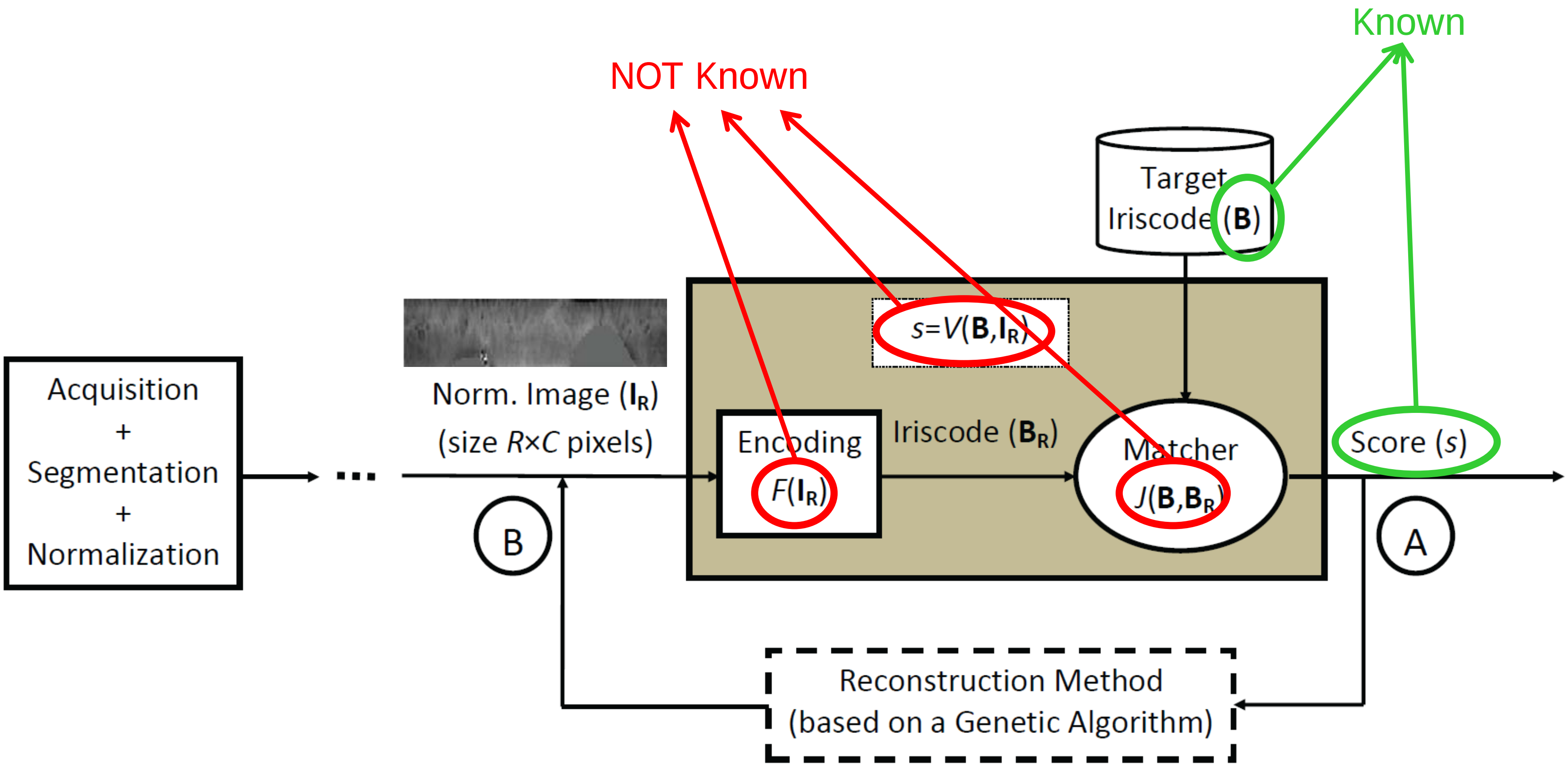
The Problem (II)

How do we find such an iris image?

Use a GENETIC ALGORITHM to look for it
(i.e., optimize the score = optimize the fitness function)

- GENETIC ALGORITHMS:
  - Heuristic search tool
  - ITERATIVELY applies certain rules inspired in natural evolution
  - To a population of individuals (possible solutions)
  - According to a given fitness function which has to be optimized

The Solution: General Architecture


Known
NOT Known
Target Iriscode (B)
$s=V(\mathbf{B},\mathbf{I}_R)$
Acquisition + Segmentation + Normalization
...
Norm. Image ($\mathbf{I}_R$)
(size R×C pixels)
Encoding
$F(\mathbf{I}_R)$
Iriscode ($\mathbf{B}_R$)
Matcher
$J(\mathbf{B},\mathbf{B}_R)$
Score (s)
B
A
Reconstruction Method
(based on a Genetic Algorithm)

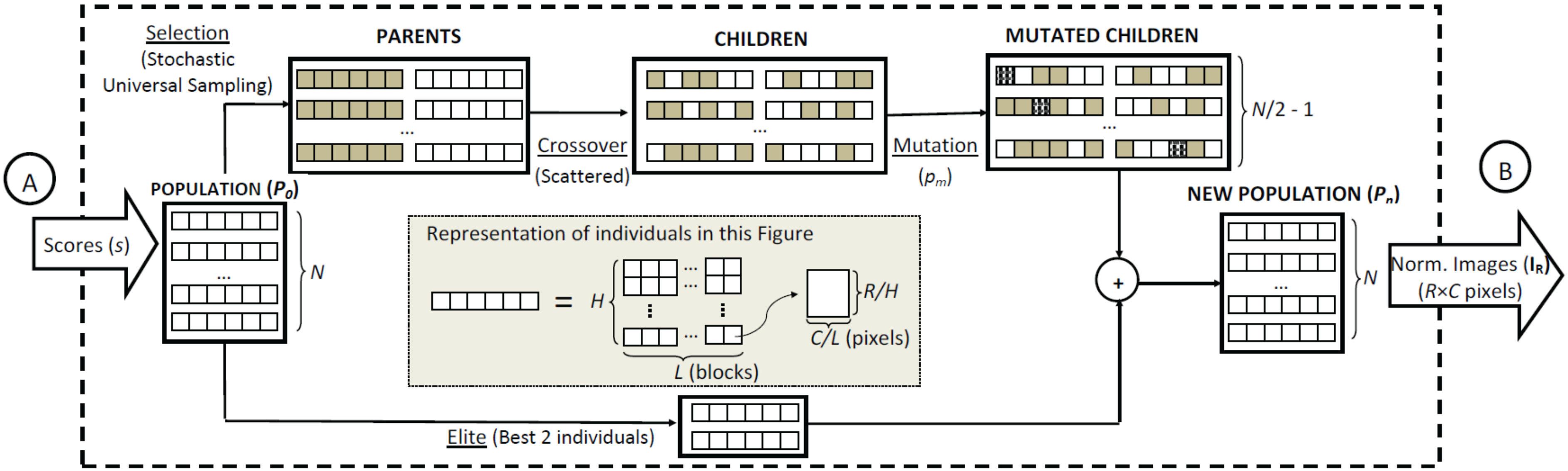
Assumption: we have access to s for several IR

The Solution: The Algorithm (I)

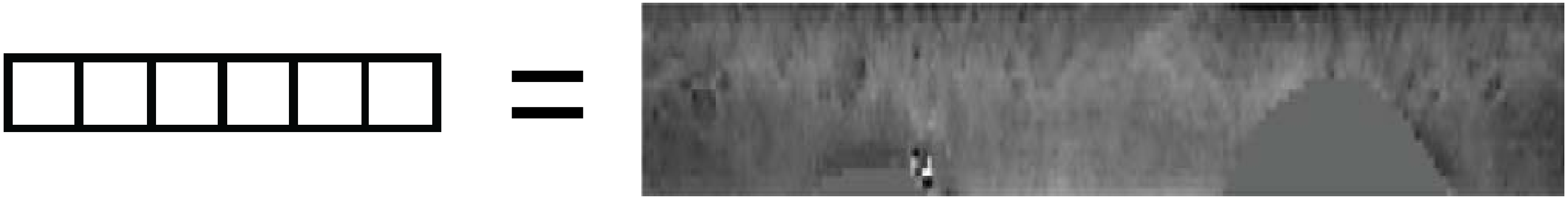
- **STEP 1**: Generate initial population P_0 with N individuals (I_R')
- **STEP 2**: Compute the N scores s_i
- **STEP 3**: Generate the next generation P_n according to four rules:
  - **Elite**: two individuals
  - **Selection**: stochastic universal sampling
  - **Crossover**: scattered crossover
  - **Mutation**: random changes
- **STEP 4**: Redefine $P_0 = P_n$ and go back to step 2.

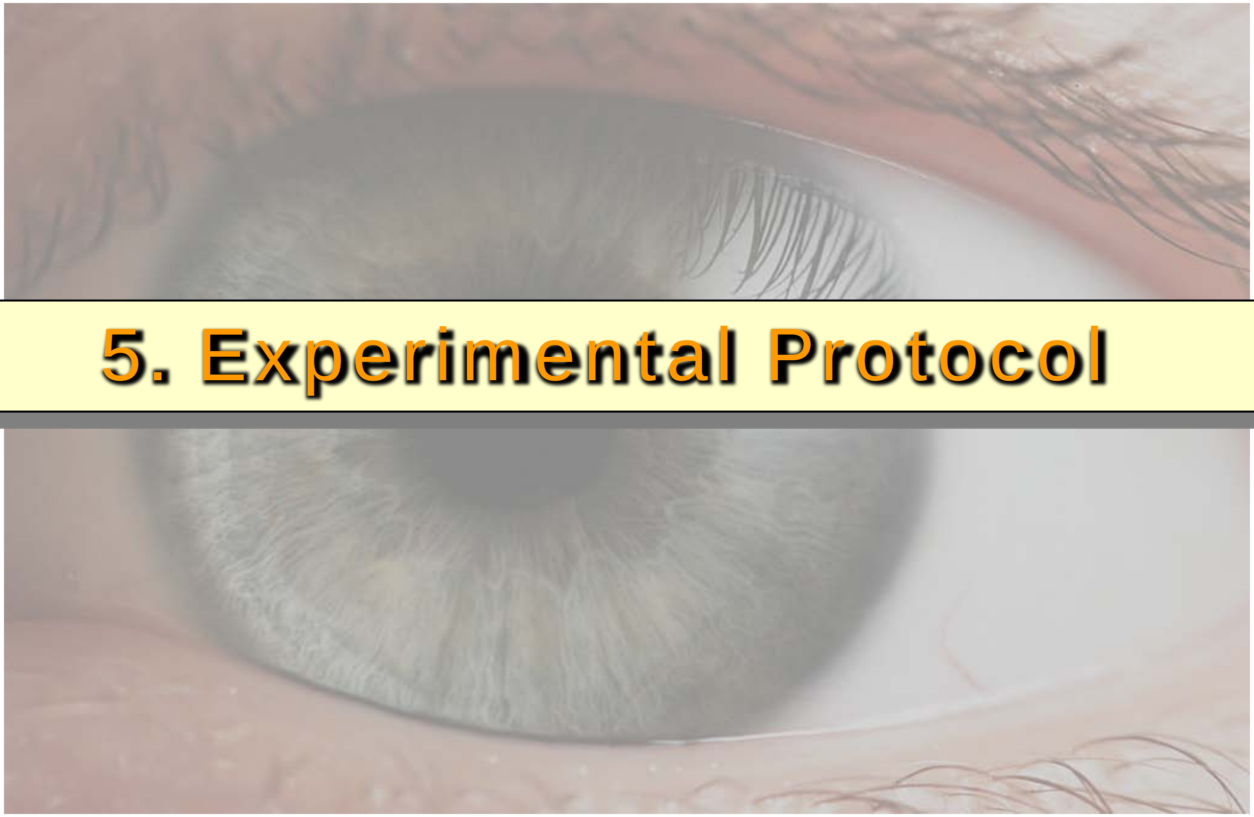
- **Stopping Criteria**:
  - The best score is higher than δ (RECONSTRUCTION OK!)
  - Score increase in the last generations is very small
  - Maximum number of generations is reached

The Solution: The Algorithm (II)



Normalized Iris Image

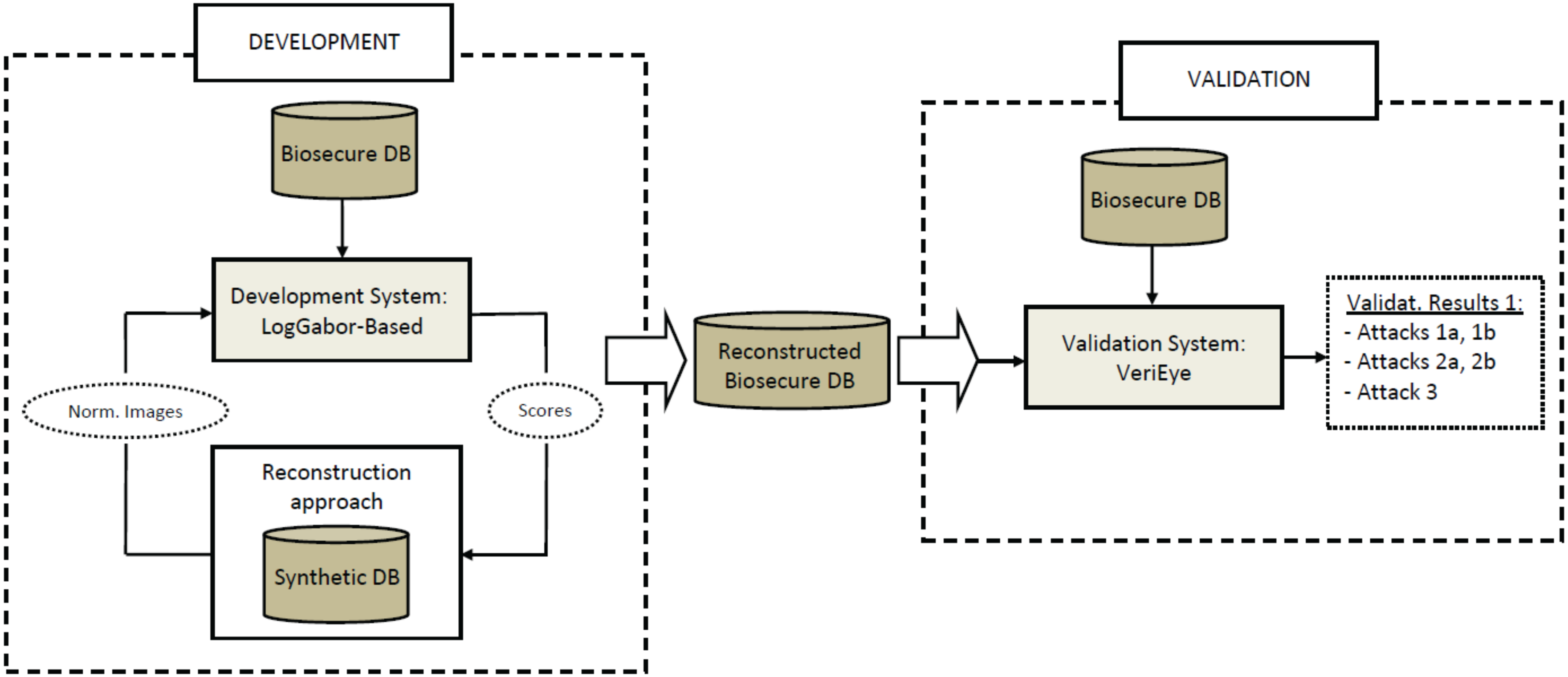




5. Experimental Protocol

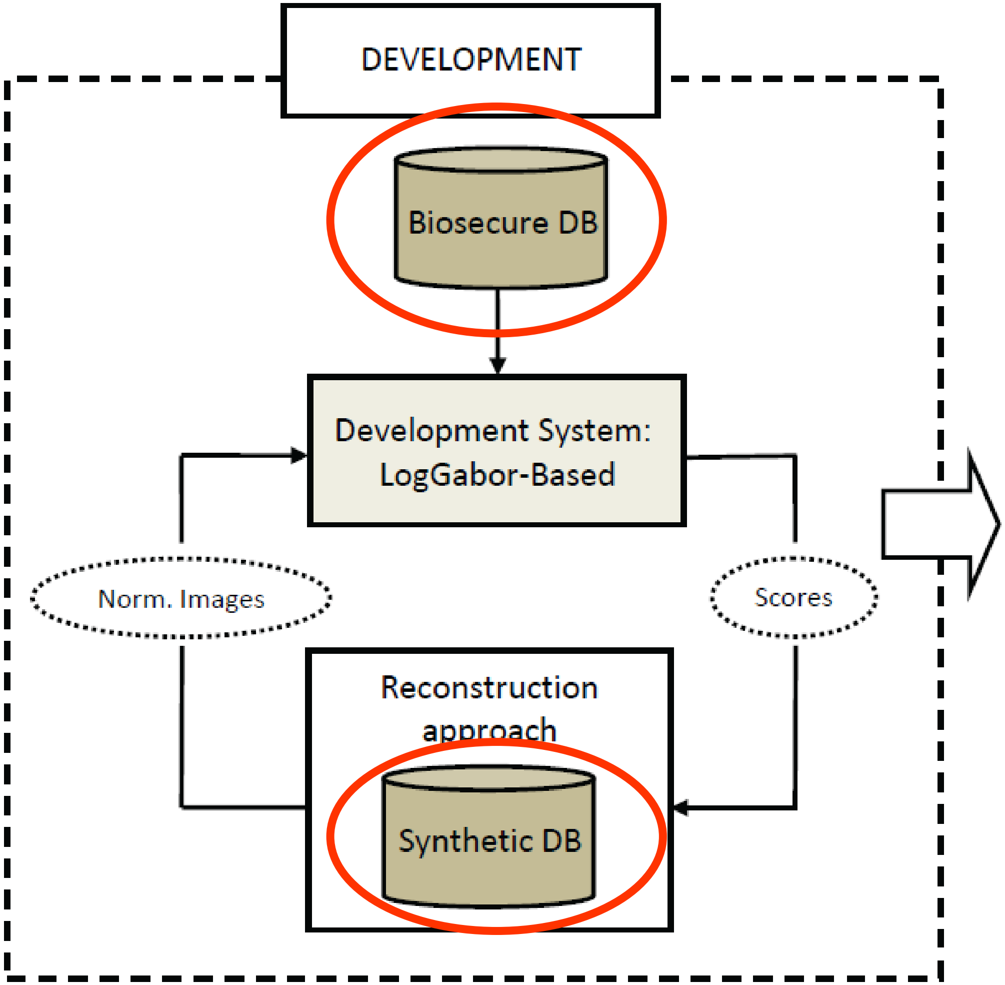
Development and Validation

- Avoid positively biased results
- Publicly available DBs and systems → reproducibility



Development: DBs (I)

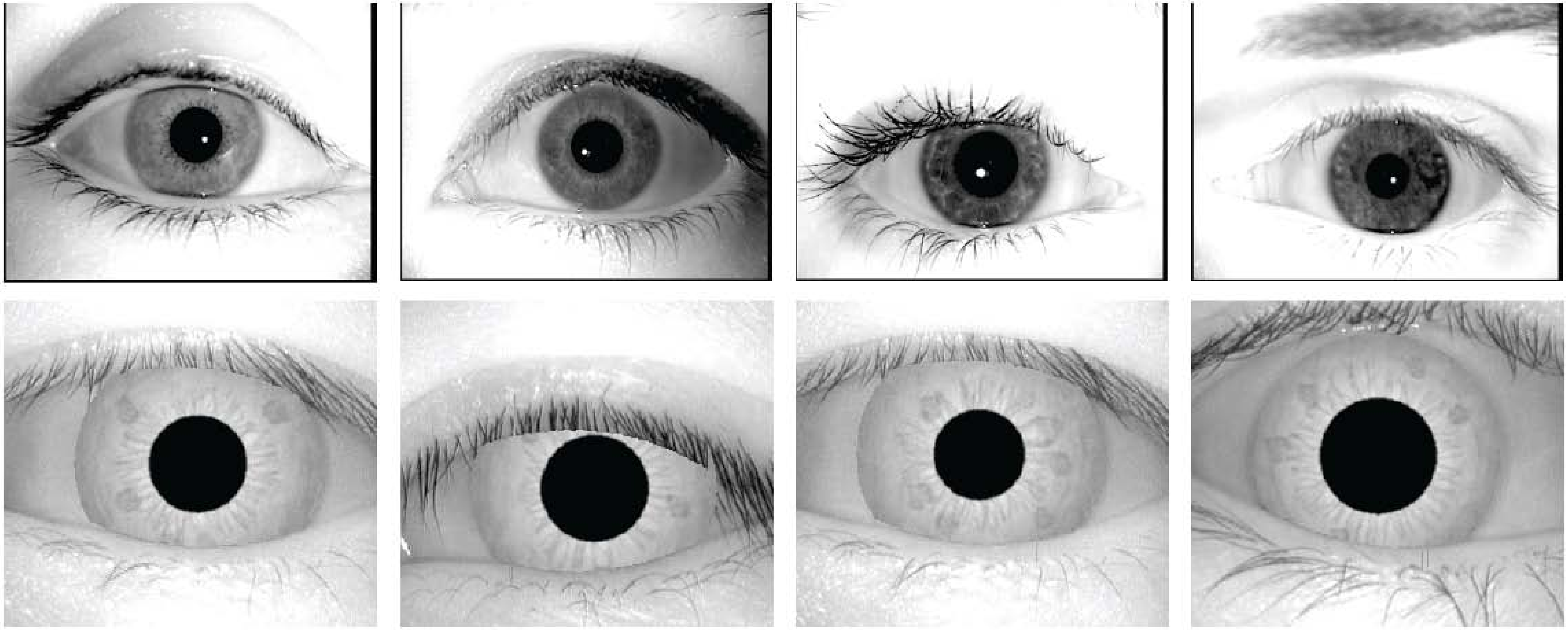
- **Development DBs**:
- Biosecure DE
  - 420 iris u
  - 2 sessior
  - 2 sample
  - Total of 4
  - Available
- Synthetic DB
  - 1000 use
  - 1 sessior
  - 7 sample
  - Total of 1
  - Available



rate P_0.

Development: DBs (II)

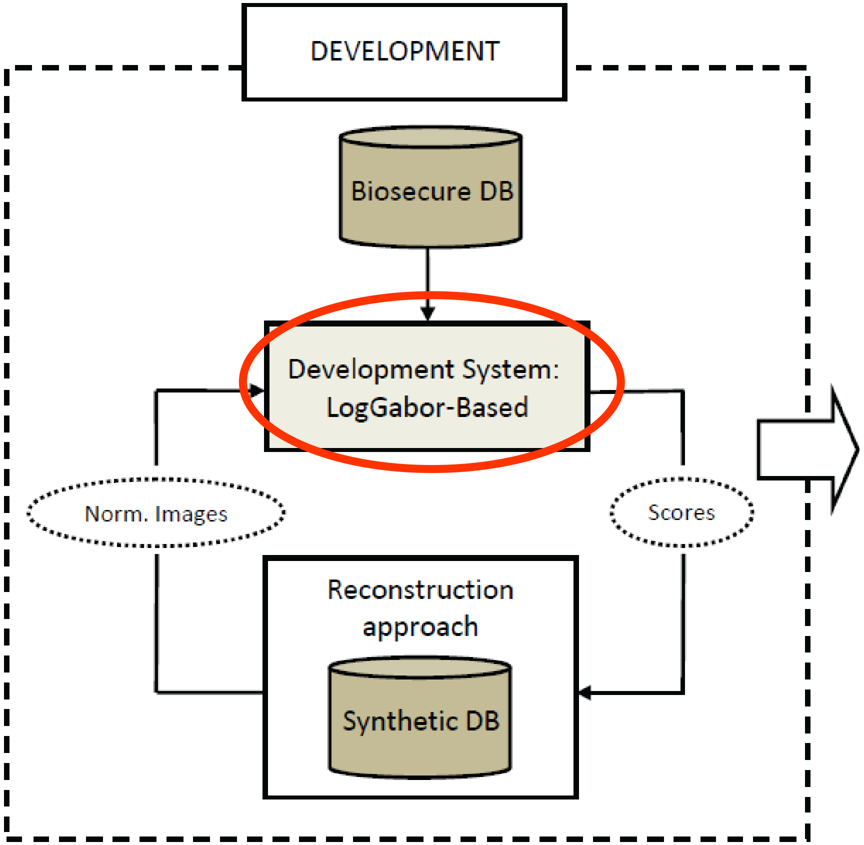
- Typical examples from Biosecure DB and SDB.
- Totally different → results are no biased.



Development: System

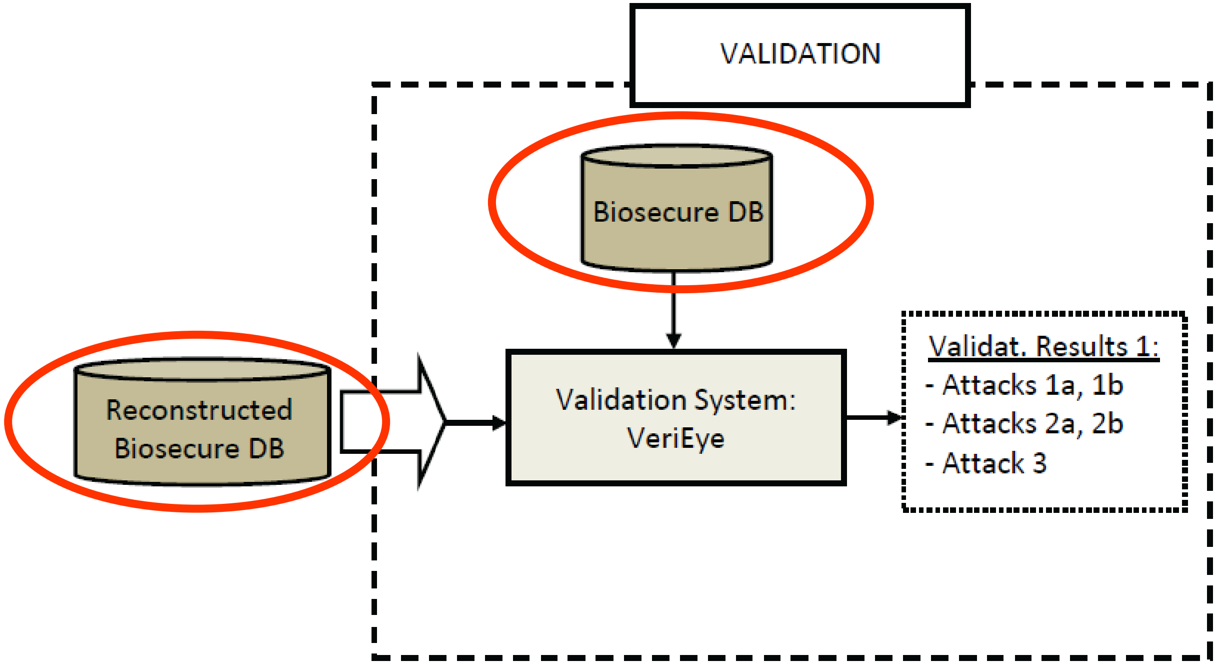
- **Development System**: academic implementation. Used to compute scores s_i in the reconstruction algorithm
  - Segmentation: iris and pupil boundaries → circles
  - Normalization: rubber sheet model
  - Feature encoding: based on 1D Log-Gabor filters
  - Matching: hamming distance

  - Available at: http://www.csse.uwa.edu.au/pk/studentprojects/libor/sourcecode.html



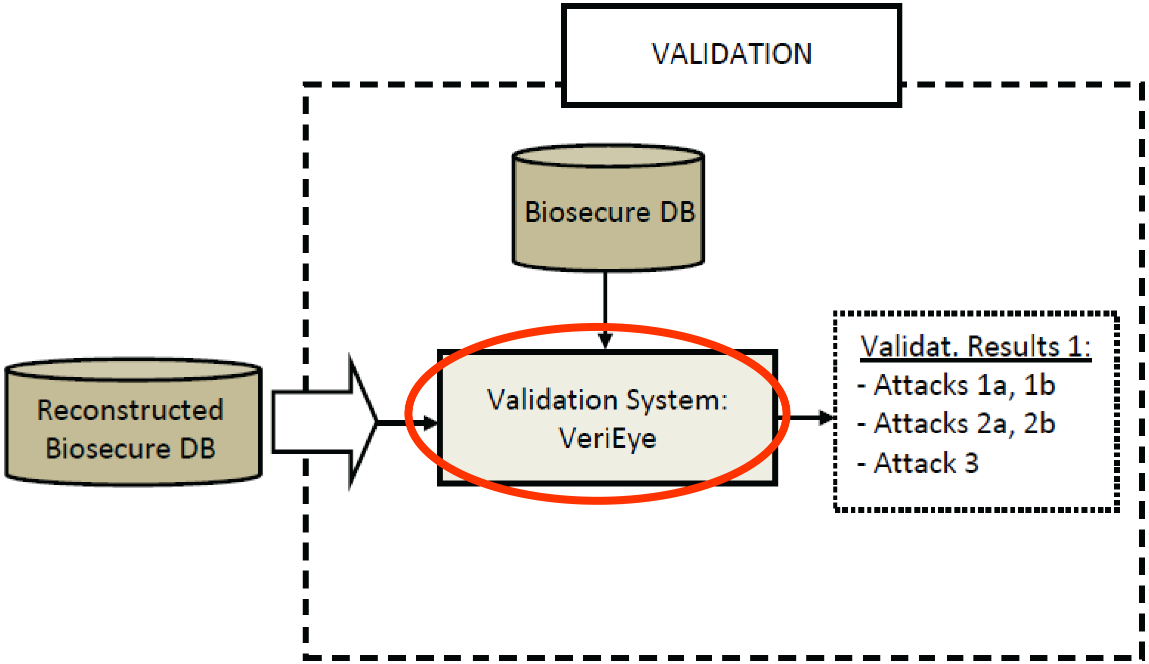
Validation: DBs

- **Validation DBs**:
- Biosecure DB: REAL database attacked.
- Reconstructed Biosecure DB: SYNTHETIC database used peform the attacks
  - 420 users
  - 5 reconstructions of 1 genuine sample per user
  - Total of 420 x 5 = 2,100 iris reconstructions



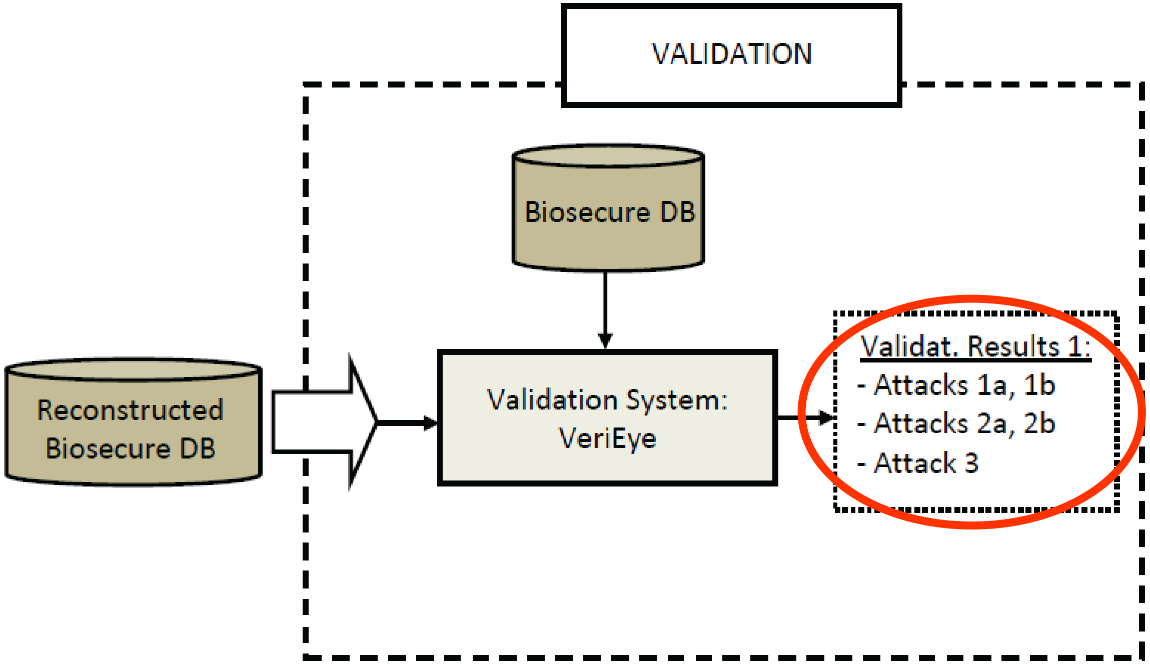
Validation: System

- VeriEye: commercial application
  - BlackBox: no info about how it works → unbiased results
  - It requires as input EYE images (NOT normalized iris images)
  - Available at: http://www.neurotechnology.com/verieye.html



Validation: Attacks

- Performance measure: Success Rate (SR) → $SR=A_s/A_T$
  - A_s = Successful attacks
  - A_T = Total attacks



- Types of a
  - **Attac**
    - At 0)
    - At =6300)
  - **Attac**
    - At
    - At 260)
  - **Attack 3**: average(4 real) vs 5 reconstructed (A_T=1x420=420)

Most likely attacking scenario

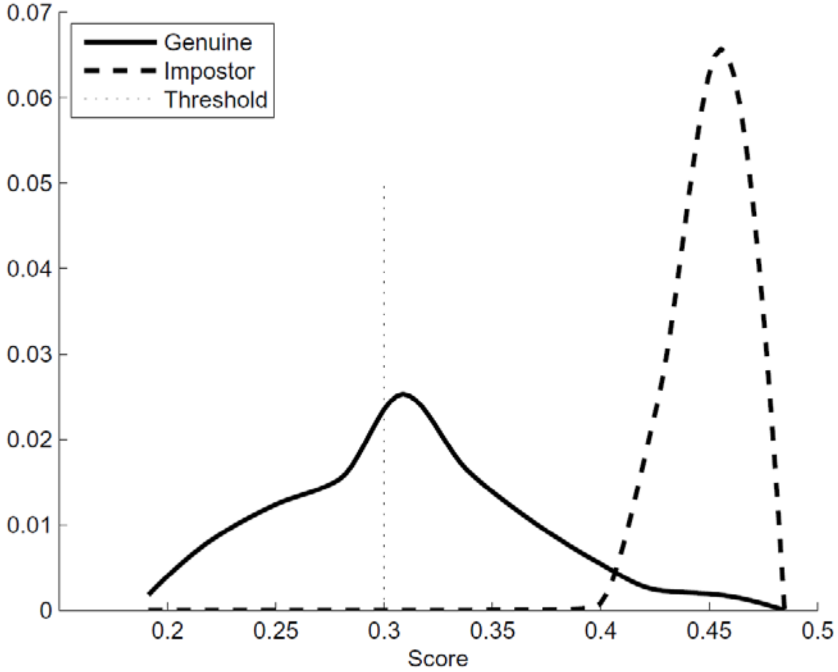
6. Results: Performance

Results: Development (I)

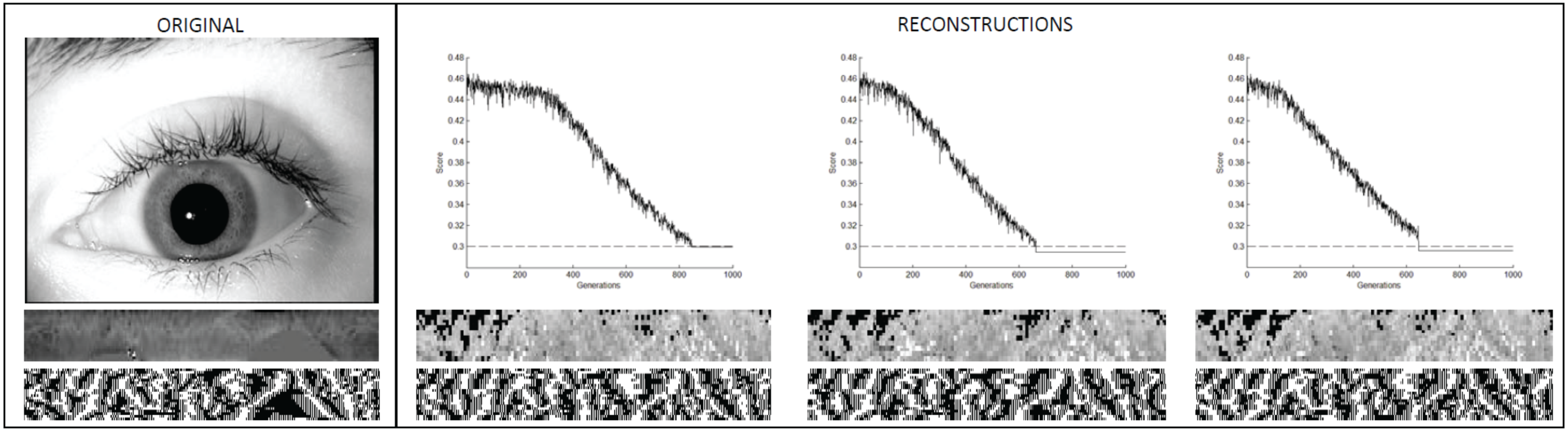
How do we know that an iris image is the reconstruction of a given template?

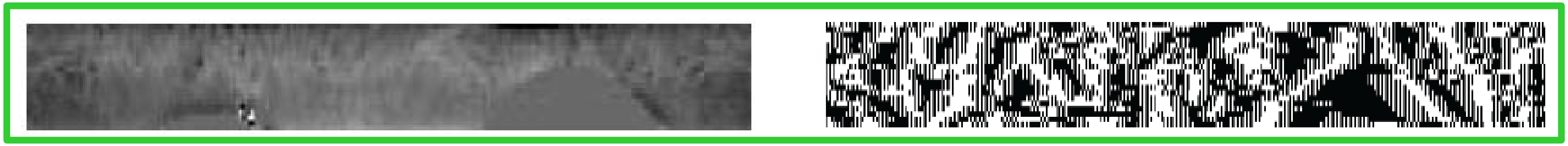
Because it is positively matched to the genuine template by iris recognition systems

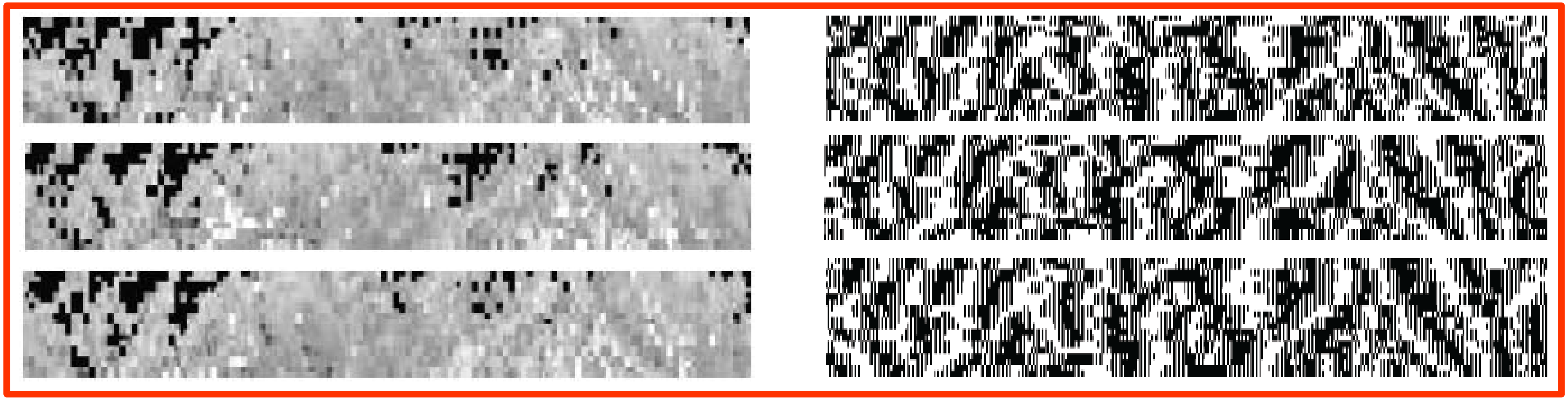
(score higher than a certain threshold δ)



Results: Development (II)



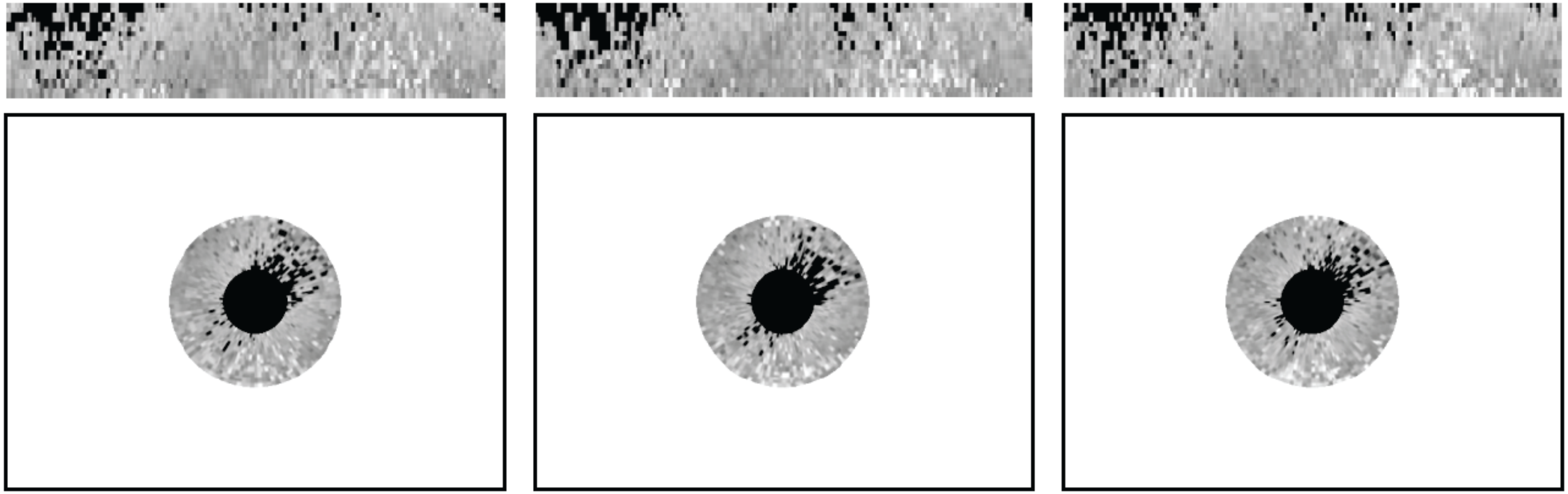




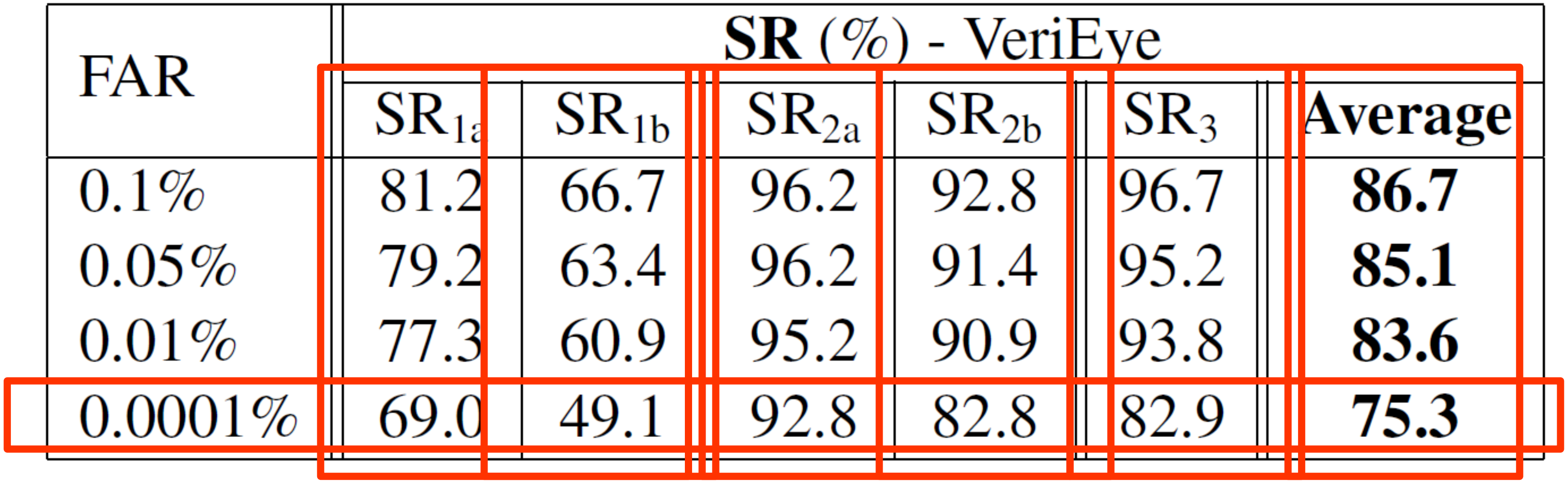
Results: Development (III)

- VeriEye (validation system): commercial application
  - It requires as input EYE images (NOT normalized iris images)

- Our EYE images look like...



Results: Validation (I)



FAR	SR (%) - VeriEye					
	SR$_{1a}$	SR$_{1b}$	SR$_{2a}$	SR$_{2b}$	SR$_{3}$	**Average**
0.1%	81.2	66.7	96.2	92.8	96.7	**86.7**
0.05%	79.2	63.4	96.2	91.4	95.2	**85.1**
0.01%	77.3	60.9	95.2	90.9	93.8	**83.6**
0.0001%	69.0	49.1	92.8	82.8	82.9	**75.3**

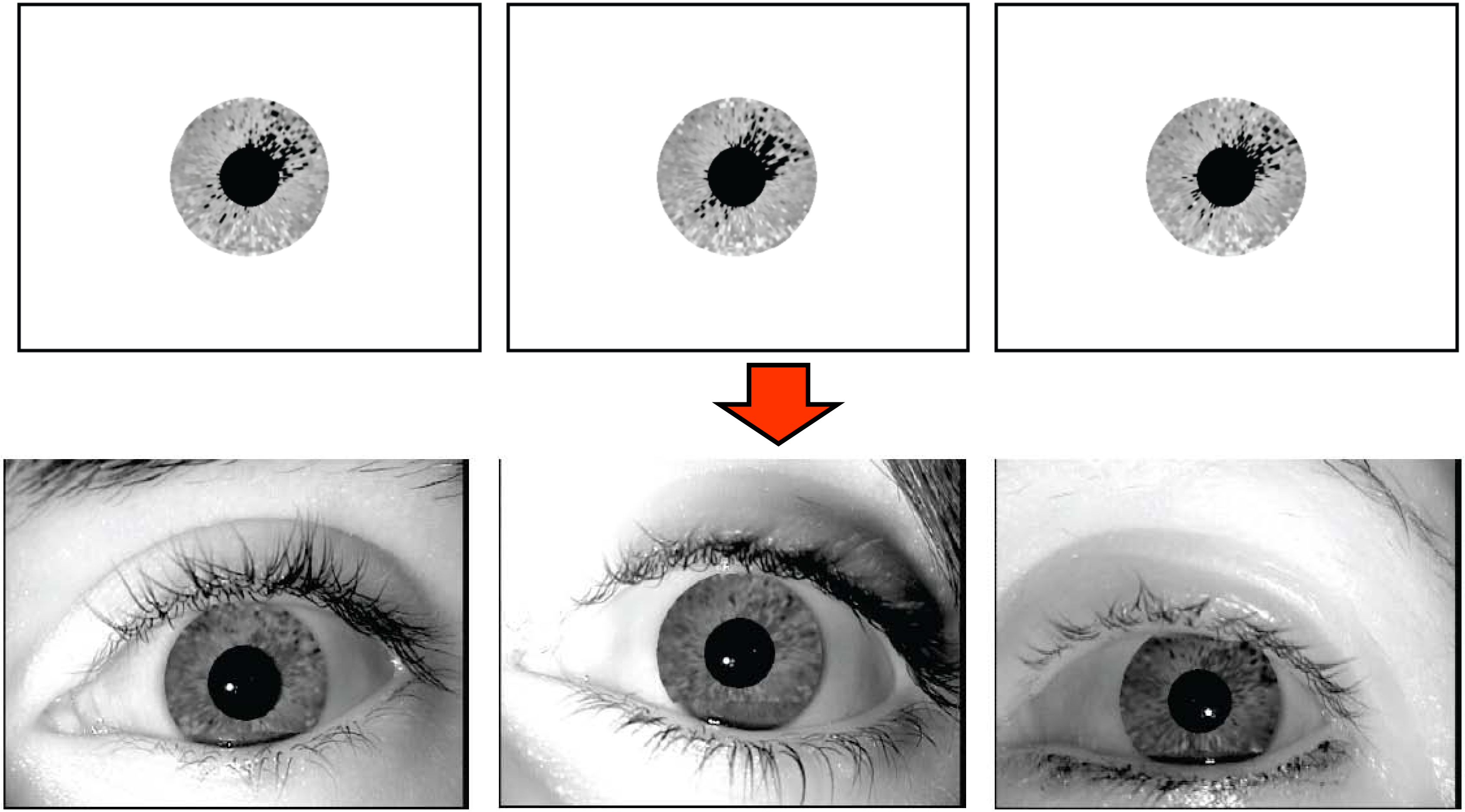
- The reconstruction algorithm is validated → very high performance
- Unrealistically high security scenario → 75% of breaking the system
- More likely to break the original sample, than other real sample from the same user.
- Still, very high probability of breaking other real samples.
- For the most likely attacking scenario → 92% SR
- More than one reconstruction → 30% SR increase
- Yet another new vulnerability → black circle+white background = Eye image

6. Results: Appearance

Results: Appearance (I)

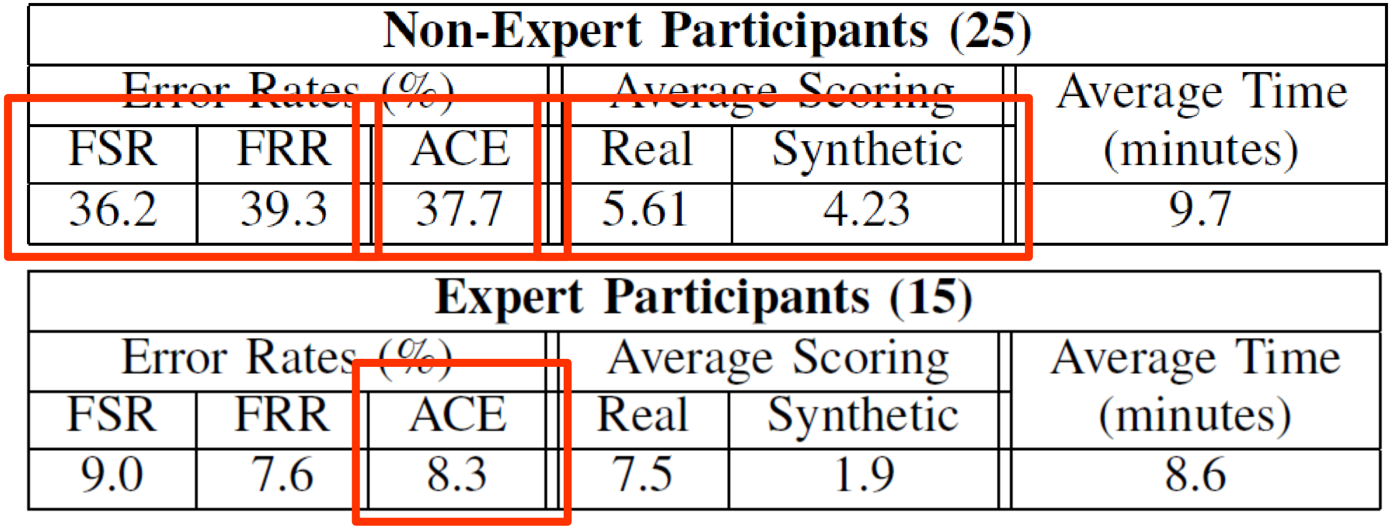
What about humans?

Are they deceived by the reconstructed irises?



Results: Appearance (II)

- 100 irises (50 real / 50 synthetic)
- 25 non-experts / 15 experts
  - Rank: 0 (fully synthetic) - 10 (fully real)
  - 15 minutes max.



Non-Expert Participants (25)

Error Rates (%)			Average Scoring		Average Time (minutes)
FSR	FRR	ACE	Real	Synthetic	
36.2	39.3	37.7	5.61	4.23	9.7

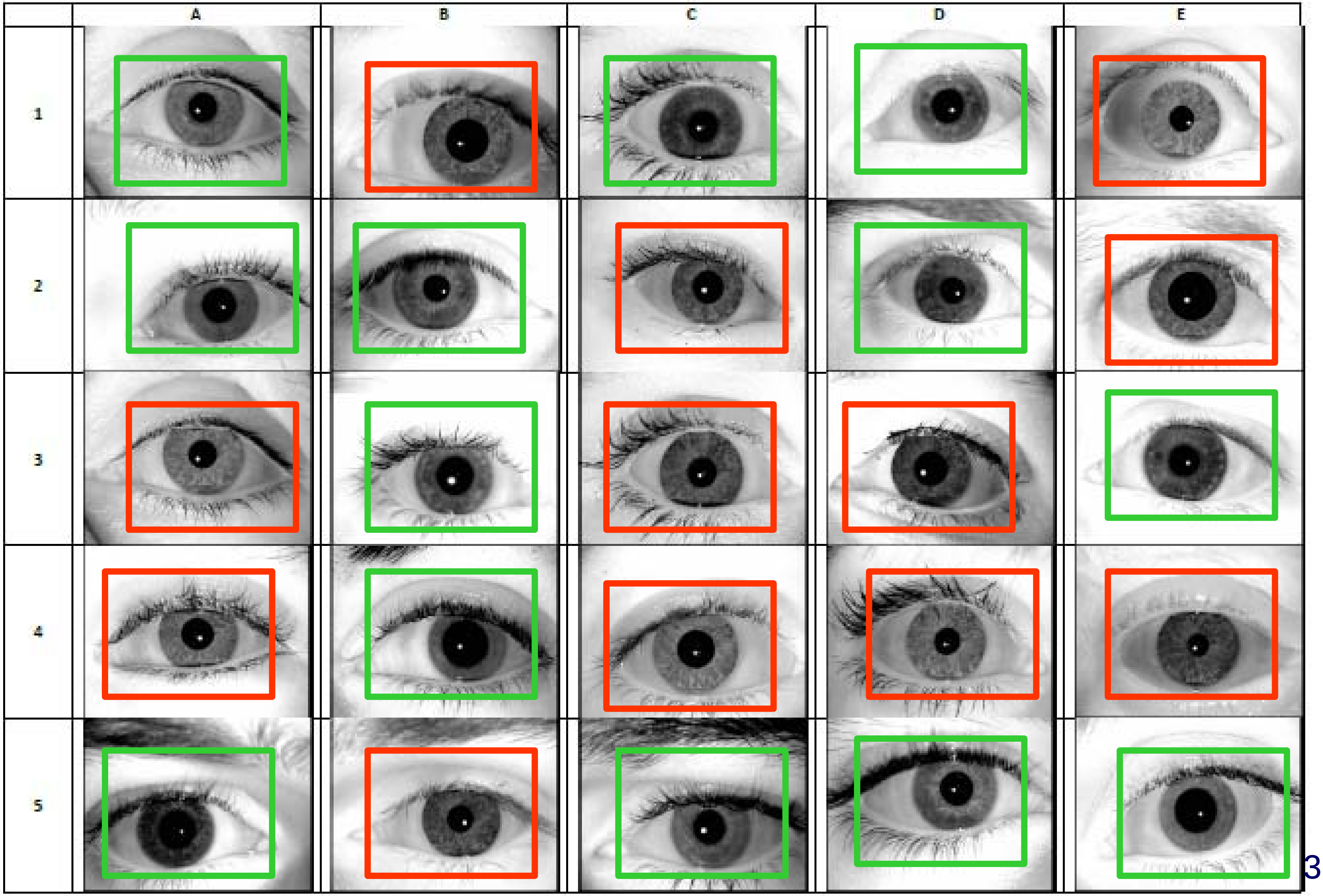
Expert Participants (15)

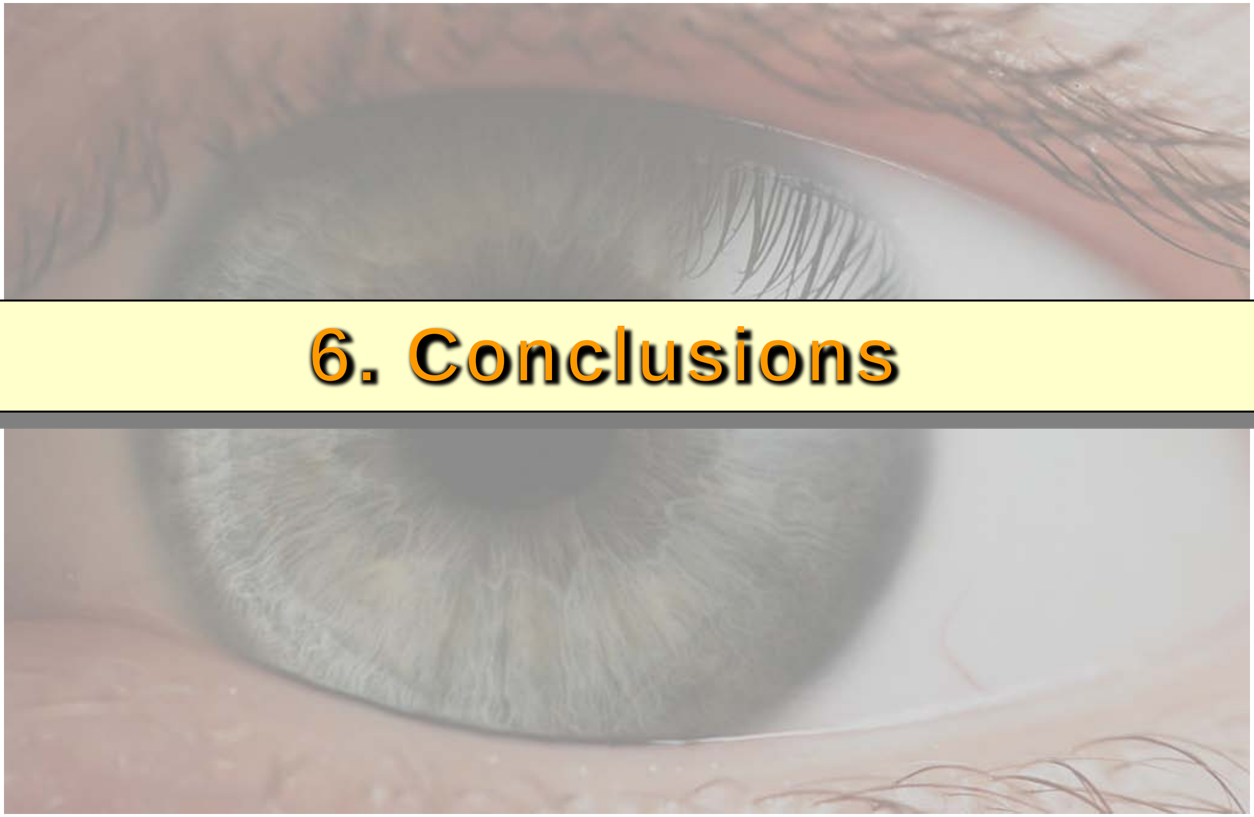
Error Rates (%)			Average Scoring		Average Time (minutes)
FSR	FRR	ACE	Real	Synthetic	
9.0	7.6	8.3	7.5	1.9	8.6

- Over 37% of misclassified irises by non-experts → real-like appearance
- FSR/FRR very close → not easier to distinguish one class over the other
- Average scoring very close → idem
- Not so easy with experts, but still possible

Results: Development (III)

- Would you like to try?





6. Conclusions

Conclusions

- Can iris images be reconstructed from the iriscode? → YES!
- Can this reconstructed images be used to successfully break iris recognition systems? → YES!
- Is it more dangerous to be able to reconstruct SEVERAL iris images? → YES!
- Should iris recognition systems check that what is being presented is really an eye image? → YES!
- Do the iris reconstructed images look real to the average human? → YES!

- To sum up... do we need to develop specific countermeasures for this new vulnerability? → YES!
  - Cryptography for the templates.
  - Liveness detection for the systems.

Javier Galbally

(javier.galbally@uam.es)

http://atvs.ii.uam.es

Escuela
Politécnica
Superior

ATVS

UAM
UNIVERSIDAD AUTONOMA
DE MADRID