FACING and UNIQUEMARK

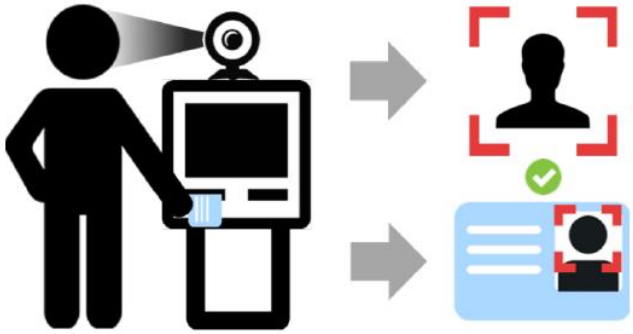
Recognizing identities beyond facial recognition

Coimbra | 2022-07-14

vis team
isr-uc

Summary

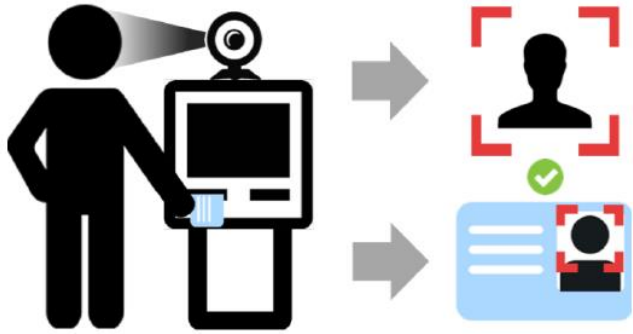
1. **FACING** challenges
    1. ICAO (International Civil Aviation Organization) compliance
    2. Face recognition
    3. Morphing attack detection
    4. Liveness detection
    5. Biometric template protection
2. **UniqueMark**



Security processes for biometric (facial) recognition

Summary

1. **FACING** challenges
    1. ICAO (International Civil Aviation Organization) compliance
    2. Face recognition
    3. Morphing attack detection
    4. Liveness detection
    5. Biometric template protection
2. **UniqueMark**

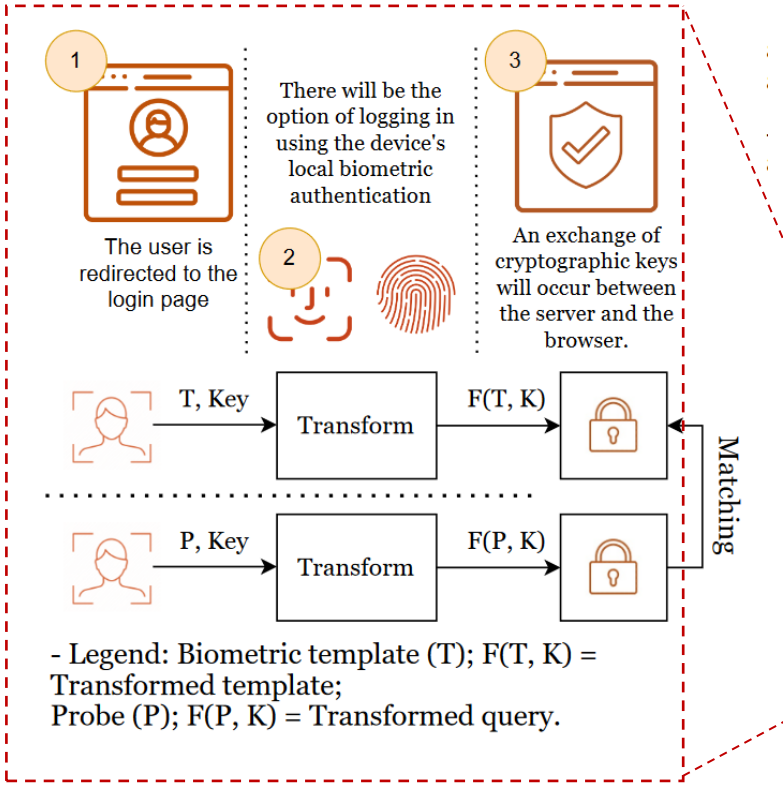


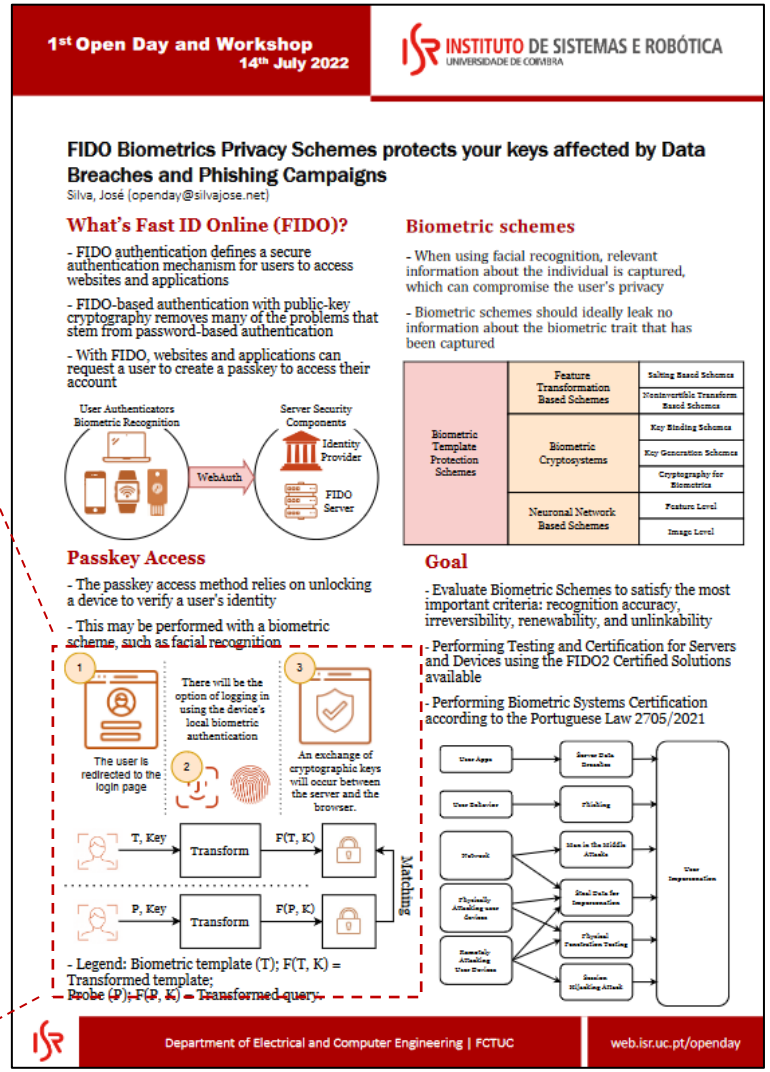
Security processes for biometric (facial) recognition

Biometric template protection

Please take a look on José Silva poster

"FIDO Biometrics Privacy Schemes protects your keys affected by Data Breaches and Phishing Campaigns"



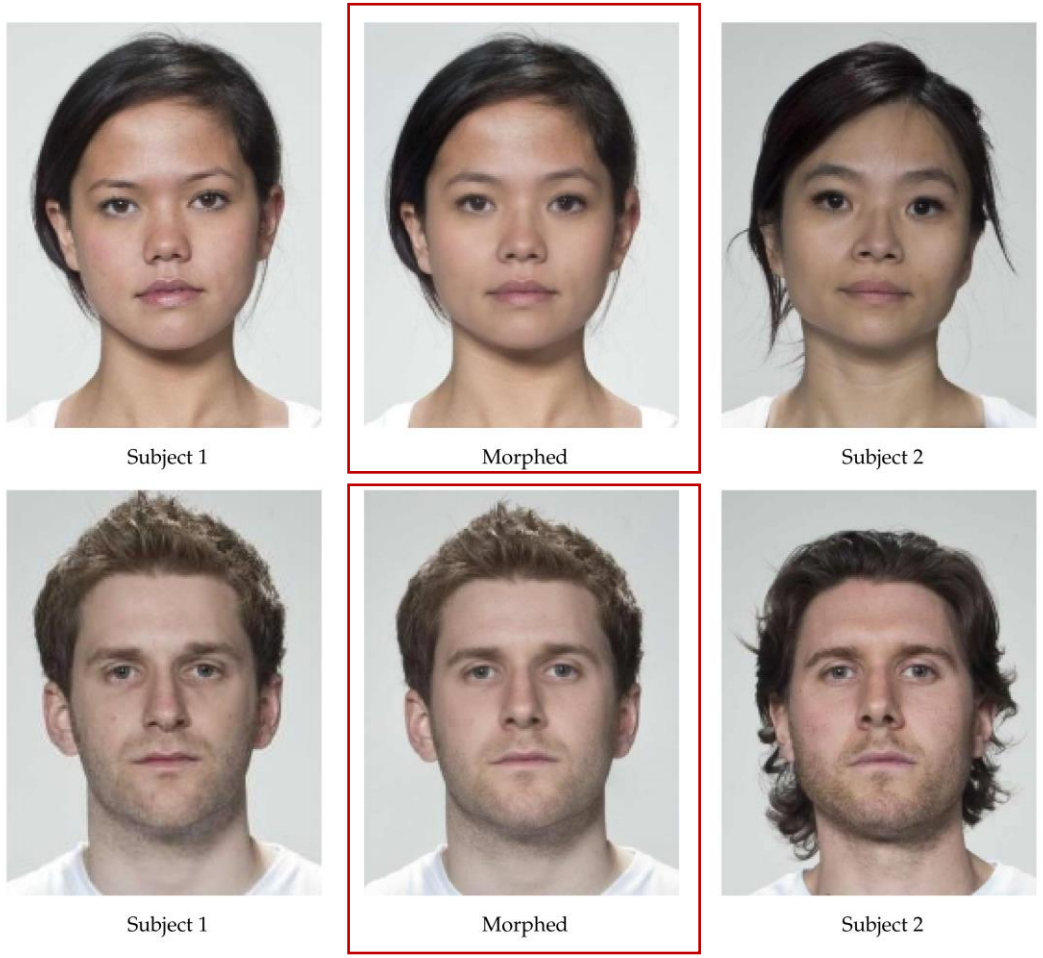


FACING - Morphing

Face Morphing

Image morphing techniques are used to combine information from two (or more) images into one image.

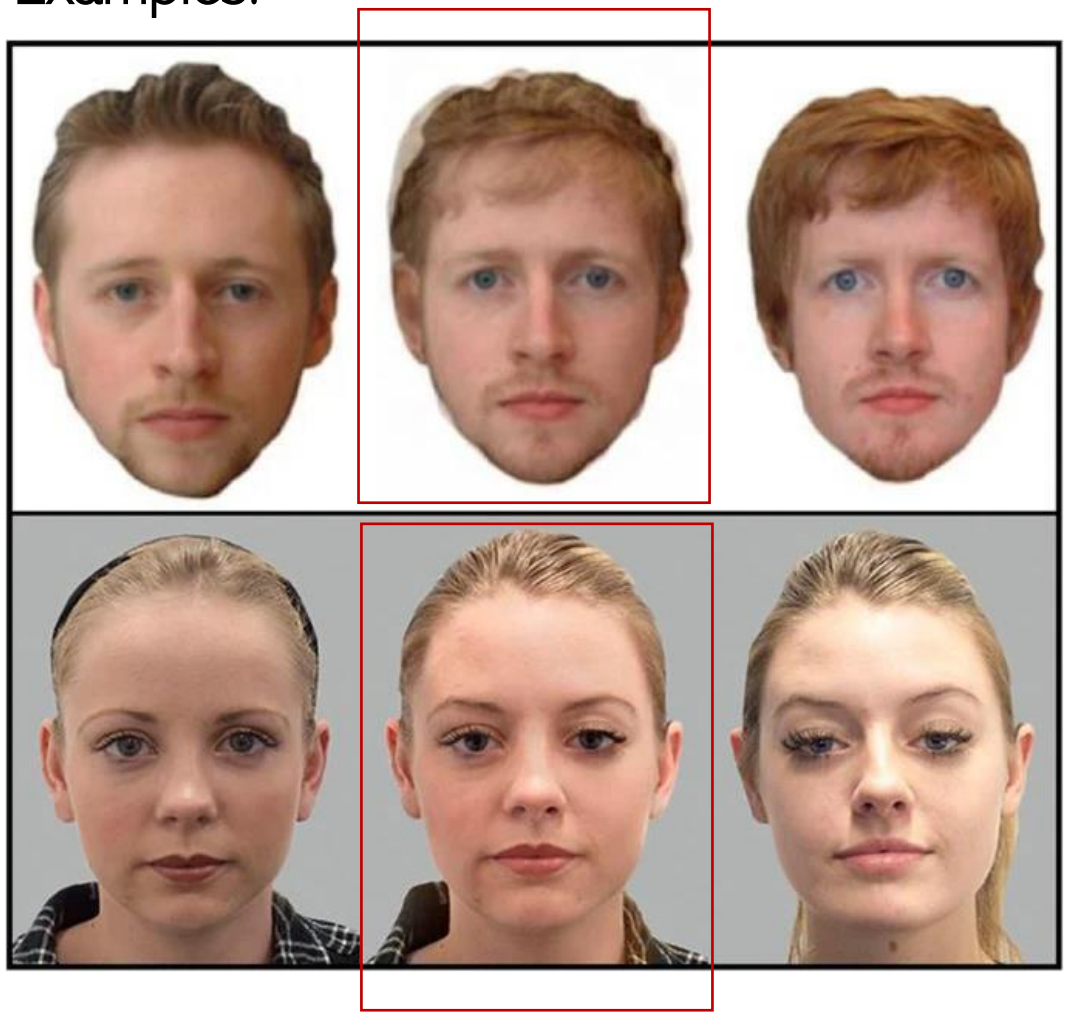
Examples:



Face Morphing

Image morphing techniques are used to combine information from two (or more) images into one image.

Examples:



Morphing attacks:

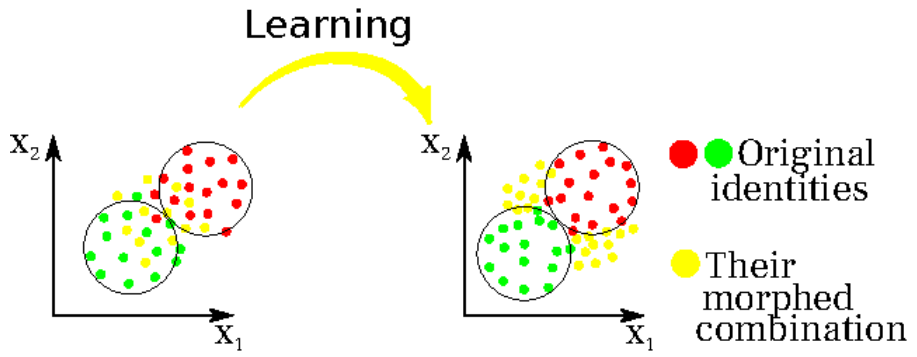
- Face Morphing oppose significant risks for document security.
- Two scenarios of morphing detection are usually considered:

  - **No-reference** (enrollment scenario)
  - **Differential** (border control scenario)

Metodology

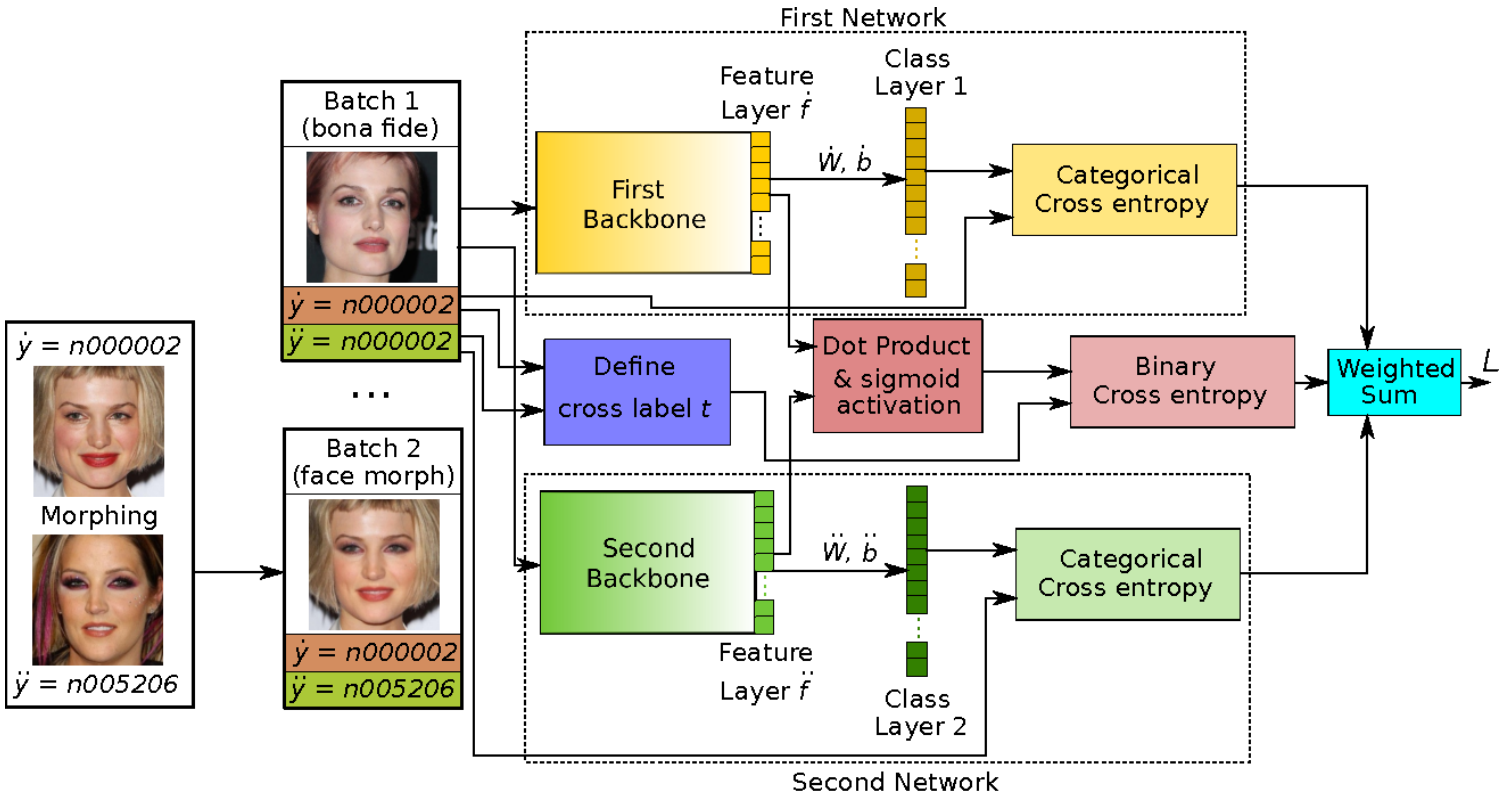
- We propose to investigate several strategies for no-reference morphing detection and improving resistance of face recognition to face morphing.

- Our approaches imply following deep learning based face recognition and designing sophisticated sample mining techniques with use of morphed face images for better control of deep feature distribution.

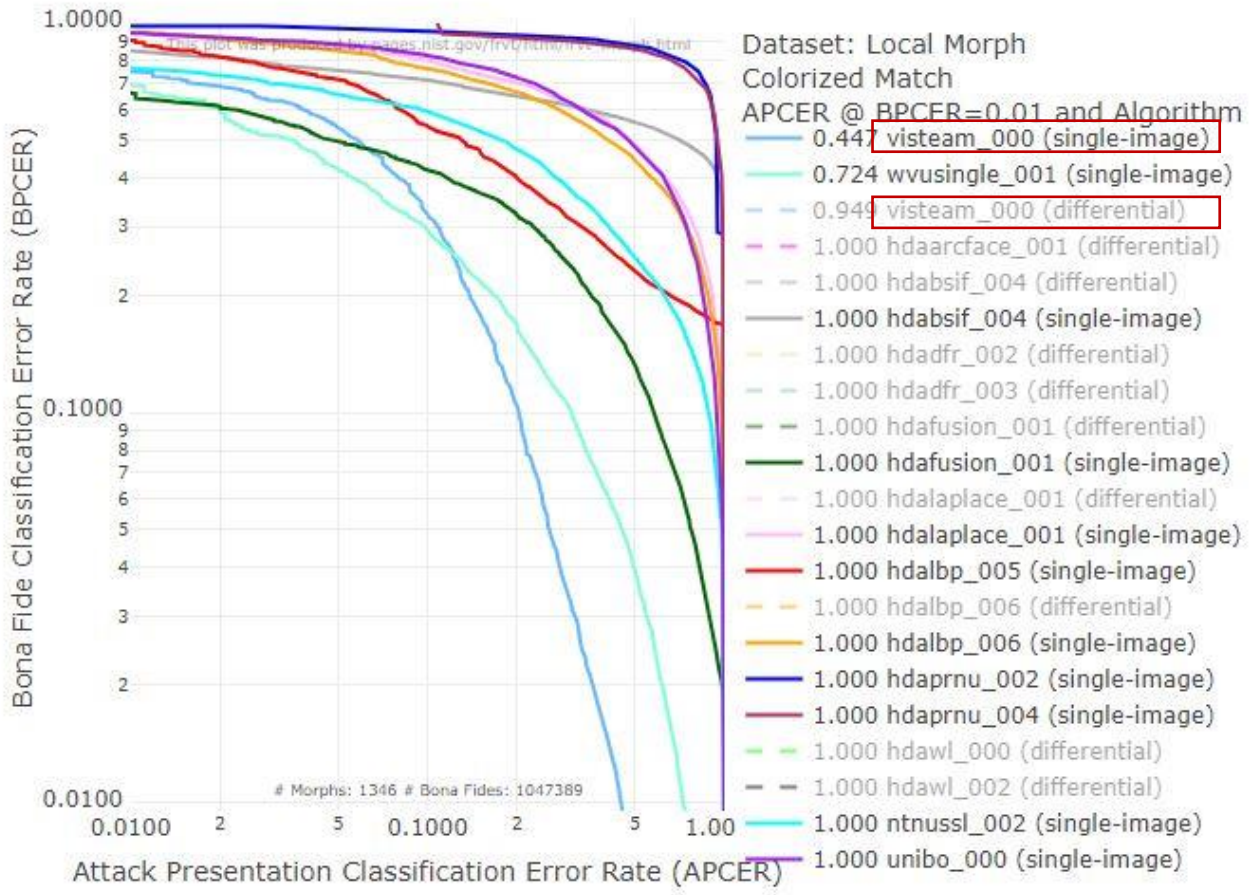


Architecture:

Our complex architecture and sophisticated class labeling strategy allows to learn deep face features, which carry information about authenticity of these features



NIST FRVT MORPH benchmark results



Conclusion and current achievements:

- State-of-the-art performance in several benchmarks of NIST FRVT MORPH.
- The project have received the direct Nvidia Hardware support.
- First publication is pending for reviews.

Further work:

- Refine no-reference morphing detection for the new NIST report.
- Expand the method to differential morphing detection.

FACING – Liveness detection

Liveness detection:

- What is **liveness detection**? Liveness Detection or Face Anti Spoofing is the task of verifying if a face presented to a system is real or an attack (*bonafide* or *spoof*)

- What is meant by "**attack**"? An attack is any attempt to change the identity of the individual who presents himself to the system, either by obfuscating his own identity or by impersonation (em português: representação ou personificação) of another subject.

Types of attacks

Print attack: display a printed image (photo)to an authentication system

Replay attack: display a video recording

Mask attack: covering one's face with a material which may present or not human facial features (impersonating or obfuscating)

Approaches

Before deep learning :

- **1)** looking for signs of liveliness, such as the micro movements of the face in a video or the heartbeat
- **2)** take a histogram of the image and according to the developed classifiers make the decision.

Currently: the vast majority of methods developed are based on Convolutional Neural Networks, because they can generalize better (it is overparametrized)

Difficulties

- All difficulties are related to the inability to **generalize the problem**
- The is no solution that works perfectly for all attacks, because there isn't a **dataset** with all the examples of attacks or that includes videos with all the possibilities of lighting or individuals from all over the world.
- The **resources** used for the problem. Excellent results are obtained with depth images but not everyone has mobile phones with this capability
- The challenge is to reduce the difference between the academic context and everyday life

UNIQUEMARK

A Method to create and authenticate a unique mark in precious metal artefacts

INCM Portuguese Mint and Official Printing Office

+500 years in mint production

UniqueMark is a product that offers:

- A **unique**, **unclonable mark** for each object (precious metal)
- A marking process using a **punch** or a **laser**
- A complete system to register and trace objects
- A complete system to validate the authenticity of marks and
- objects using **cameras**, **microscopes** or **smartphones**

How to achieve a unique mark:

Physically Unclonable Functions are:

- Unique for each object
- Natural to the material of the object (characteristic of each object) or created by a random chaotic process
- Practical to validate in terms of authenticity
- Impractical to reproduce and replicate with the same exact result

UniqueMark

UNIQUEMARK CREATION

PUNCHING WITH DIAMOND PARTICLES

LASER MARKING WITH DETERMINISTIC PATH

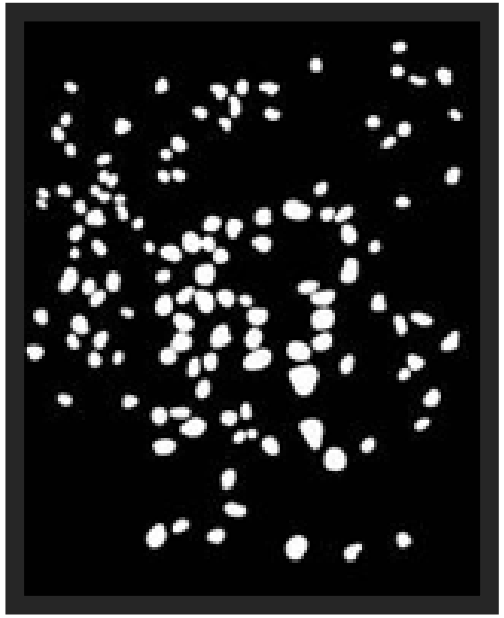
UNIQUEMARK REGISTRATION

UNIQUEMARK VALIDATION

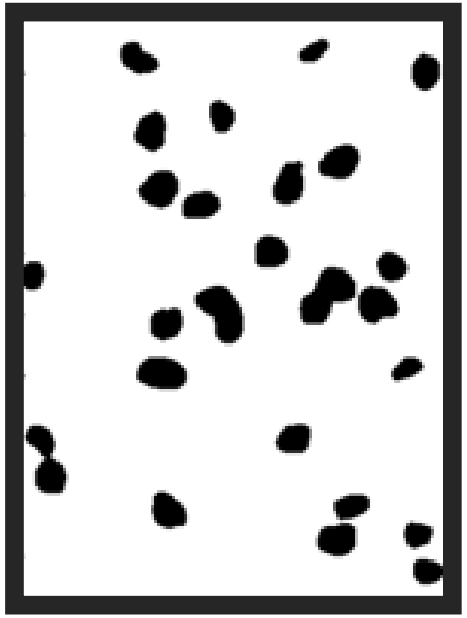
UniqueMark

Punching with diamond particles

Gold (material)



Pattern



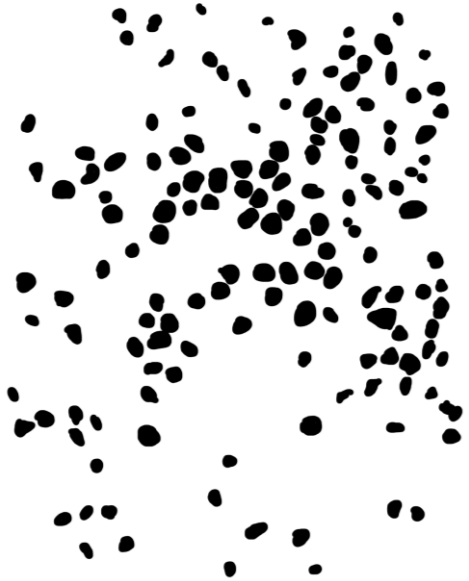
Pattern

Brass (material)

UniqueMark

Some more details on the punching process:

- Particles have approximately diameter between 40 and 100 micros
- Marks have approx. 1 mm2 but can be made of any dimension
- Number of particles depend on the desired density :
  - complexity and search time increase with the number of particles
  - discriminatory capacity decreases for a too low number of particles
  - number of particles between 100 and 200 seems to be adequate
- Vibration in the deposition of particles is important

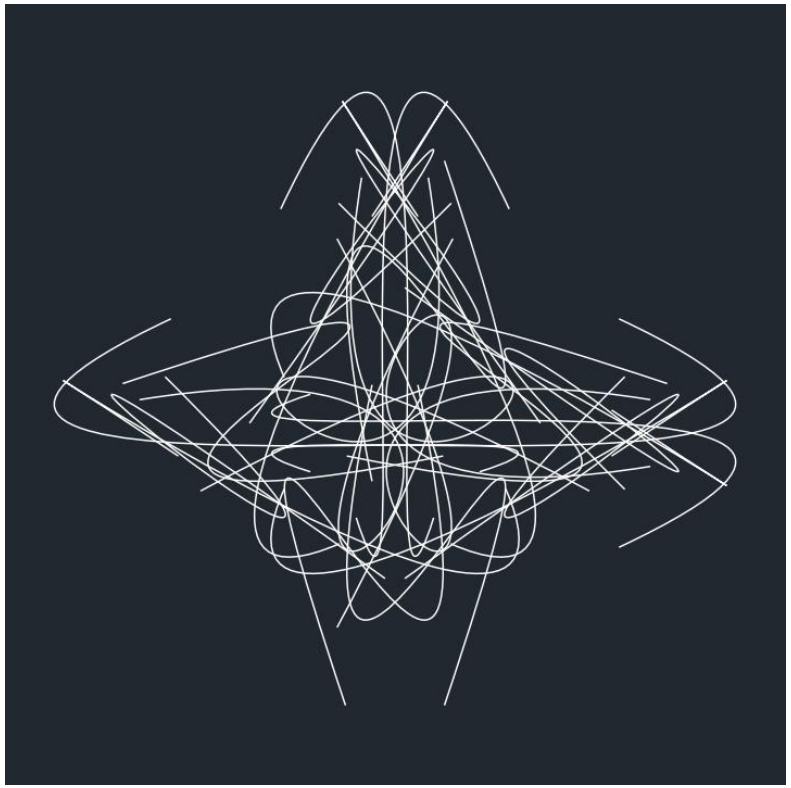


UniqueMark

Laser mark with a deterministic drawing:

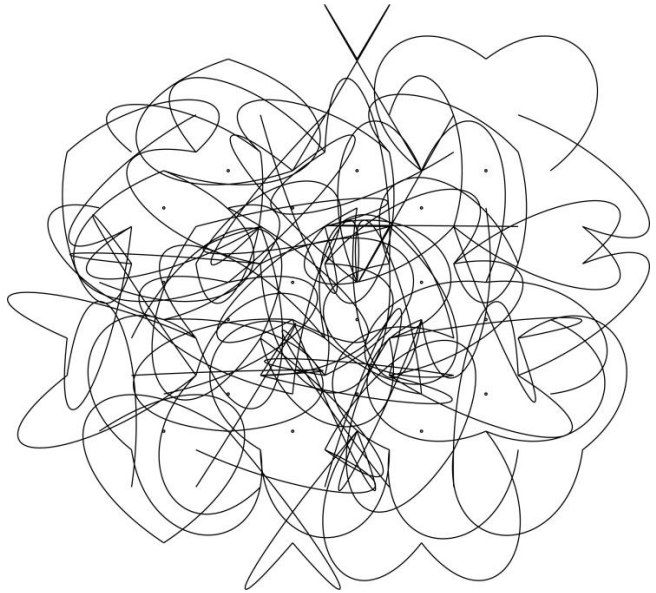
- Mark a deterministic drawing using laser
  - Mathematical description of the drawing to maximize uniqueness
- If the drawing is intricate enough the result is a unique irreproducible mark
- Although the drawing is deterministic, the reproduction of the same drawing in another mark will produce different distinguishable marks due to different behaviour of the supporting material

Examples of laser marks

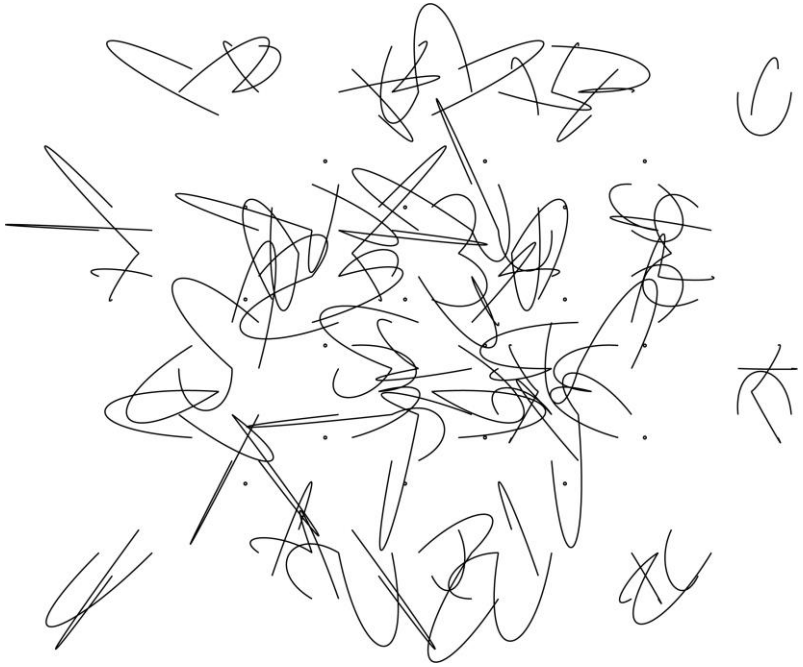


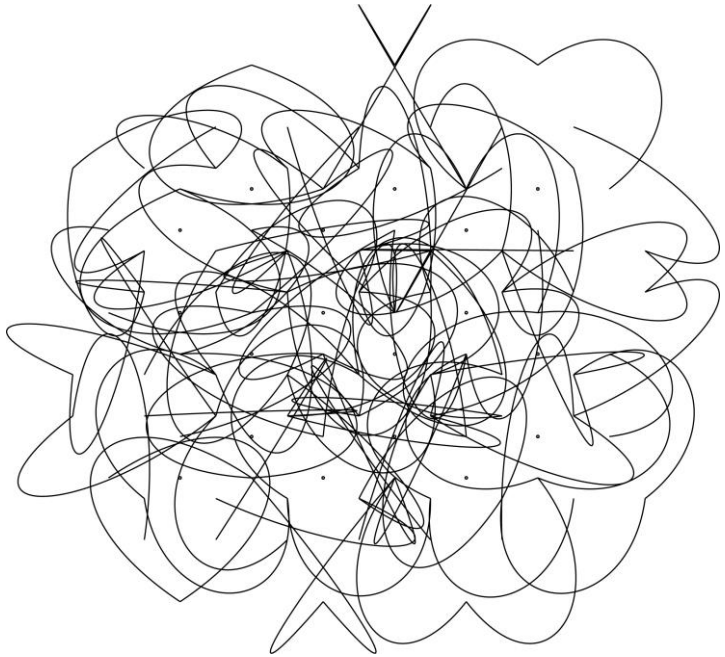
Laser mark with a deterministic drawing

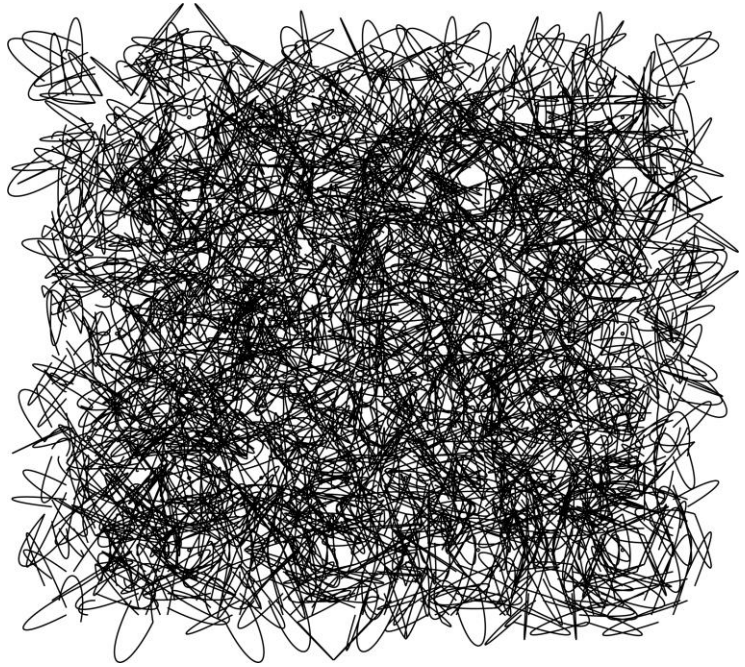
Laser mark with a deterministic drawing *(cont.)*



Laser paths (drawings) with different levels of density



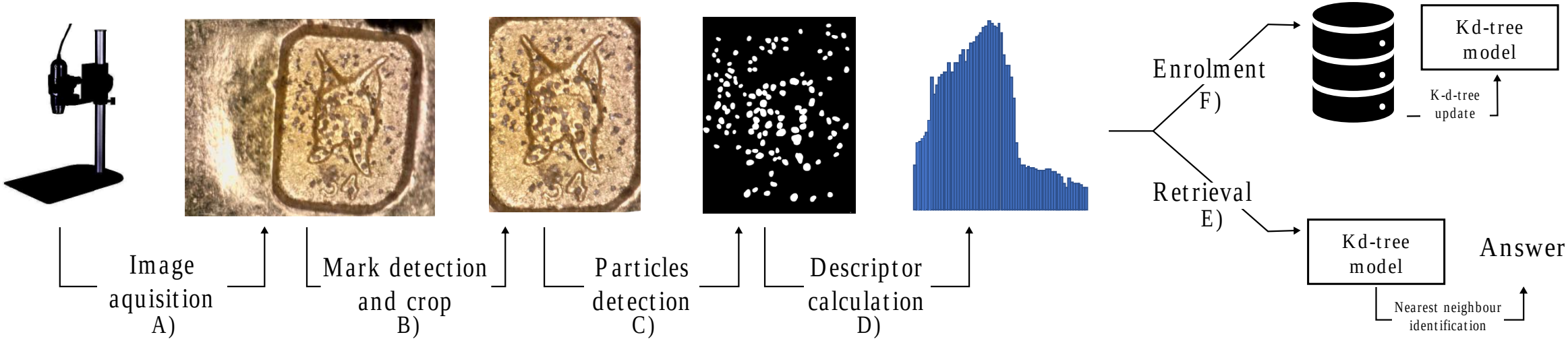




UniqueMark

UNIQUEMARK CREATION → **UNIQUEMARK REGISTRATION** → **UNIQUEMARK VALIDATION**

Registration and validation pipeline



Validation and traceability

- Validation:
  - UniqueMarks can be validated using smartphones or consumer cameras
  - Several levels of security and validation
    - for consumers – simpler and ubiquitous
    - for professionals, producers and authorities – complex and highly secure
  - No fraud is possible - one object, one marking, one identity
- Traceability:
  - Georeferencing data can be saved
  - Items can be easily tracked
  - Producers and authorities can improve knowledge about items, the market and consumers

Thank you!

Visit us at:

https://visteam.isr.uc.pt