Digital Security of Physical Objects

Slava Voloshynovskiy
Stochastic Information Processing Group
University of Geneva
Switzerland

Outline

- Physical object security
- Why not traditional security?
- Proposed solutions for
    - Object recognition
    - Design verification
    - Physical uncloneable functions
- Conclusions

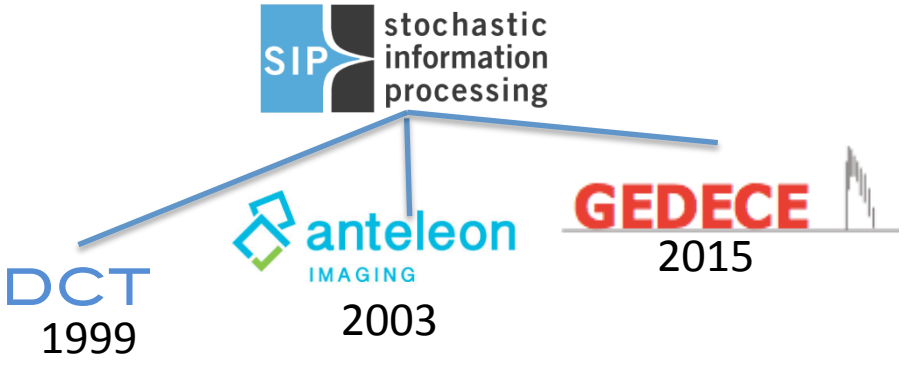
SIP group at glance

- **Basic facts:**
  - Founded in 1998
  - Currently 8 people
  - Group produced 10 PhDs

- **Main background:**
  - Statistical image processing
  - Information theory
  - Machine learning

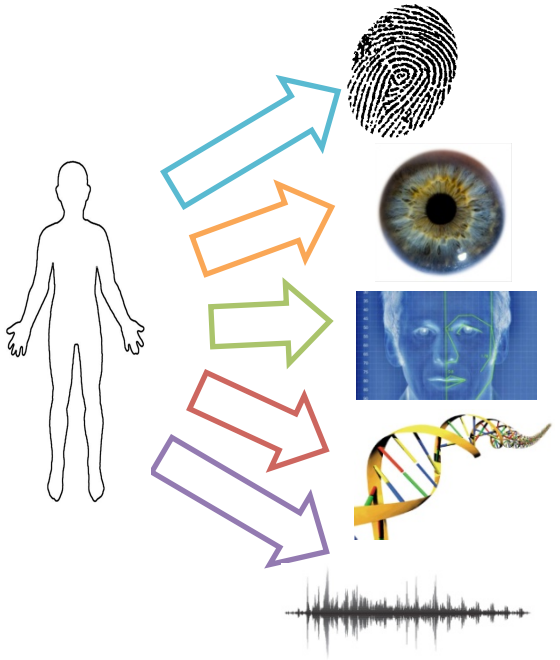
- **Expertise in:**
  - Digital watermarking
  - Fingerprinting
  - Physical object security

- **Technology valorization:**
  - 6 licensed patent families
  - 3 spin-offs

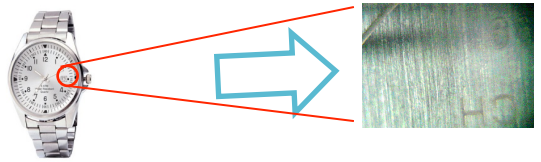


1. Physical object security

Humans = biometrics

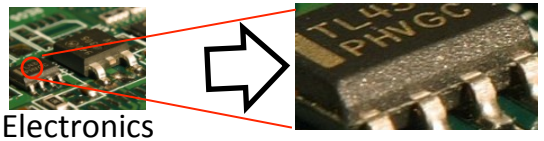


Physical Objects



Watches

Packaging



Electronics

All physical objects are unique like humans

Why security is important?

- Damage of brand reputation
- Loss of profit
- Danger for life
- …..

Main security concerns

- Authenticity
- Origin (identification)
- Ownership
- Track and trace

2. Why not “traditional” security

Main restriction of existing security technologies for physical objects:

- Proprietary technologies (rare or expensive materials, inks, holograms, etc.)
  - obsolete and easy to clone by modern means
  - expensive for mass markets
  - special equipment or special knowledge of original features are required

- Crypto security
  - not directly applicable to noisy data
  - very sensitive to light and geometrical variations

- RFID/Connected devices/Internet of Things
  - still quite expensive
  - serious security wholes

2. Why not “traditional” security

Requirements to modern physical object security:

- **easy to verify authenticity but difficult to clone**
  - cloning should economically inefficient
- **non-proprietary: based on physical-crypto principles**
  - protection mechanism is assumed to be public
- **no special equipment required**
  - preferably on mobile phone (in possession of everyone)
- **no special training required**
  - any user can validate it
- **cheap and scalable to mass markets**
  - millions or billions of products
- **non-invasive**
  - products and production should not be modified

3. Product security: a framework

Typical object features

Micro features of design

Micro features of carrier (PUFs)

Three levels of security:

- Object recognition
  - Printed/reproduced visible features typical for all object of the same category

3. Product security: a framework

Typical object features

Micro features of design

Micro features of carrier (PUFs)

Three levels of security:

- Object recognition
  - Printed/reproduced visible features typical for all object of the same category
- Design verification
  - Features of probe are verified wrt features of original template

3. Product security: a framework

Typical object features

Micro features of design

Micro features of carrier (PUFs)

Three levels of security:

- Object recognition
  - Printed/reproduced visible features typical for all object of the same category
- Design verification = digital forensics
  - Features of probe are verified wrt features of original template
- Individual object identification
  - Features of probe carrier are tested wrt features of enrolled PUFs

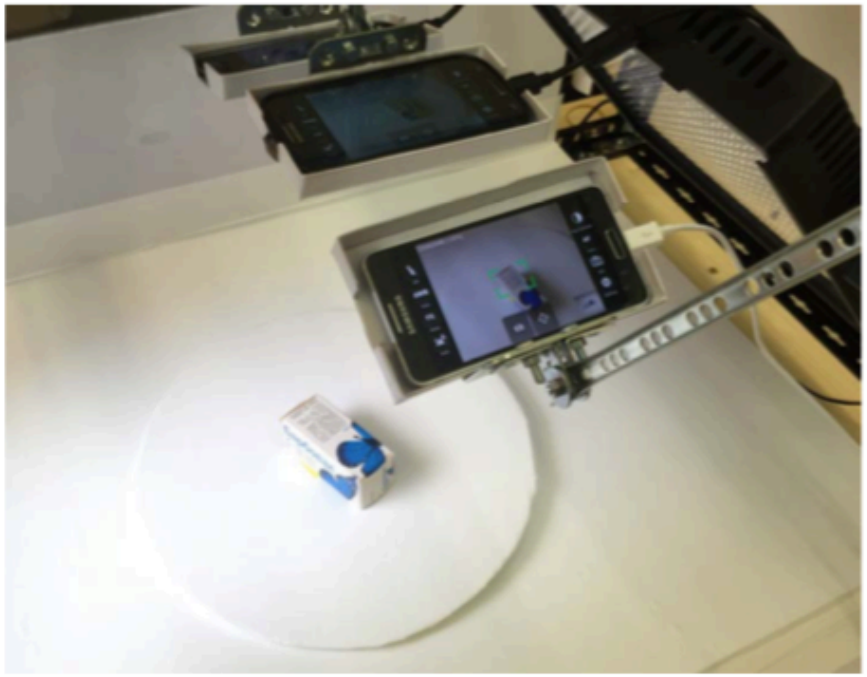
3.1. Stage 1: object recognition

Main specs to object recognition:

- Mobile phones
- Very accurate
- Fast and scalable to millions
- Invariant to observation conditions such as light, geometry, etc

Experimental dataset

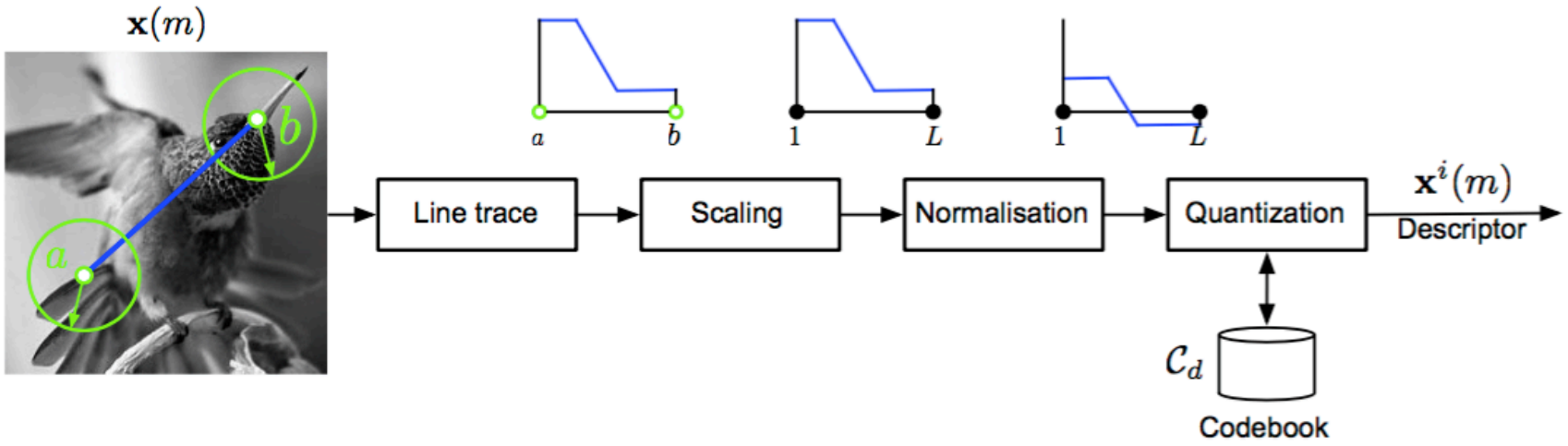
Enrollment system



3.1. Stage 1: object recognition (**universal SketchPrint descriptor**)

SketchPrint main idea

Extract a sketch connecting two reference points

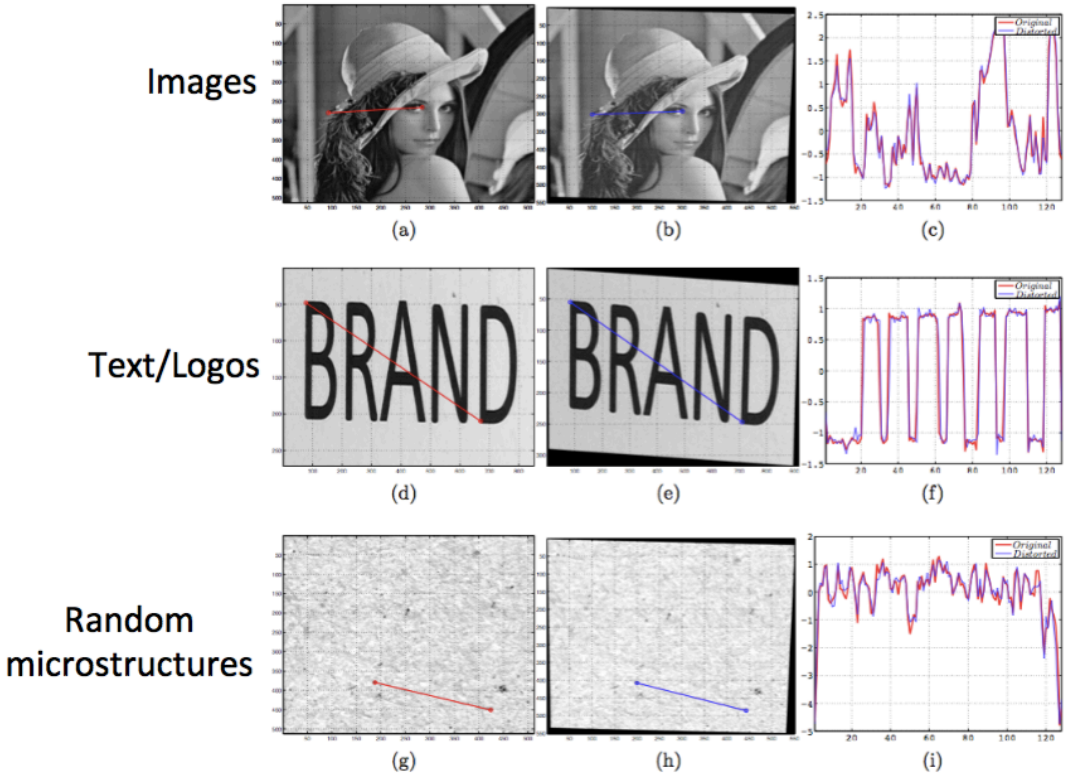


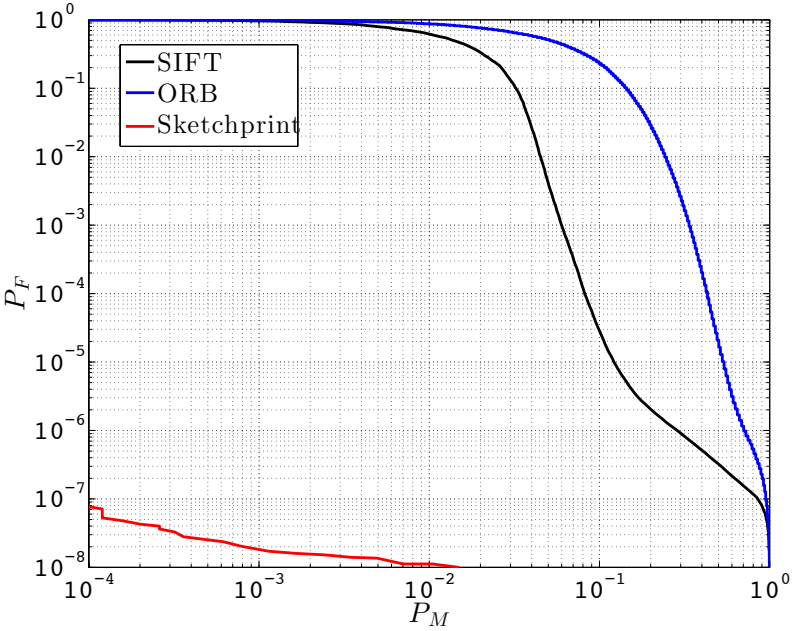
Main steps of SketchPrint:

- key-points detection
- SketchPrints extraction and filtering
- aggregation of many SketchPrint descriptors into one super-vector

3. Stage 1: object recognition (**universal SketchPrint descriptor**)

Performance and comparison to SOTA



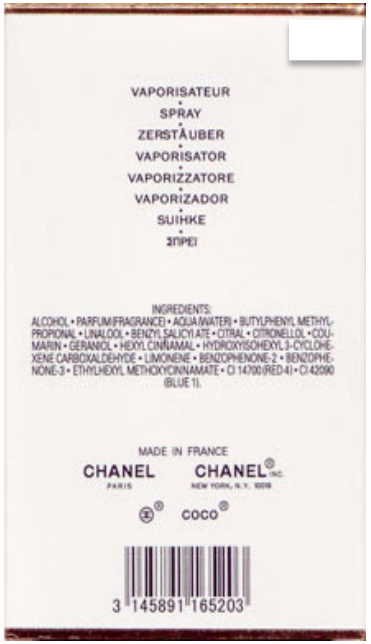


Remark

- SketchPrint considerably outperforms both SIFT and ORB
  - smaller number of descriptors per image $\Rightarrow$ less memory

3.2. Stage 2: design verification

Given: a package



Question:

- Is this package authentic?

Remark: you have never seen it or remember its design roughly…

Your thinking: well….quality of print looks OK

……logo seems OK

……..I buy it from a reputable vendor (incl web

……..**so probably authentic!**

3.2. Stage 2: design verification

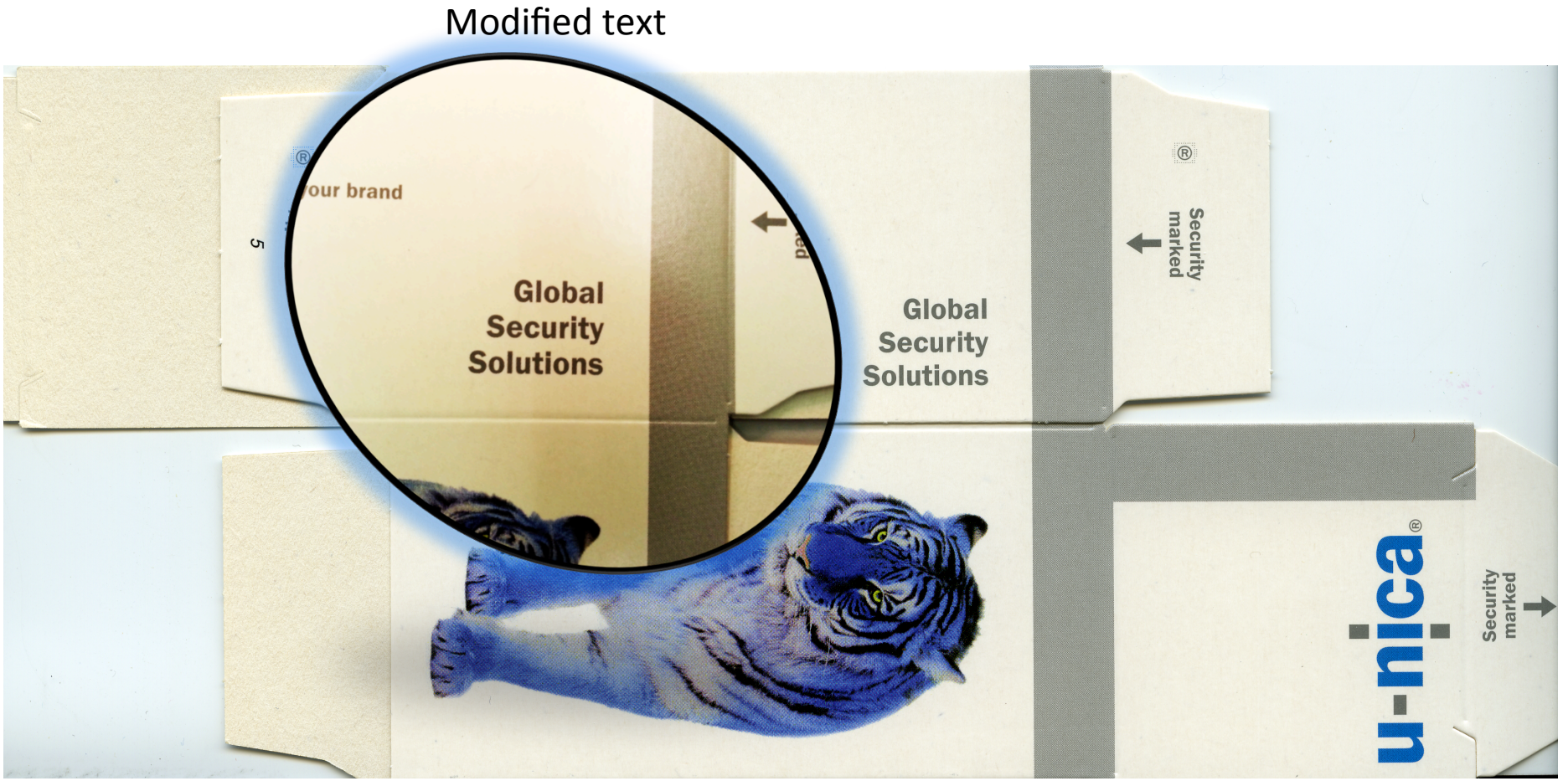
Observation: if we know the original design, we can easily verify its authenticity.

Question:

- Can we perform the design verification automatically?
- And how accurately (say with the precision about 10-15 microns)?

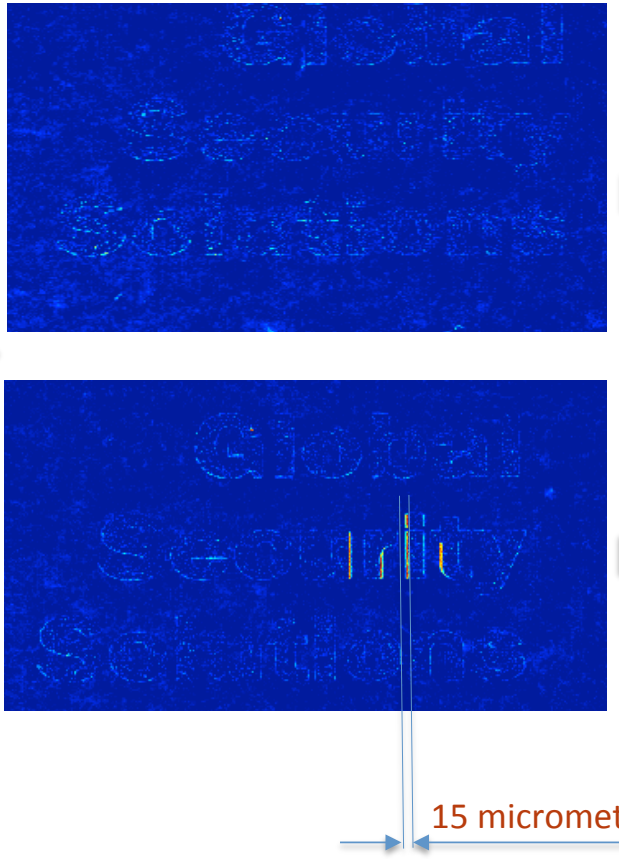
3.2. Stage 2: Automatic design verification on mobile phones

5’000 printed objects



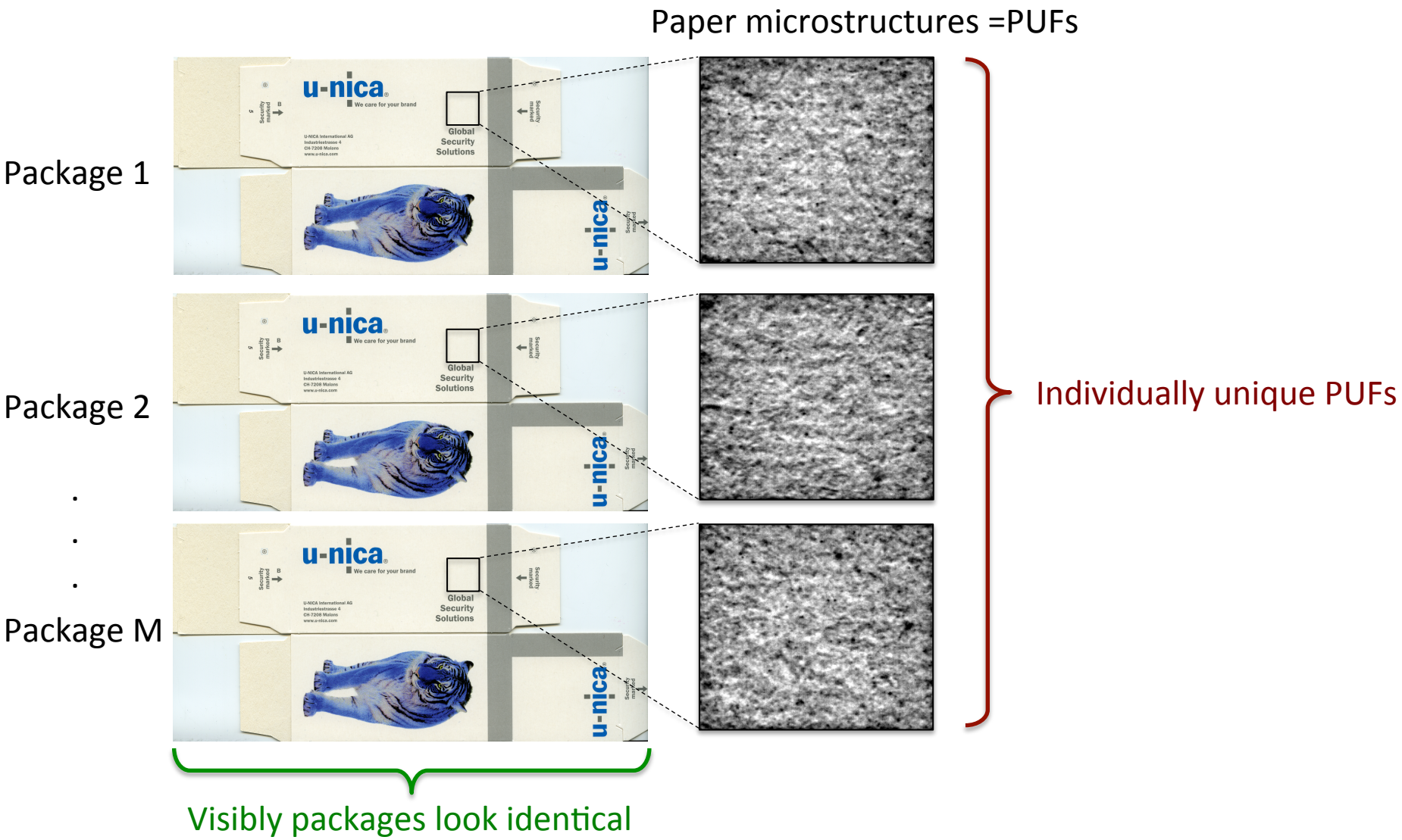
3.2. Stage 2: Automatic design verification on mobile phones

Text
Graphics
Images
Microstructures
Watches
Photos



3.3. Stage 3: individual object recognition

- **Question: can we differentiate** each individual object?

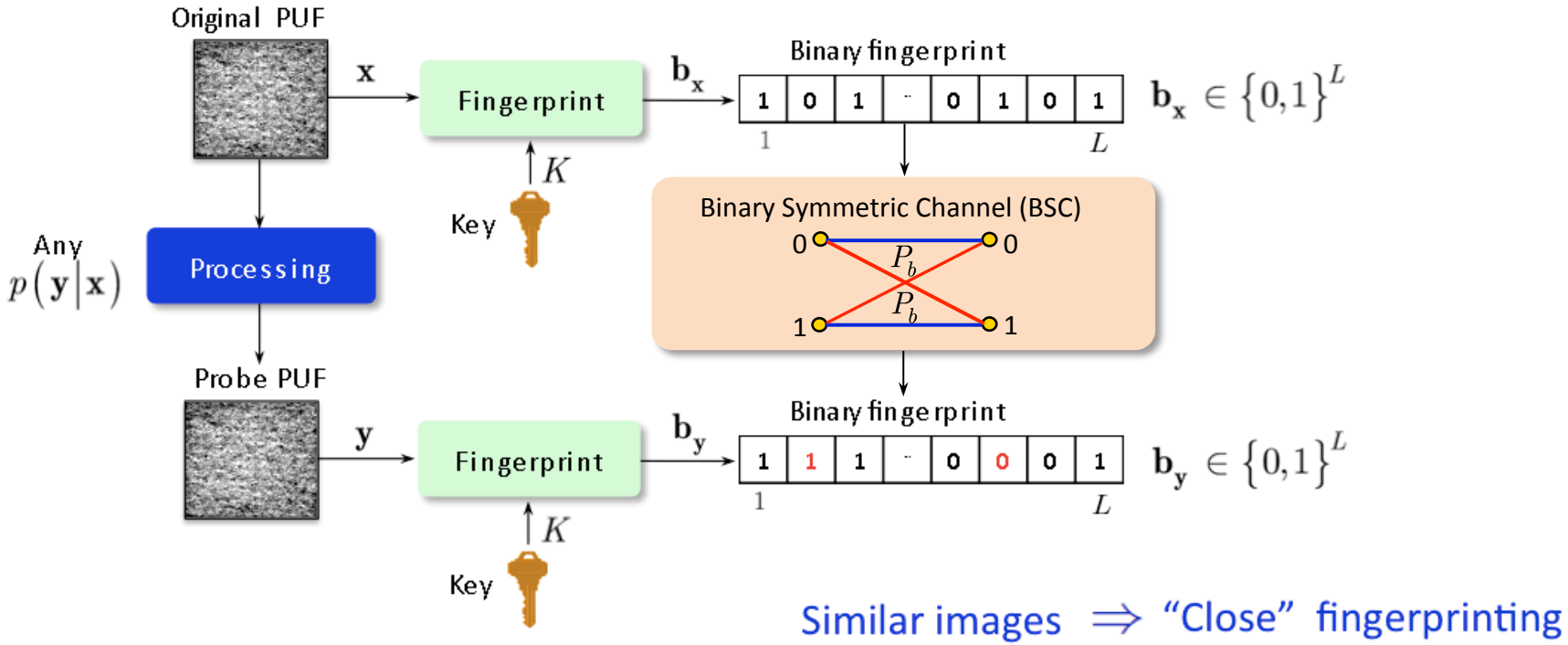


2. Stage 3: individual object recognition

- **Open issue: Big Data (millions of objects with high-dimensional features)**

Definition (Digital content fingerprinting)

Digital content fingerprinting *(a.k.a. robust perceptual hashing)* is a technique for computing a compact robust, secure and private binary representation of image.

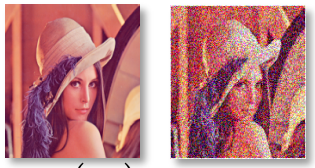


Similar images $\Rightarrow$ "Close" fingerprinting

3.3. Stage 3: individual object recognition

Properties

Correct acceptance



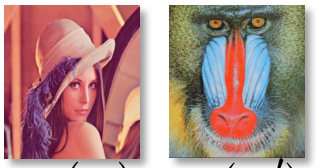
$\mathbf{x}(m)$ $\mathbf{y}$

$$\Pr\left[D^H(\mathbf{b}_\mathbf{u}(m), \mathbf{b}_\mathbf{y}) \leq \gamma L\right] \to 1$$

Binomial distribution

$$D^H(\mathbf{b}_\mathbf{u}(m), \mathbf{b}_\mathbf{y}) \sim B(L, P_b)$$

Correct rejection



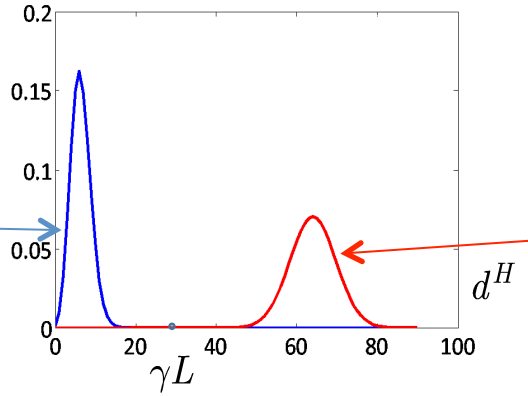
$\mathbf{x}(m)$ $\mathbf{x}(m')$

$$\Pr\left[D^H(\mathbf{b}_\mathbf{u}(m), \mathbf{b}_\mathbf{x}(m')) \leq \gamma L\right] \to 0$$

Binomial distribution

$$D^H(\mathbf{b}_\mathbf{u}(m), \mathbf{b}_\mathbf{y}) \sim B\left(L, \frac{1}{2}\right)$$

Hypothesis testing



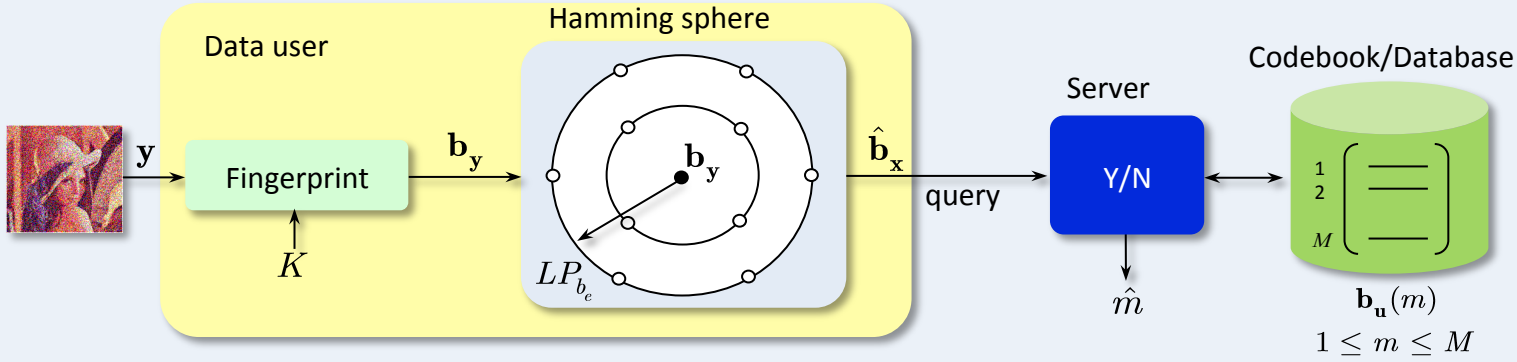
3.3. Stage 3: individual object recognition

- **Fast search**

Hamming sphere decoding

Observation: the most likely codewords $\mathbf{b}_{\mathbf{u}}(\hat{m})$ are within a Hamming sphere with radius γL around $\mathbf{b}_{\mathbf{y}}$.

Identification = codeword presence verification



4. Conclusion

- **Physical object security = multidisciplinary research field covering:**
  - Image processing
    - Computer vision
      - PUFs
        - Crypto
          - Big Data

- **Physical object security is of:**
  - great interest for industry and especially for the Swiss industry (protection of Swiss brands)
  - great significance for end users

- **Demos after presentation slot**