stochastic information processing

Multimedia Security and Privacy

S. Voloshynovskiy

Copyright notice

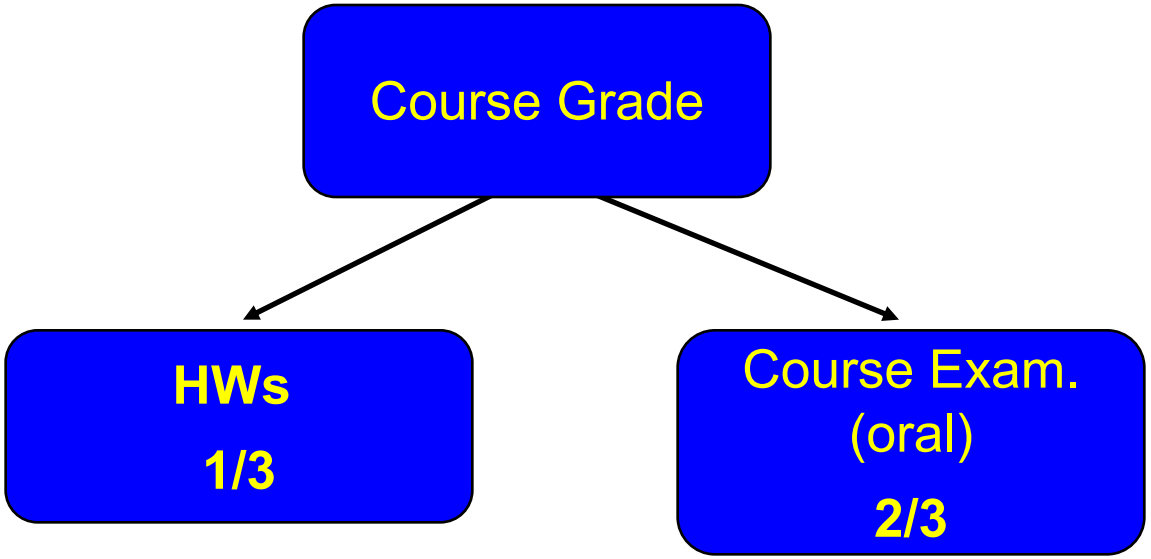
This course uses in part some materials from

- Book: I. Cox, M. Miller and J. Bloom, “Digital Watermarking: Principles and Practice”, *Morgan Kaufmann Publisher Inc.*, San Francisco, 2001;
- Book: M. Barni and F. Bartolini, “Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications”, *Marcel Dekker*, 2004;
- Book: M. Barni and F. Bartolini, “Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications”, *Marcel Dekker*, 2004;
- Book: J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 2009

And some papers, books, presentations that will be indicated along the course.

Grading Policy

The final grade will be determined based on laboratories and a final examination.



Notations

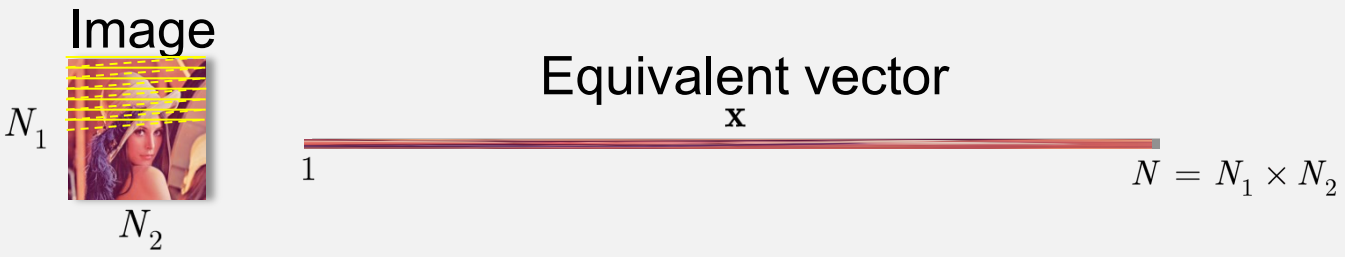
Notations

X Random variable with some distribution $p(x)$

$\mathbf{X}$ Random vector of length N: $\mathbf{X} = \{X_1, X_2, \cdots, X_N\}$

x Realization of random variable

$\mathbf{x}$ Realization of random vector $\mathbf{x} = \{x_1, x_2, \cdots, x_N\}$



Notations

$$H \times W$$

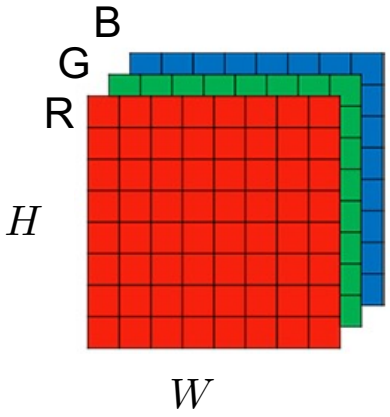
$$x_i \in \mathcal{X} = \{0, \cdots, 255\}$$

$$8\text{bits} : 2^8 = 256$$

Total size: $(H \times W) \times 256$

$$\begin{bmatrix} | \\ \mathbf{x} \\ | \end{bmatrix}_{N = H \times W}$$

Notations



$x_i^{R,G,B} \in \mathcal{X} = \{0, \cdots, 255\}$

Total size: $(H \times W) \times 3 \times 256$

Notations

108 Mpx

12 Mpx

Motivation

What is a modern image? Why is it interesting to consider it?

Value: copyright, NFT

Interface between the physical and digital worlds: a link between physical assets and digital tokens

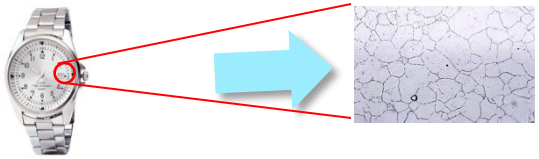
- Any physical object
- Human (biometrics)

As a container of information in forms of :

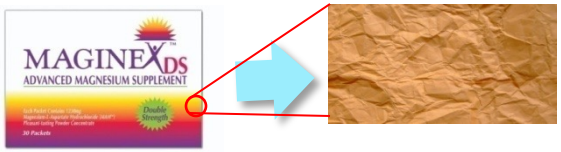
- Digital invisible watermark – copyright protection
- Steganography – hidden/secret communications in multimdeia data
- Tamper proofing – detection of modifications/alterations in data

Applications and main concerns

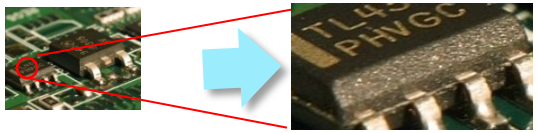
Physical Objects



Luxury products = “Annoying”



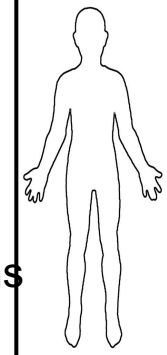
Medicine = “Dangerous”

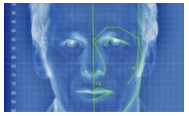


Electronics = “Security as whole”

concerns

Humans





Digital Content

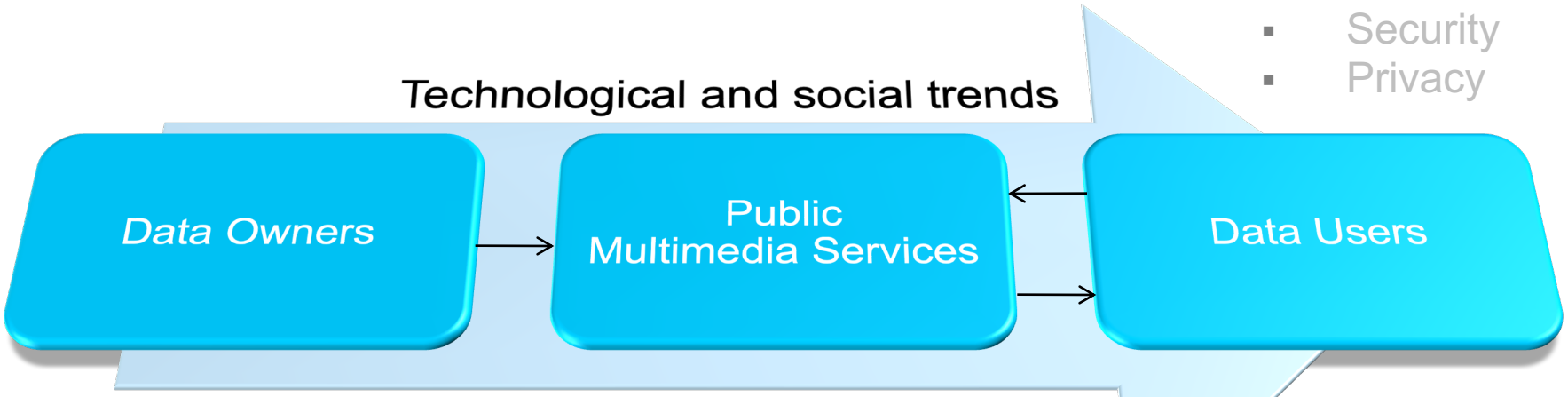
Images Videos Audios Text docs

Online sharing services

Main concerns

- Identification: identity, authenticity, origin, ownership, …
- Tracking and tracing
- Automatic tagging

Modern networked multimedia applications



Concerns
- Security
- Privacy

Private data
- Multimedia (MM)
- Medical data
- Biometrics …

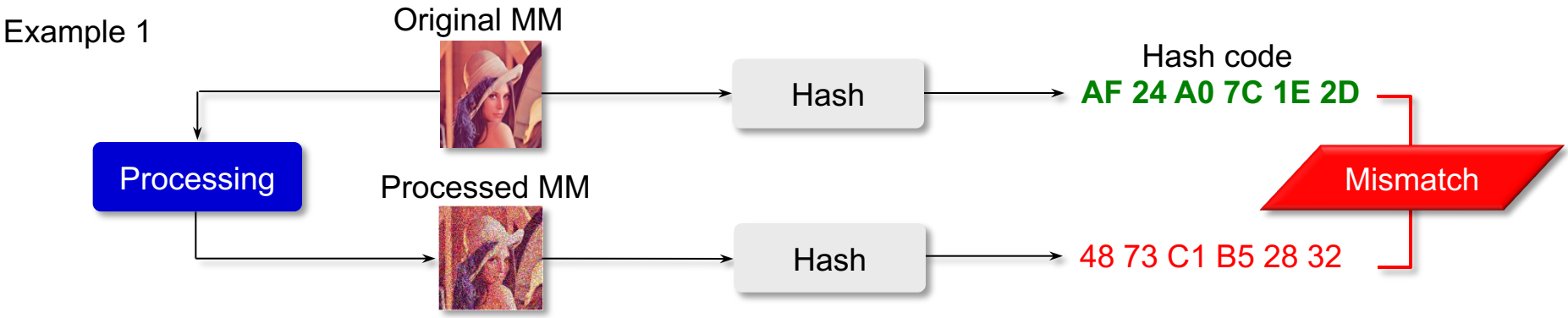
Untrusted intermediaries
- Search engines
- File sharing systems
- Social sites …

Tasks
- Search
- Identification
- Authentication
- Classification
- Mining …

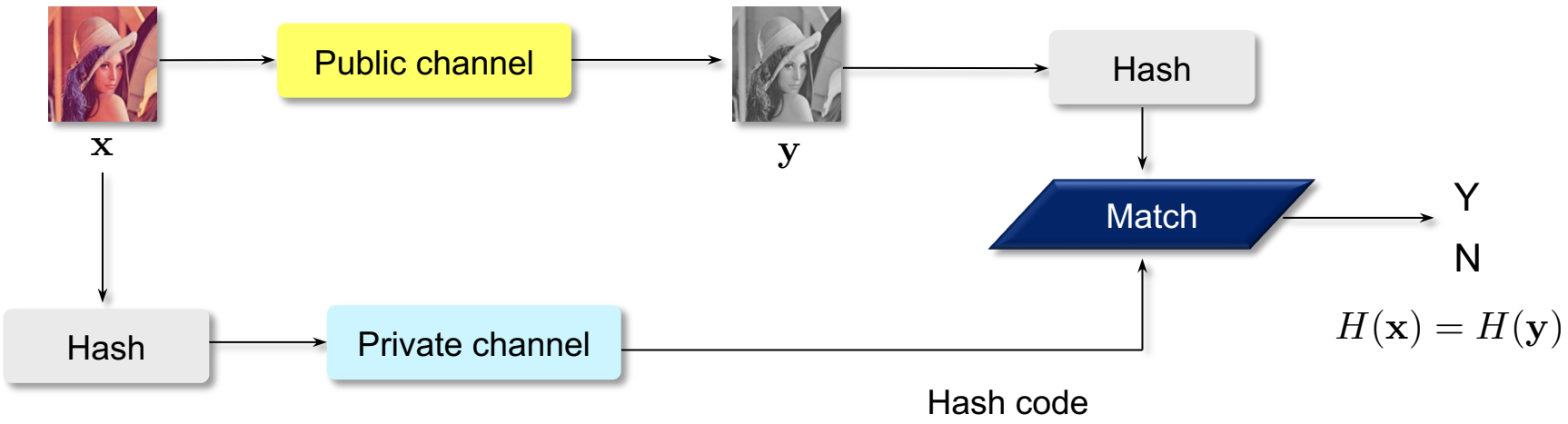
Multimedia security

Why are traditional security tools not suitable for multimedia?

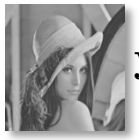
- Traditional *security*:
  - Cryptographic encryption (confidentiality of information)
  - Cryptographic hashes (authentication, trust, access control)
- Main concerns of classical crypto-based algorithms:
  - Sensitivity to noise and unintentional distortions in input data
  - Data handling in the encrypted domain



Practical implementation

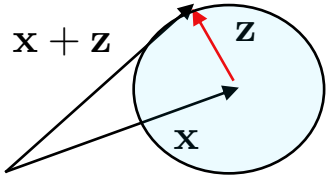


Multimedia security



$$\mathbf{y} = \mathbf{x} + \mathbf{z}$$

$$\mathbf{y} = \mathbf{x} + \mathbf{z}$$

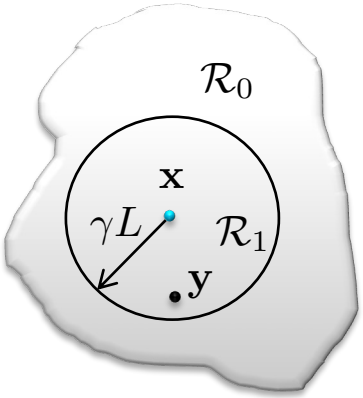


Crypto-hashes

Fingerprtining

$$\mathbf{x} = \mathbf{y}$$

$$H(\mathbf{x}) = H(\mathbf{y})$$



Decision region

$$||\mathbf{y} - \mathbf{x}||_2^2 = 0$$

$$||\mathbf{y} - \mathbf{x}||_2^2 \leq \gamma L$$

Multimedia privacy

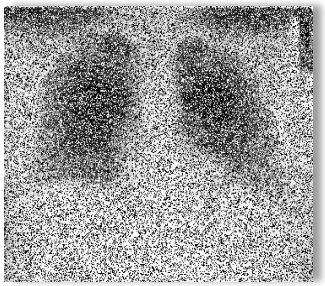
Why are traditional privacy tools not suitable for multimedia?

- Traditional *privacy protection*:
  - Data owner (protect data): based on data degradation and randomization (noise addition, lossy compression, data removal, dimensionality reduction…)
  - Data user (protect requests): based on anonymization, randomized rules
- Main concerns of classical privacy preserving algorithms:
  - Reduction of accuracy (data utility)
  - Not very efficient against experienced attackers (sensitivity analysis)

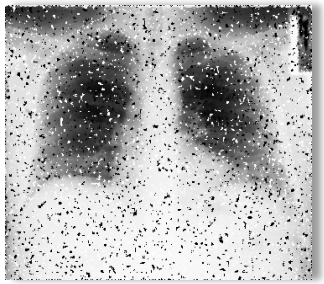
Example 2:

Original

50% removed based on key

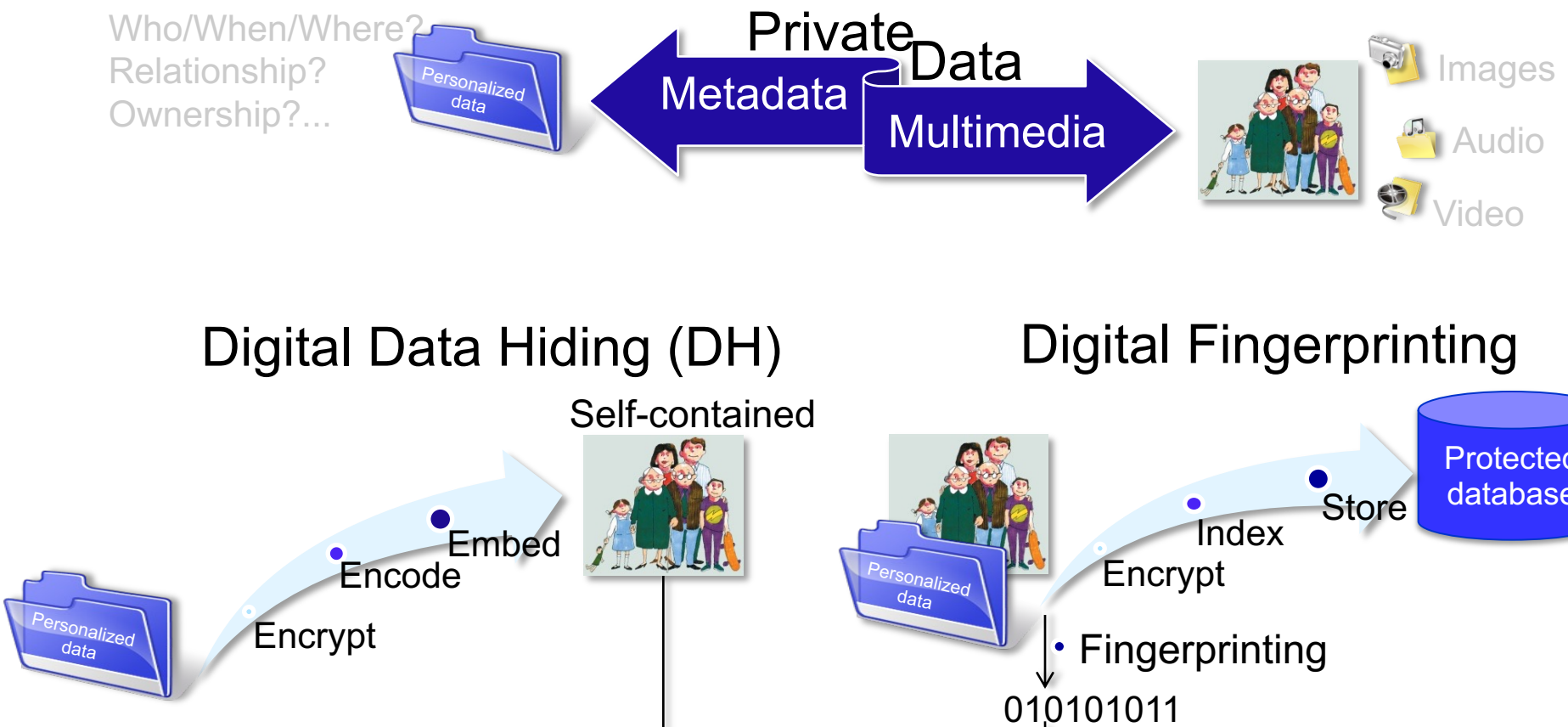


Median 9x9



Adaptive recovery

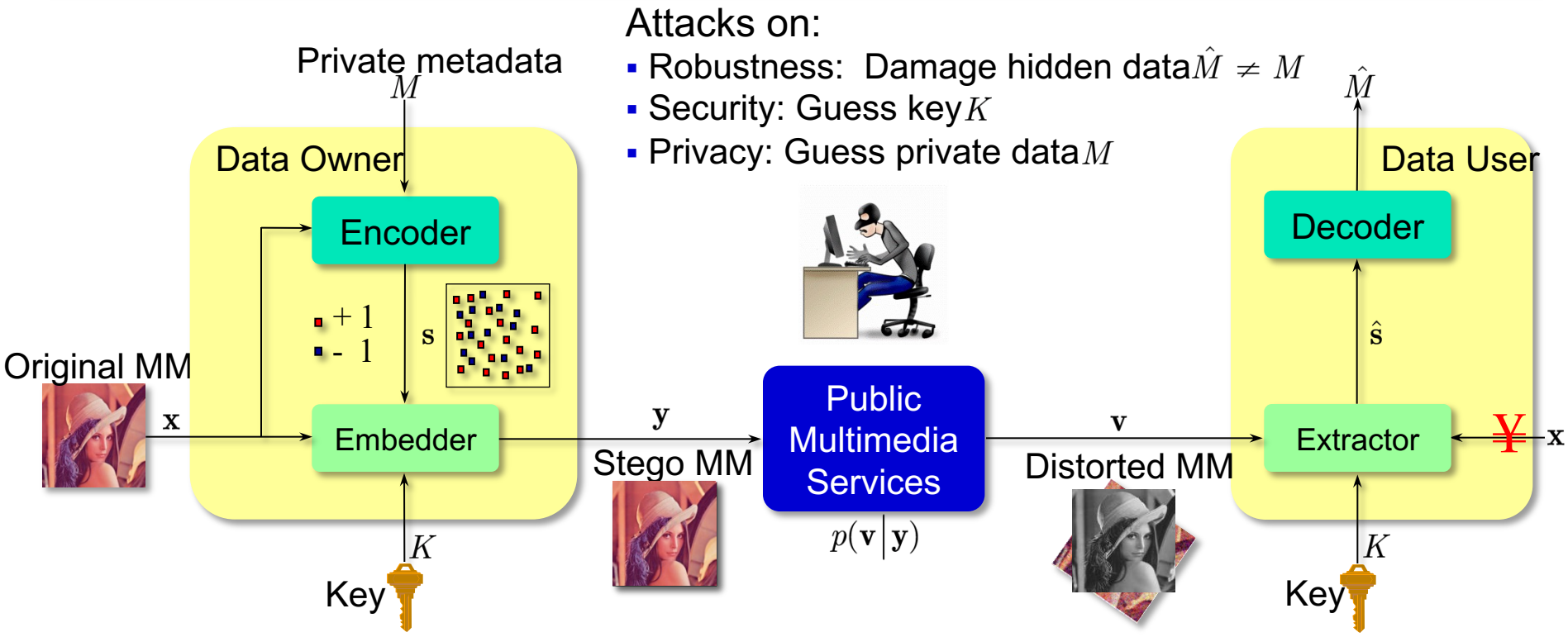
New tools for multimedia privacy and security



Digital data hiding: definition and concept

Definition (Digital data hiding)

Digital data hiding (*a.k.a. steganography*) is the art of perceptually and statistically undetectable robust information embedding in multimedia content.



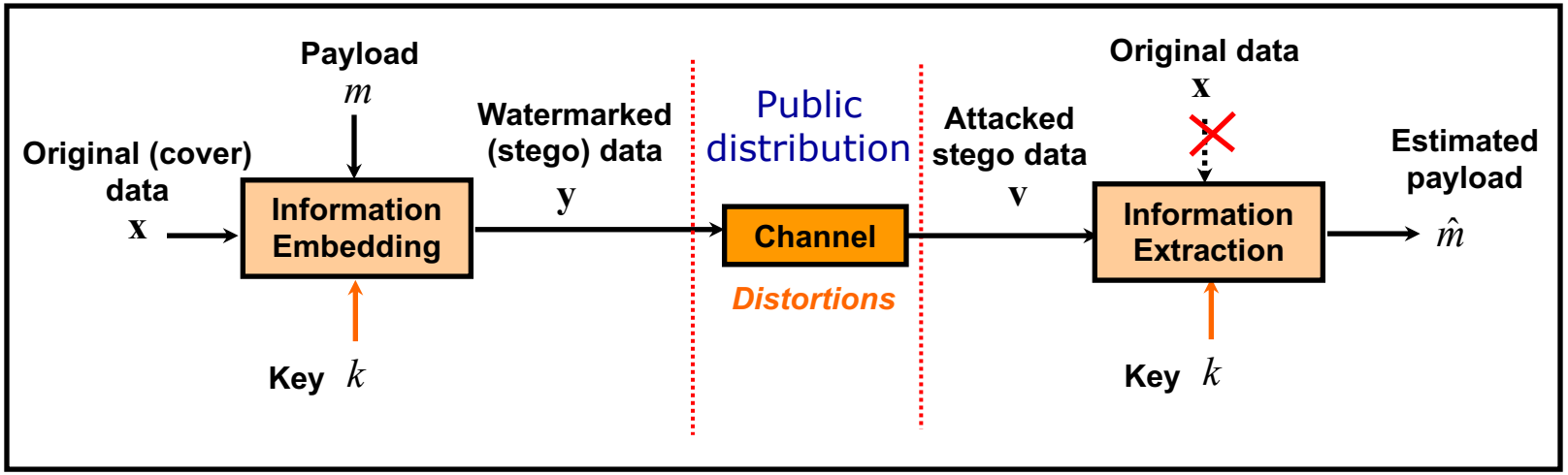
Digital data hiding: definition and concept

Types of digital watermarking

- Robust watermarking
- Steganography
- Tamper proofing

Digital data hiding: definition and concept

Robust watermarking

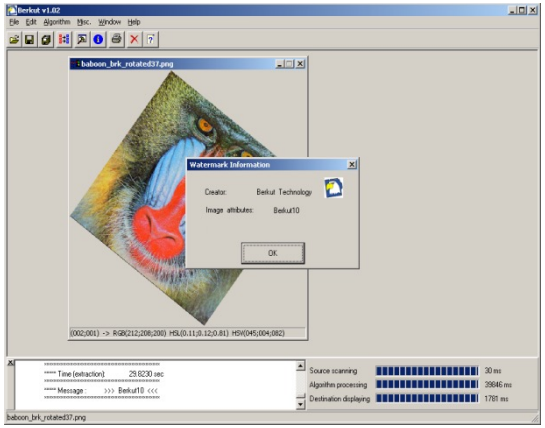


- Copyright protection: who is an owner of content
- Robustness: to ensure realible extraction of secret message
- Secure: to ensure inability to extract a seceret message or to estimate a secret key

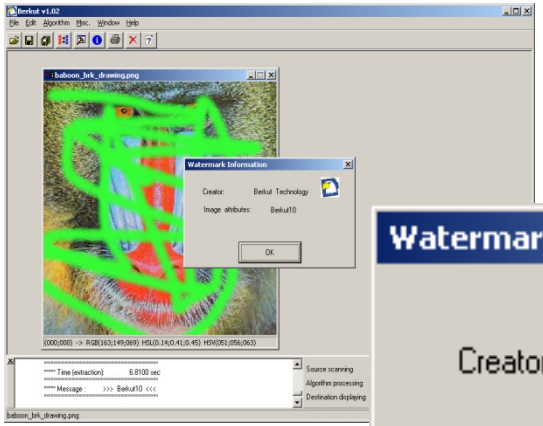
Typical message length: 64-128 bits/entire image in all 3 channels

Digital data hiding: definition and concept

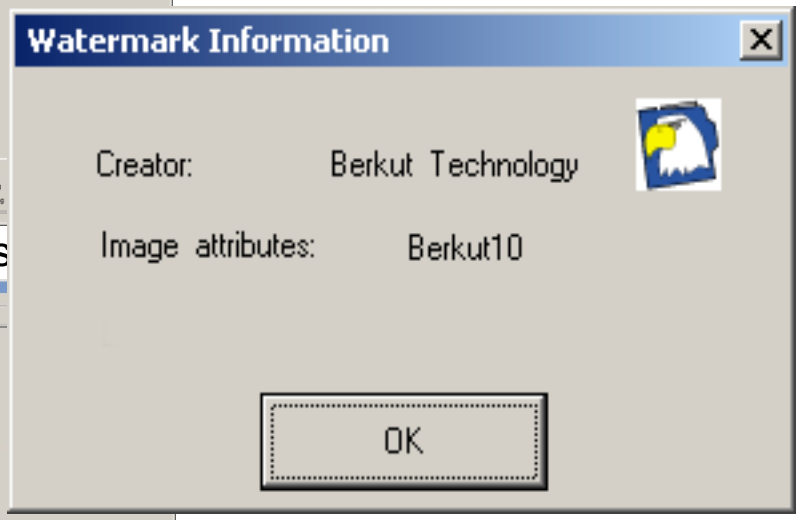
Robust watermarking

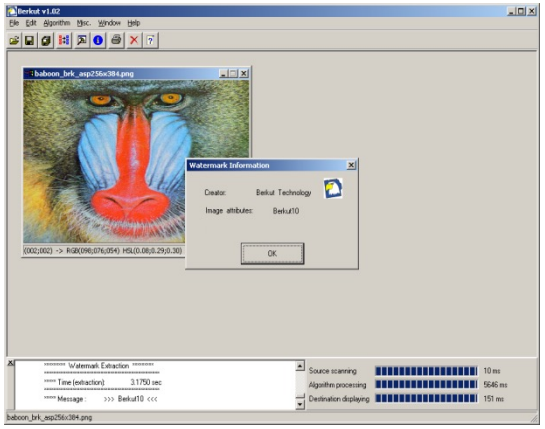


Rotation/shearing

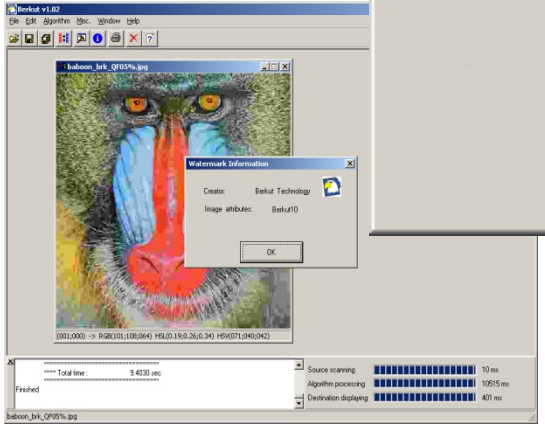


Drawing/erasures





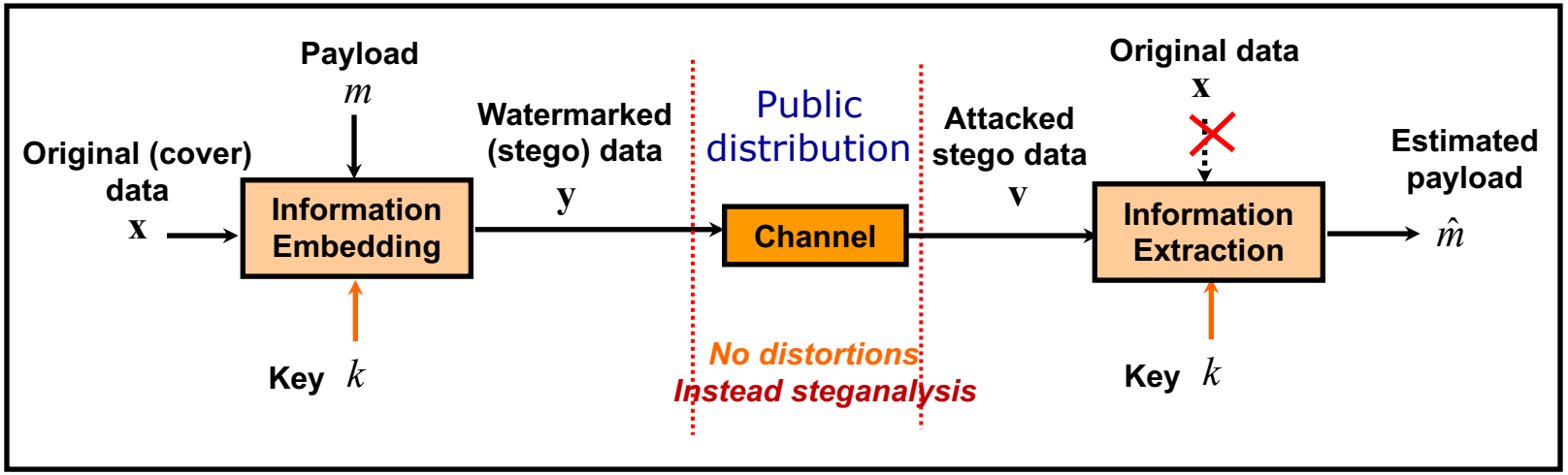
Scaling/aspect ratio



Lossy compression JPEG/JPEG2K

Digital data hiding: definition and concept

Steganography



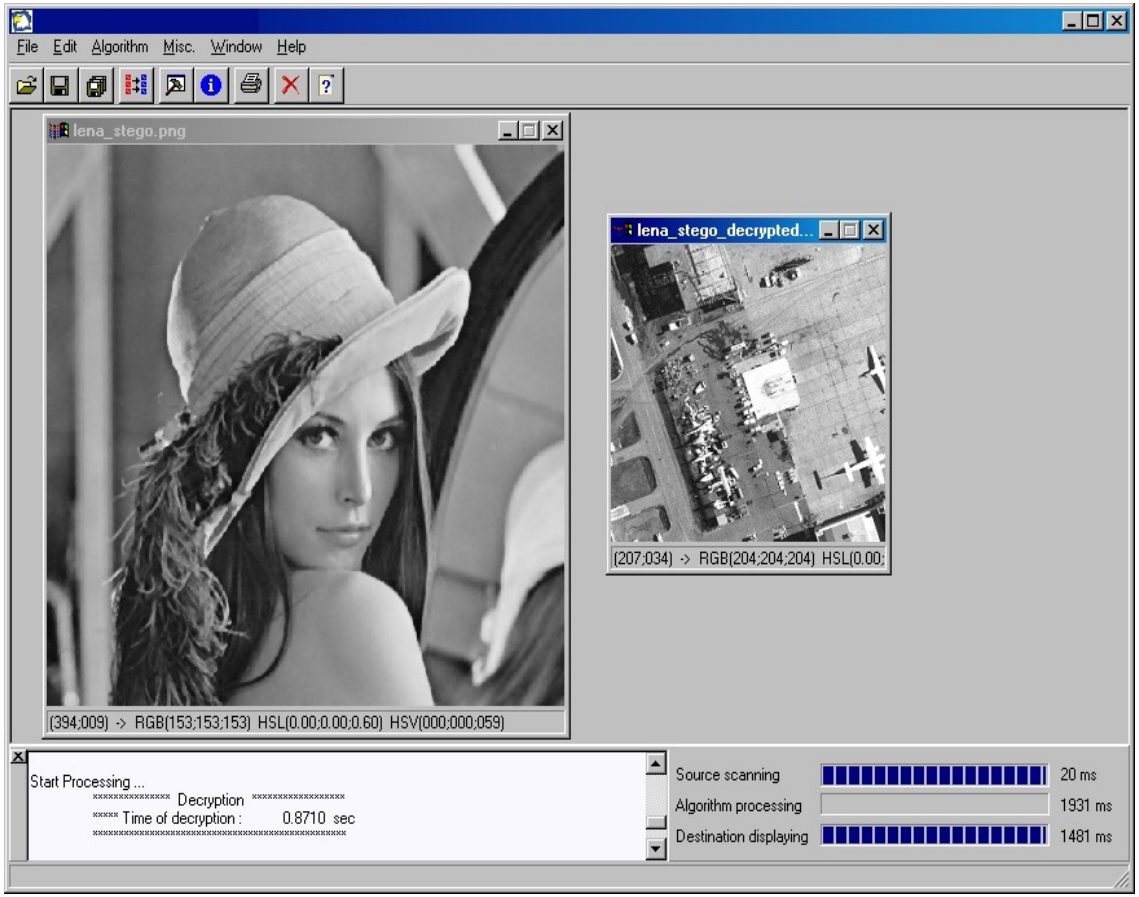
- Secret communications: to hide a fact of message communication
- Robustness: not nessary needed. Instead a fact of secret communication should stay secrtet as such
- Secure: to ensure inability to extract a seceret message or to estimate a secret key

Typical message length: Kbytes per entire image in all 3 channels;

can also be distributed over many images

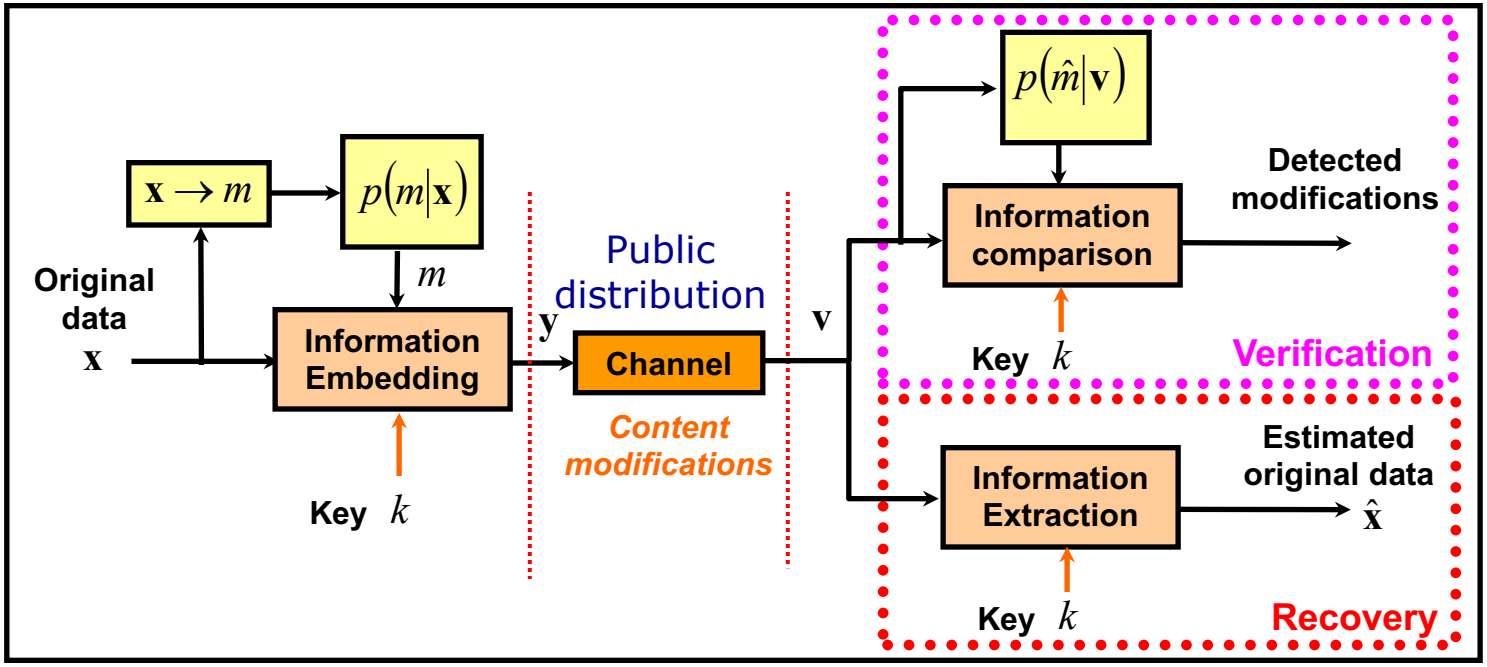
Digital data hiding: definition and concept

Steganography



Digital data hiding: definition and concept

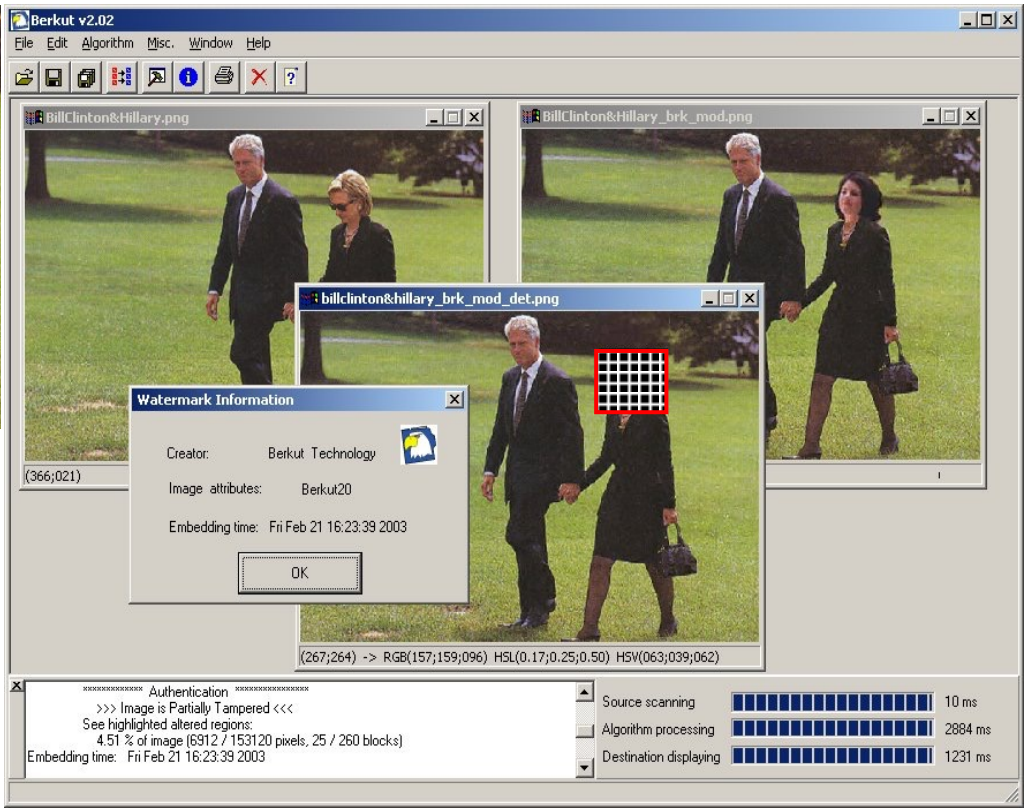
Tamper proofing



- Detect modification in data or localize them
- Robustness: to certain extend only (legitimate distortions)
- Secure: to ensure inability to extract a seceret message or to estimate a secret key

Digital data hiding: definition and concept

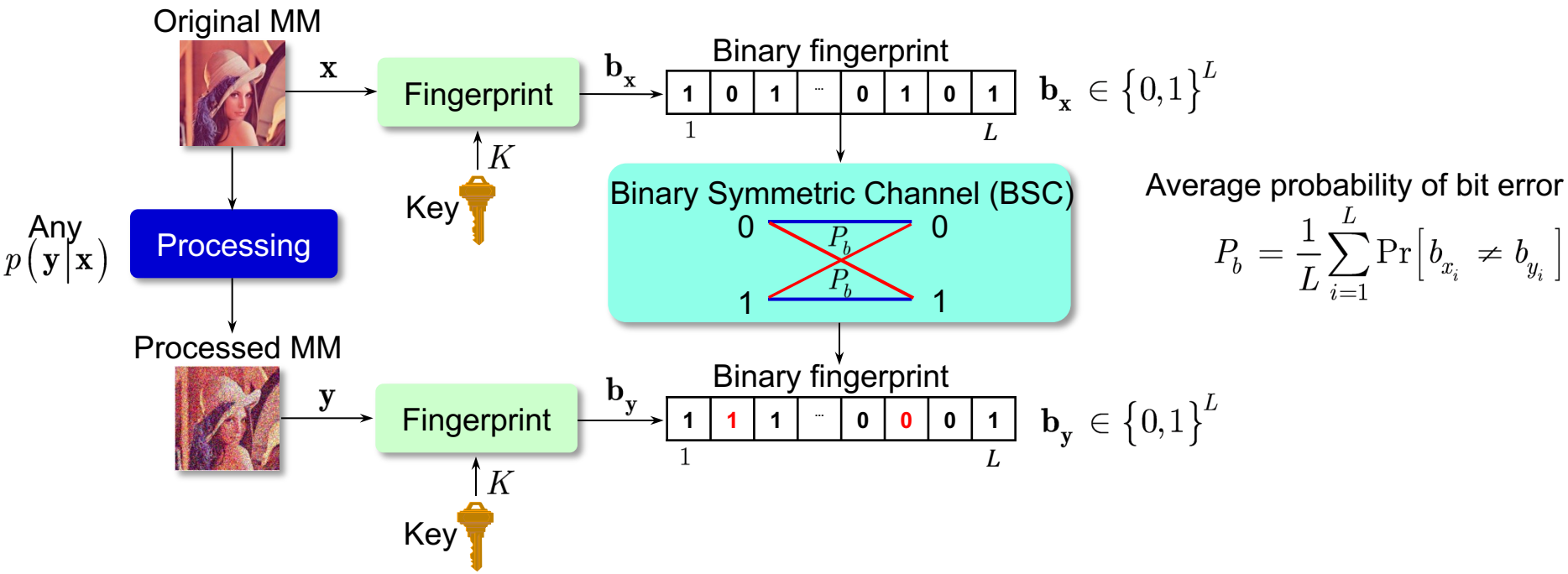
Tamper proofing



Digital fingerprinting: definition and concept

Definition (Digital fingerprinting)

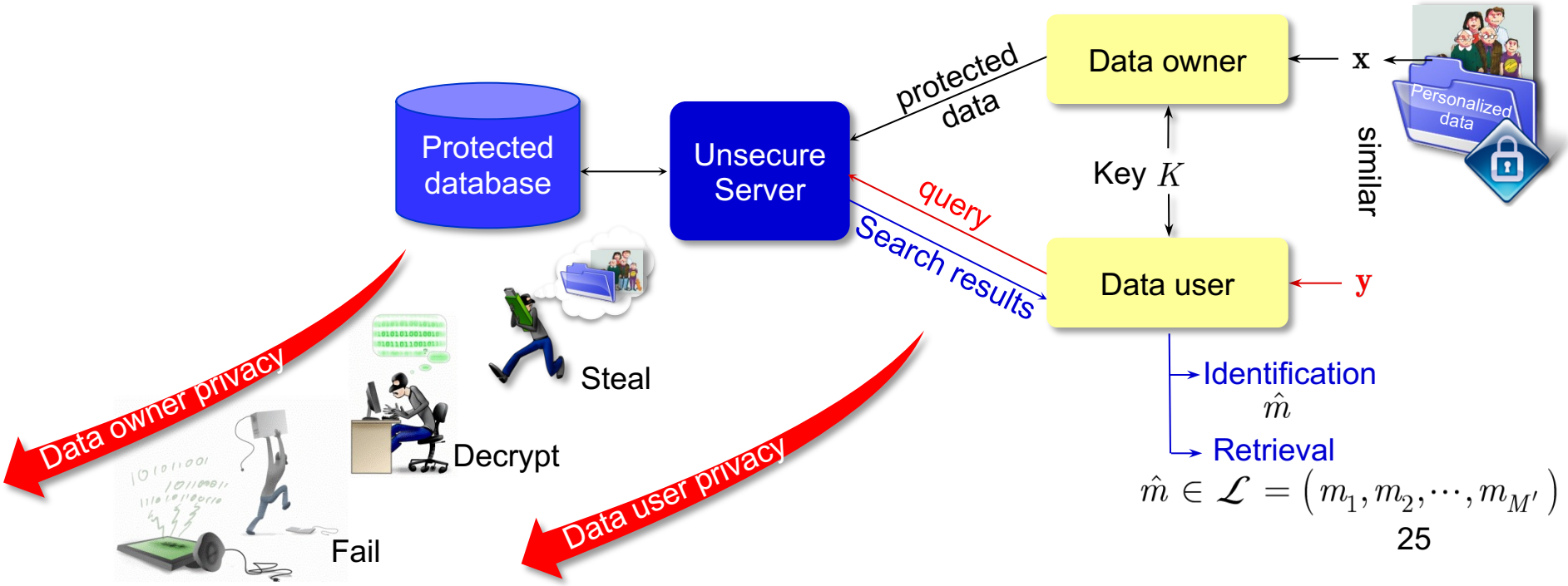
Digital fingerprinting *(a.k.a. robust perceptual hashing)* is a technique for computing a compact robust, secure and private binary representation of multimedia content.



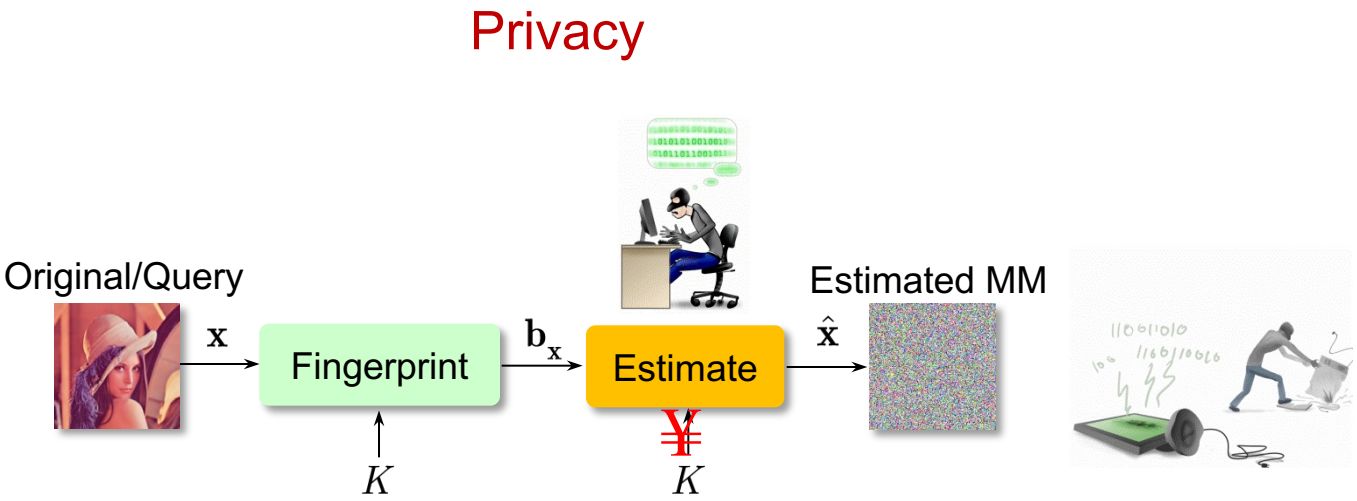
Privacy-preserving search: concept

Main concerns of privacy-preserving search in large-scale systems

- Exact queries and binary distributed hash tables in P2P systems (incl. LSH)
- Complexity:
  - Optimal Maximum Likelihood-based search is a NP-hard problem $\left(\mathcal{O}\left(2^L\right)\right)$
  - Cryptographic homomorphic encryption is computationally expensive

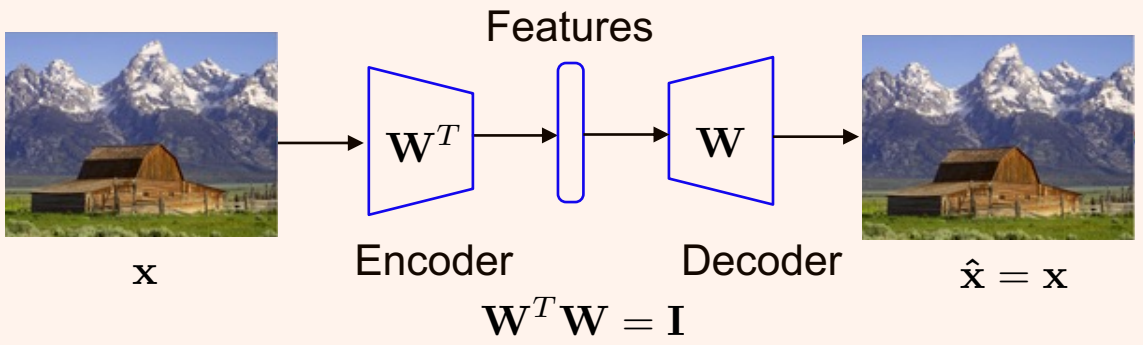


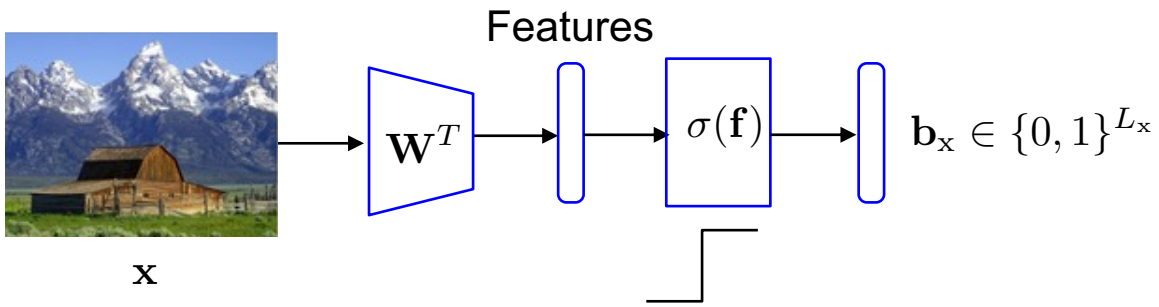
Privacy-preserving search: concept



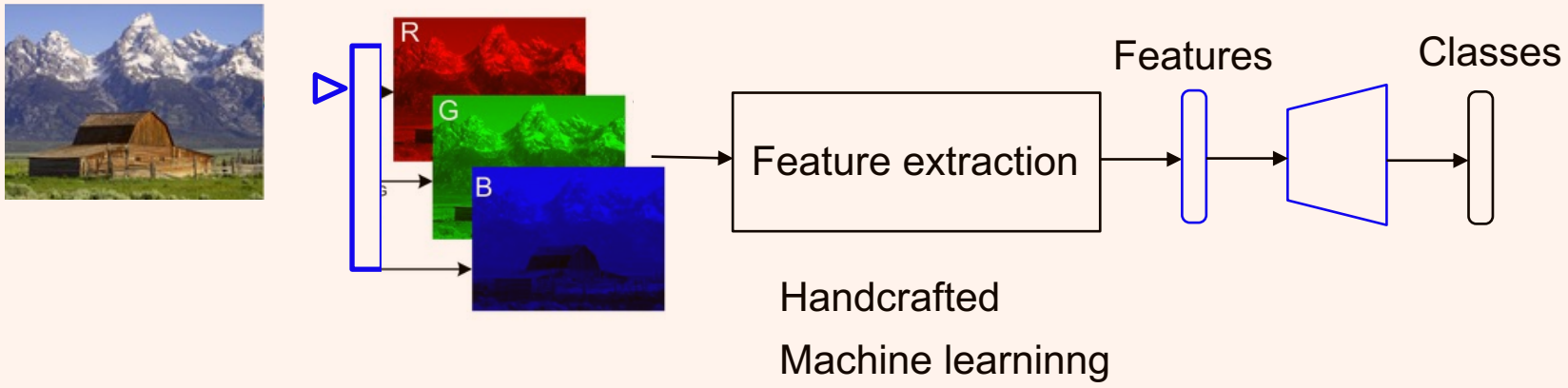
Multimedia security

Hand-crafted based fingerprtining





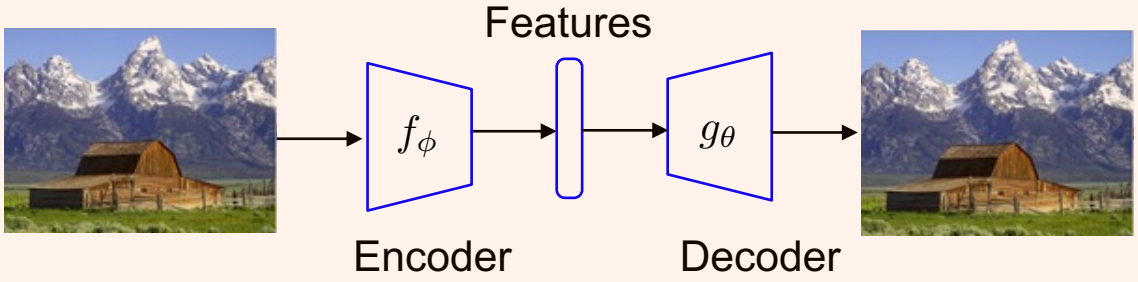
Multimedia security



ML based fingerprtining

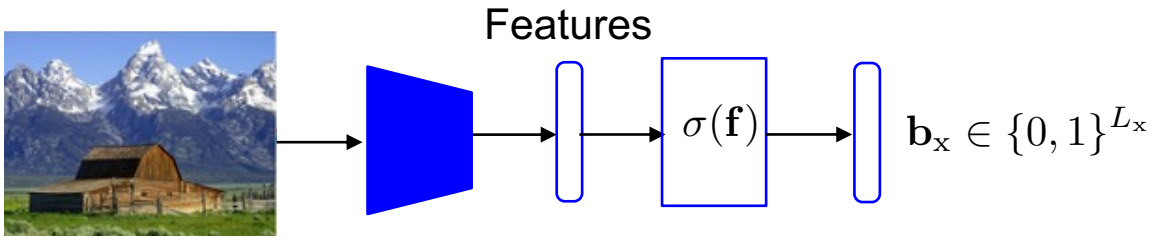
Features taken from auto-encoding

Training



$$f_\phi(\mathbf{x}) = \sigma_K(\mathbf{W}_K....(\sigma_1(\mathbf{W}_1\mathbf{x} + b_1) + b_K)) \qquad \phi = \{\mathbf{W}_K, ..., \mathbf{W}_K; b_1, ..., b_K)$$

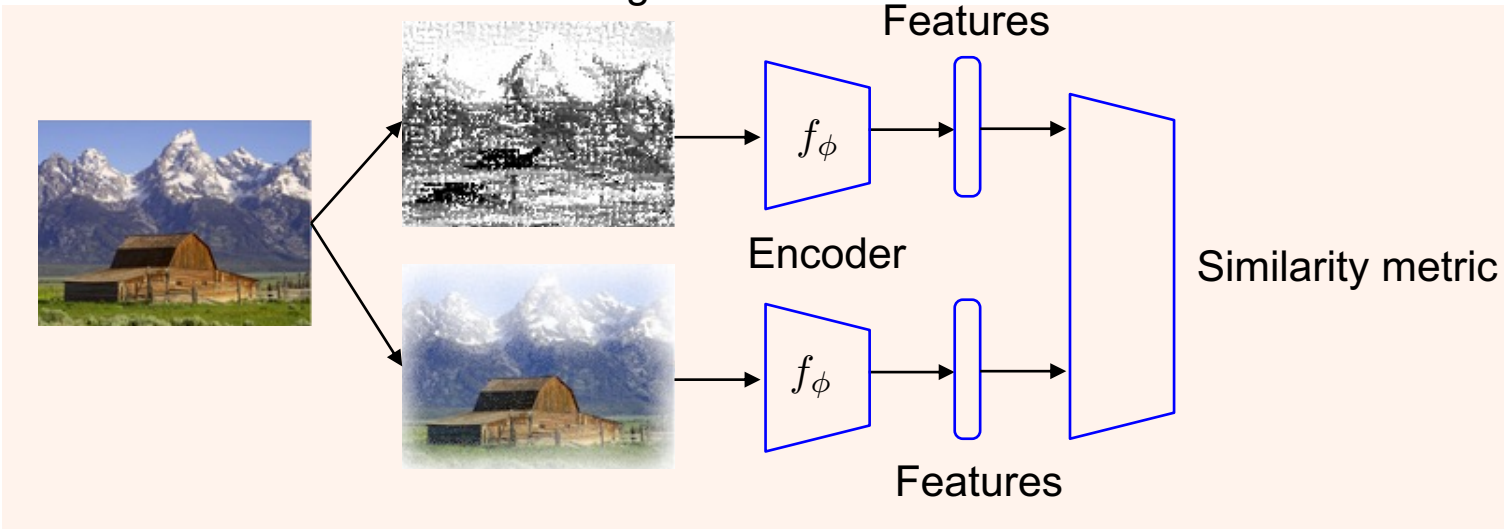
Embedding or feature extraction



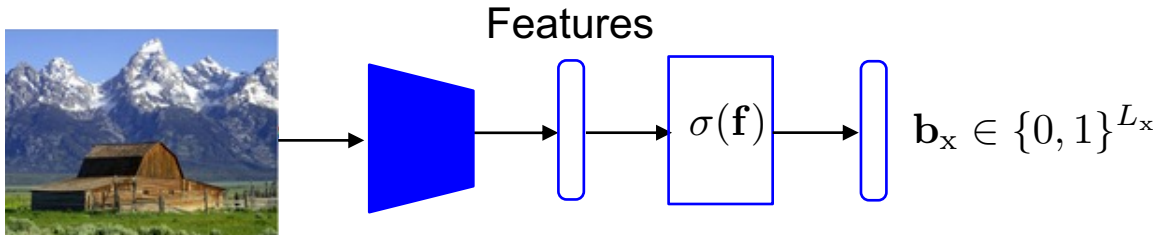
Multimedia security

ML based fingerprtining

Features taken from self-learning



Embedding or feature extraction



Course outline

- Digital watermarking
- Digital content fingerprinting
- Privacy protection

Extensions

- Physical world security
- Security based on smart phones

Applications and main concerns

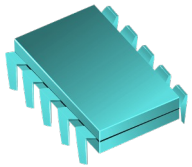
Protection of physical objects

ID docs

Certificates

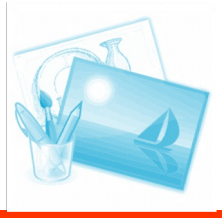
Banknotes

Electronics



Luxury objects

Art objects



Packaging

Risks of counterfeiting

- Danger for life
- Market loss
- Damage of brand reputation

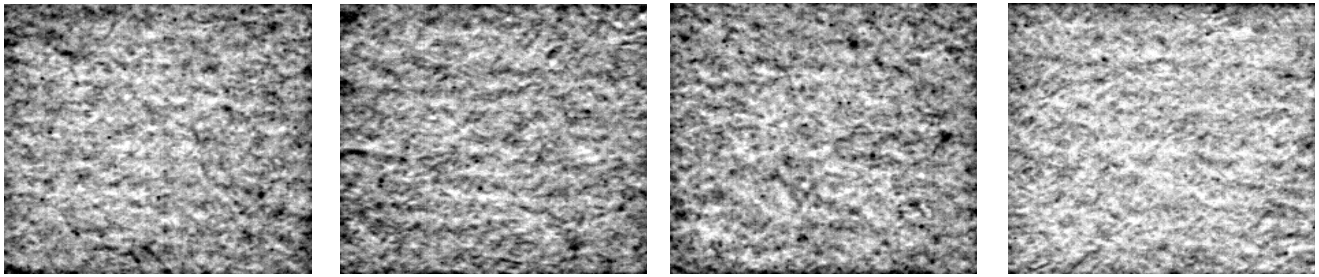
Restraints

- Inefficient authentication technologies
- High cost of track and trace infrastructure
- Lack of awareness for product originality

Protection of physical objects: natural randomness

Definition (Natural randomness)

Natural randomness represents unclonable features created by nature or some uncontrollable randomized process initiated by humans.



Features

- Easy to evaluate but is hard to characterize
- Structure is unique for each item
- Manufacturer not-reproducible

Protection of physical objects: natural randomness

Sample items with random surface structure (cardboard)

u-nica®

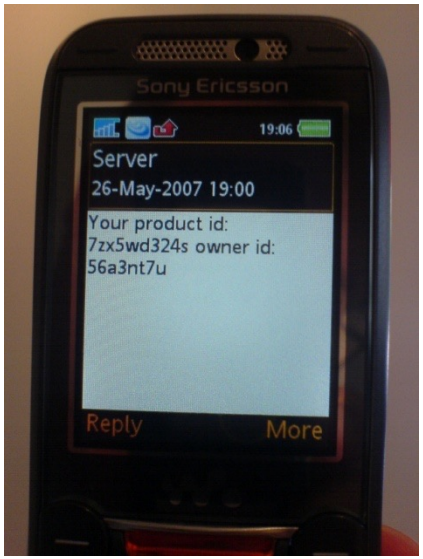
Global Security Solutions

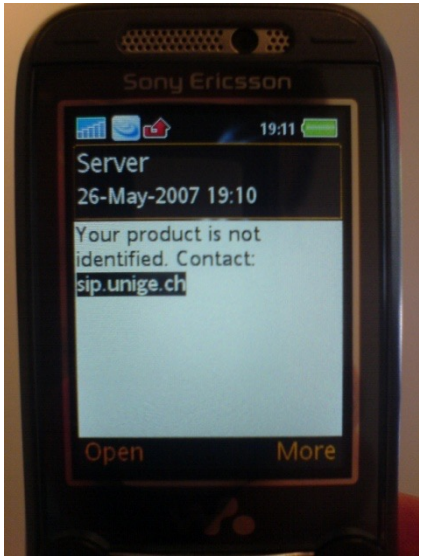
Item 1, unique surface features on every item

Item 2, unique surface features on every item

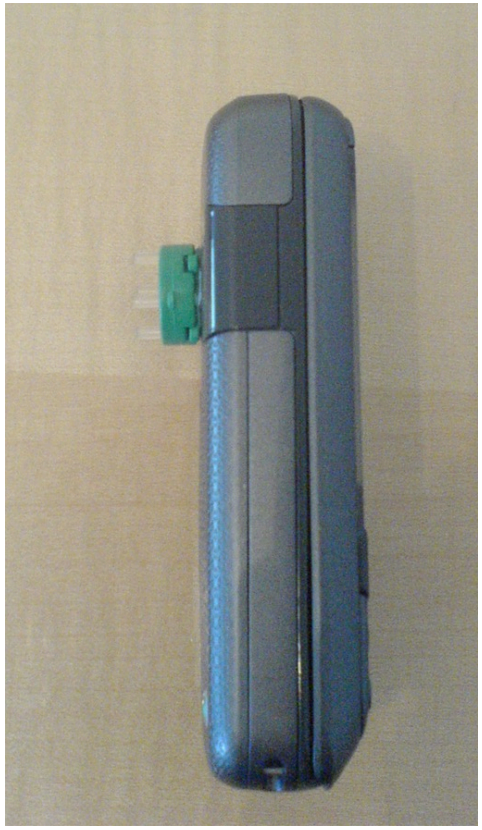
Verification on mobile phones

Watch identification





Verification on mobile phones



Applications and main concerns

Object recognition

Goal

Accurately recognize each object on mobile phone

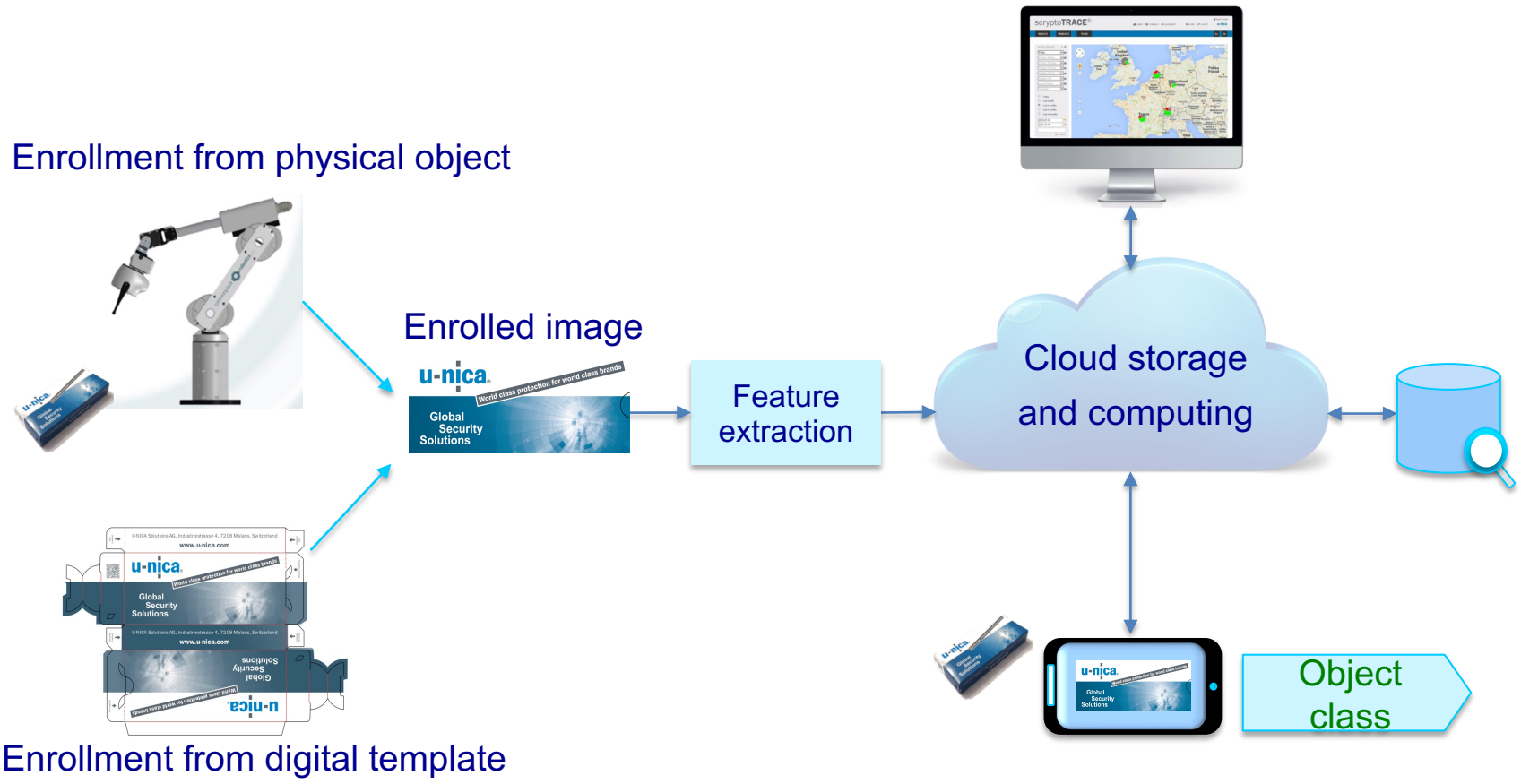
Object class

Challenges

- Billions of items
- Very similar

Applications and main concerns

Object recognition



Applications and main concerns

Object authentication

source: originalideas.info

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)?

Applications and main concerns

Object authentication

Integral verification

Text

Graphics

Images

Microstructures

Halftoning

Original

Authentic

High quality fake

Not authenti

15 micrometers

Applications and main concerns

Object identification

Paper microstructures =PUFs

Package 1

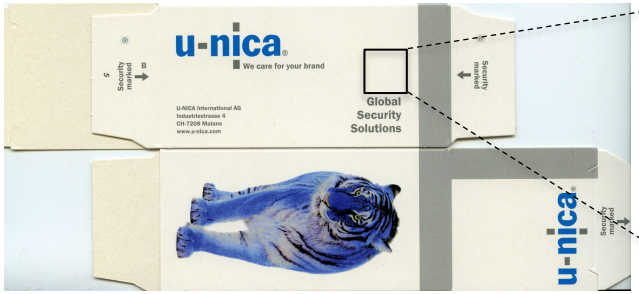
Package 2

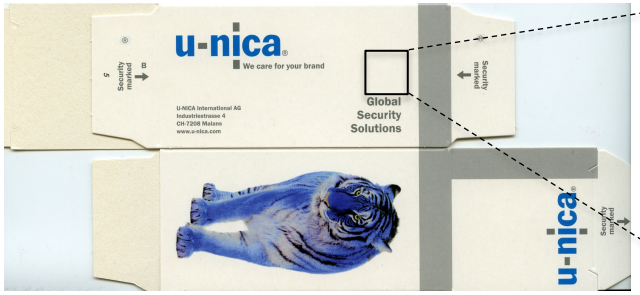
.

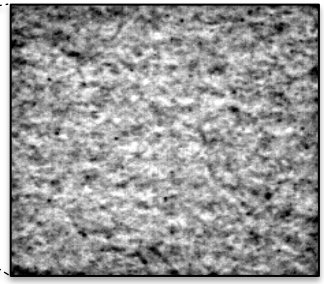
.

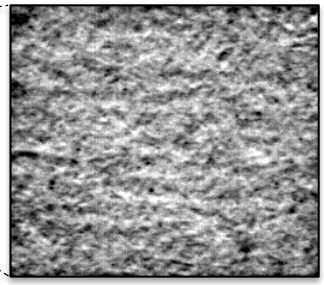
.

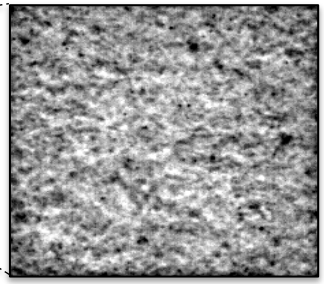
Package M











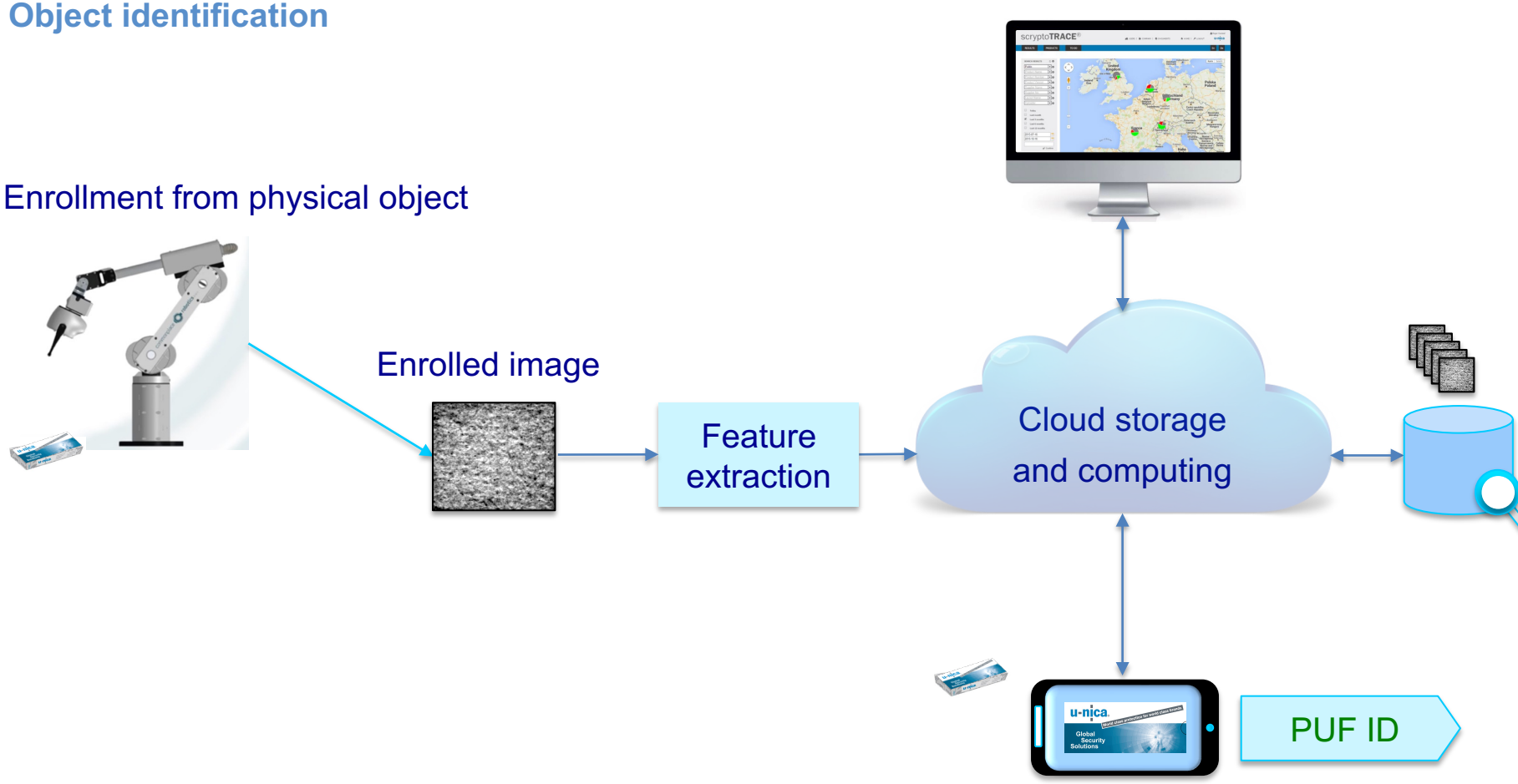
Individually unique PUFs

= unique identifier for Track&Trace

Visibly packages look identical

Applications and main concerns

Object identification

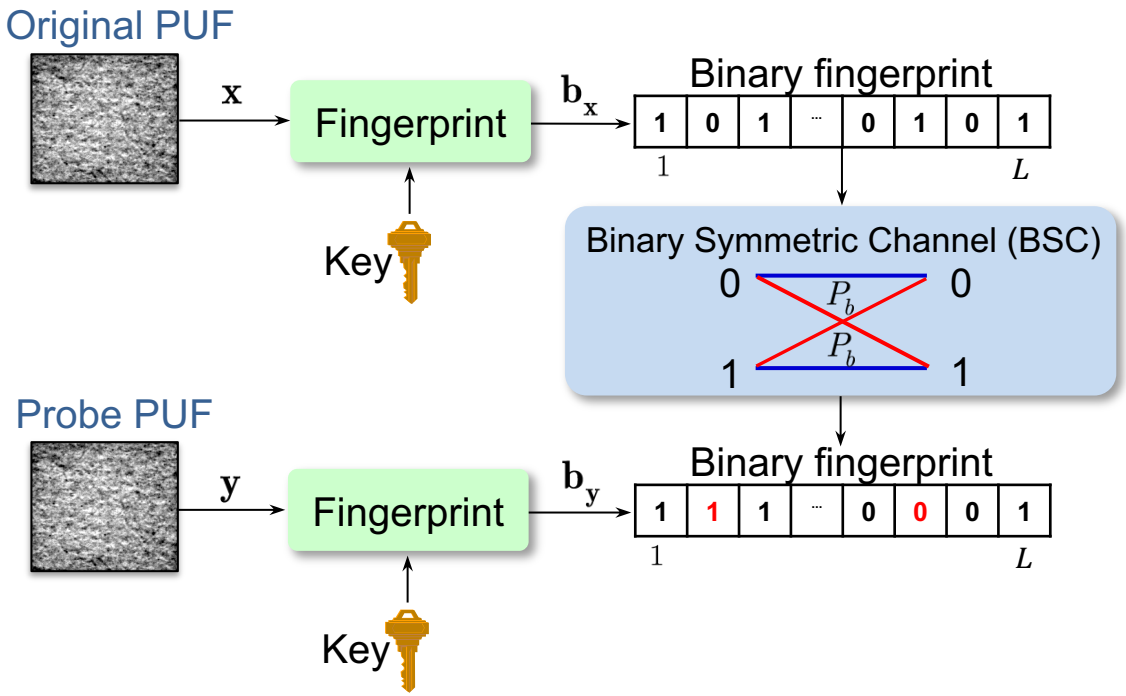


Applications and main concerns

Object identification

Open issue:

Big Data (millions of objects with high-dimensional features)

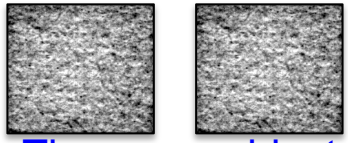


Applications and main concerns

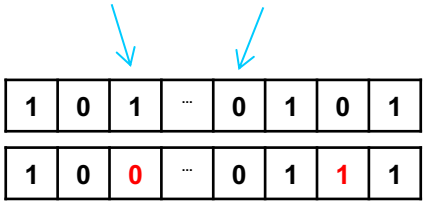
Object identification

Properties of PUFs: Close PUFs = close fingerprints

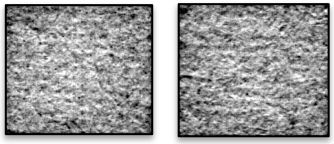
Correct acceptance



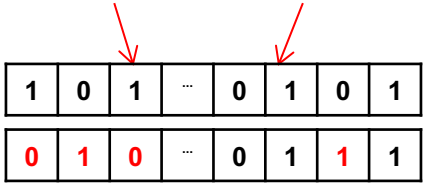
The same object



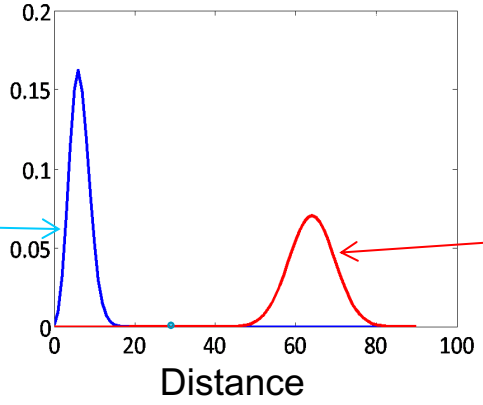
Correct rejection



Two different objects



Hypothesis testing



Applications and main concerns

Benefits

Recognize physical objects

Direct interaction with physical objects

Detect fake objects

Prevent end user consuming fake objects

Track market activity

Tracking goods, market trends and activity

Smartphone app

Public app not requiring any special training

Real-time reporting

Dynamic reporting and visual analytics

Mobile marketing

Consumer engagement and product promotion