

# Tomasz Grajek

## Multimedia Communications

### *Lecture slides*

## Poznań University of Technology

© Tomasz Grajek

These slides are intended as supplementary material for the lecture  
*Multimedia Communications*  
given by dr Tomasz Grajek  
for students of Electronics and Telecommunications  
at Poznan University of Technology.

Note: These slides contain copyrighted material.

Any copying, distribution, and non-authorized usage is strictly prohibited.  
*In particular, electronic distribution over Internet is prohibited*

# Steganography vs. cryptography

- **Steganography**

is the practice of **concealing** a file, message, image, or video within another file, message, image, or video.

Concealing:

- the fact that a secret message is being sent, and
- the contents of the message

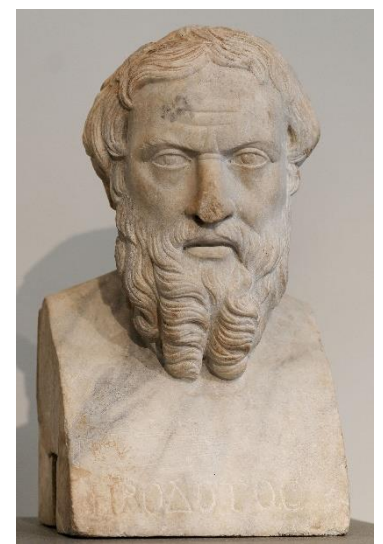
- **Cryptography**

is the practice of protecting the contents of a **message alone**.

# Ancient steganography

- **Herodotus (485 – 525 BC)**

is the first Greek historian. His great work, *The Histories*, is the story of the war between huge Persian empire and the much smaller Greek city-states.



Herodotus recounts the story of **Histaiaeus**, who wanted to encourage **Aristagoras of Miletus** to revolt against the Persian king.

In order to securely convey his plan, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to regrow.

The messenger, apparently carrying nothing contentious, could travel freely. Arriving at his destination, he shaved his head and pointed it at the recipient.

# Conventional watermarking - example

- Patterns in currency notes which are visible only when the note is held to light.



# Digital watermarking

- A **digital watermark** is a kind of **marker** covertly embedded in a noise-tolerant signal such as an audio, video or image data.
- **Watermarking** is the process of hiding digital information in a carrier signal.
- The hidden information should, but does not need to, contain a **relation to the carrier signal**.
- Digital watermarks may be used **to verify the authenticity or integrity** of the carrier signal or **to show the identity** of its owners. It is prominently used for tracing copyright infringements and for banknote authentication.

# Digital watermark

- **Visible**

The watermark remains visible  
(can be easily localized)  
in the signal in which it was embedded.



Jak odpowiadać na trudne pytania, czyli meandry rozmowy kwalifikacyjnej.

Pełni energii (i nerwów), pachnący i czysty i zapotrzebowania wszelkie niezbędne informacje o firmie w której chcemy pracować udajemy się w miejsce kadri, zwane popularnie gabinetem Szefa bądź rekrutera. Nie potknięcy się w progę, siadamy na wyznaczonym miejscu - zwierci i gotowi - oczekując zatrważającego grądu podchwytliwych pytań, którymi rekruter będzie próbował obnażyć naszą ignorancję, wyprowadzić nas z równowagi i doprowadzić do krótkiego

rozmyślenia - "czyż nie uczasz się?" - zakłamanie nerwowe.  
Pytanie rekrutera nie biera się - a przynajmniej nie powinno - z powietrza. Każde pytanie zadane kandydatowi ma na celu zdiagnozowanie konkretnych, wymaganej na danym stanowisku, kompetencji. Pytanie „Jaki Pan szuka pracy?” nie ma na celu sprawdzenia jak bardzo zdecydowany jest nasz kandydat, tylko jak bardzo zdecydowany do osiągnięcia celu. Pytanie - „Jedziesz na rozmowę kwalifikacyjną i właśnie ochłapał Cię samochód - co robisz?” nie sprawdza jak czysty czy kulturalny jest potencjalny pracownik, ale jak szybko podejmuje decyzje.

(...)

„Wady i zalety” - o ile zazwyczaj ludzkiem łatwiej przychodzi opowiadać o swoich słabościach niż mocnych stronach, podczas rozmowy kwalifikacyjnej, pytanie o wady jest najbardziej problematycznym. Różnicę poradzi, radzą, aby na wywiadzie taką cechę, która w rzeczywistości może być traktowana jako zaleta (np. pracowitość, bądź skrupulatność) - nie ma nic bardziej błędnego.

Po pierwsze - osoba przeprowadzająca rozmowę, chce nas poznać, aby móc właściwie określić nie tylko czy nadajemy się na dane stanowisko pod względem formalnym, ale także czy będziemy w stanie odnieść się w tej konkretniej sytuacji do naszej aplikacji. Jeśli mamy problemy z np. punktualnością, to praca w firmie, gdzie bezstrasznie przestrzegasz się godzin przyjazdu, będzie katorgą, w której długo nie wytrzymamy. Jeśli wolimy pracować indywidualnie i w pogardzie mamy innych, to nie ma sensu udawać, że z natury jesteśmy dużą towarzyską - rozczarowanie bowiem obu stron będzie bolesnym rezultatem szybkie.

Po drugie - rekruter nie jest pozbawiony mózgu i odwołamy mu inteligencję wyliczając w trakcie spotkania wady, przemianowujemy wypracowane sposoby na zalety. I tak się orientuje, a co najwyżej zostaniemy zakwalifikowani jako podzi i przyzwili oszusti.

Po trzecie - każde stanowisko ma swoją specyfikę - najważniejsze dla niego cechy zwykle są podane w ogłoszeniu rekrutacyjnym - nie ma więc spójności wyliczyć takich rzeczywiście wady, które w konkretnie danym momencie nie będą przeszkadzające. Piekarz czy programista może być nieśmiały, a rekruter koparki podejrzliwy - nie wpływa to bowiem na jakość wykonywanych przez nich prac.

Po czwarte - cechy osobowości mają swoje natężenie. Nie można ich jednoznacznie określić jako „dobrych” czy „złych”. Interpretowanie to przychylna cecha - zakładam, że pracownik nie posiada dokumentów, że w terminach, a jego biurko nie zarosło pleśnią, ale zbyt silna tendencja do strachu w przestrzeni wokół zmienia się w podatłość, która w pracownictwie jest w stanie doprowadzić do szale.

Najbardziej więc wypracuj w trakcie rozmowy kwalifikacyjnej swoje rzeczywiste wady, niekoludzące jednak z charakterem stanowiska na które aplikujemy.

(...)

„Jak wyróżnia Pan siebie idealnego Szefa?” - pytanie niezwykle trudne, zakładam bowiem bezwzględnie opina Szefa idealnego, od którego rzeczywisty, przynajmniej był - siedzący na krześle - może być nierównie stał. On zaś kandydatem jest osoba noworodka. 7 latni

- **Invisible**

The watermark is **unnoticeable** by the recipient,  
properties of human hearing or visual systems are utilized

# Digital watermark

- **Robust**

Modifications of watermarked content **will not affect** watermark

**vs.**

- **Fragile**

The watermark **is unnoticeable** by the recipient, properties of human hearing or visual systems are utilized

- **Public**

Users of content are authorized to detect watermark

**vs.**

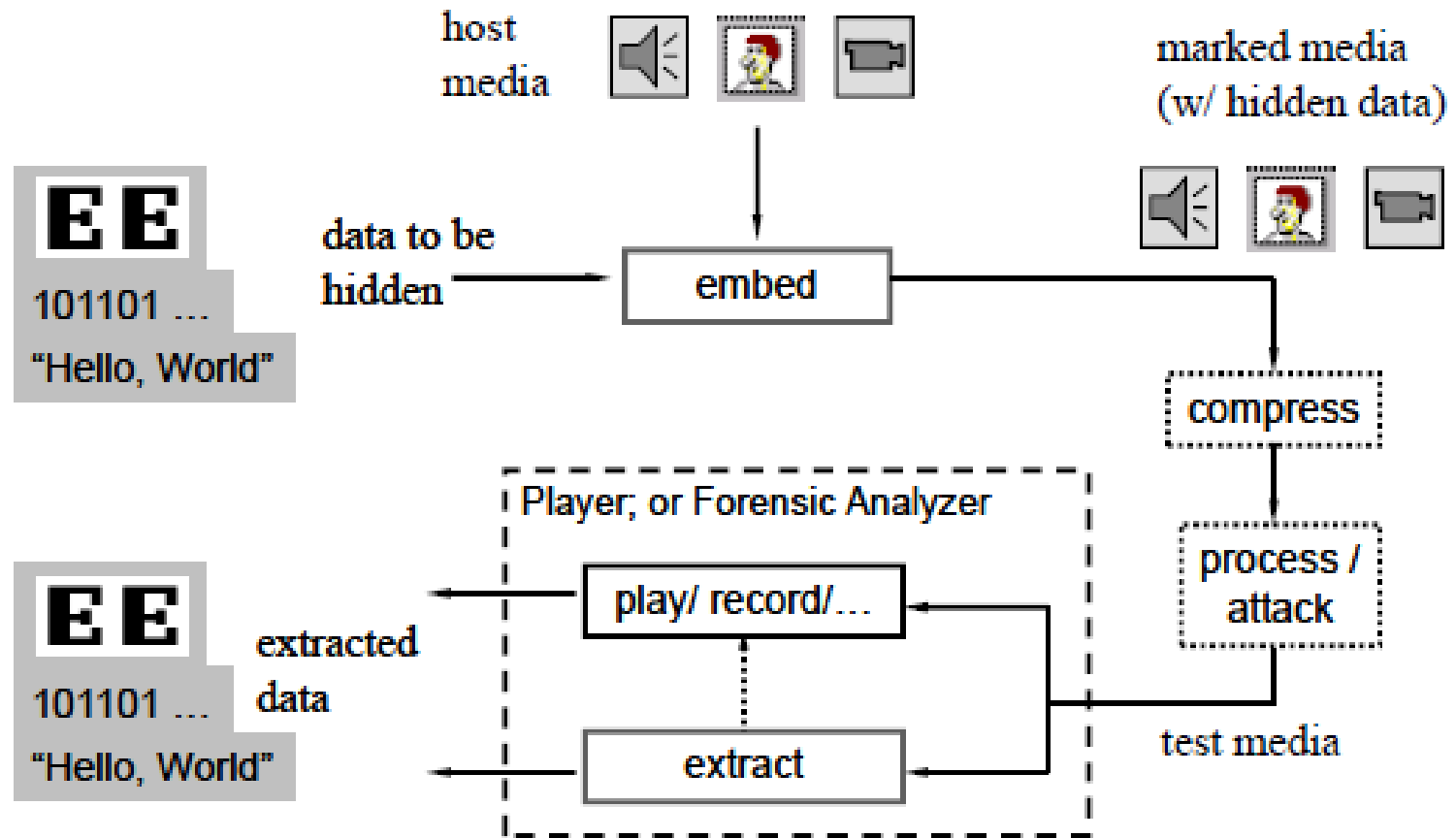
- **Private**

Users of content are NOT authorized to detect watermark

# The need of watermarking: robust vs. fragile

- **Copyright protection:**  
prove the ownership, DRM systems
- **Fingerprinting:**  
trace the source
- **Copy protection:**  
prevent illegal copying
- **Data authentication:**  
check authenticity of data
  - *Fragile or semi-fragile watermarking*

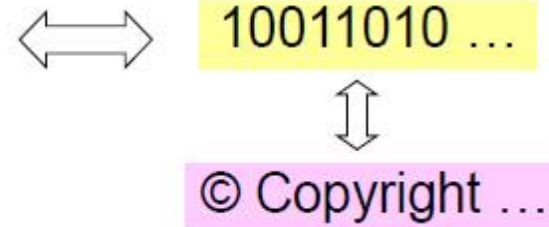
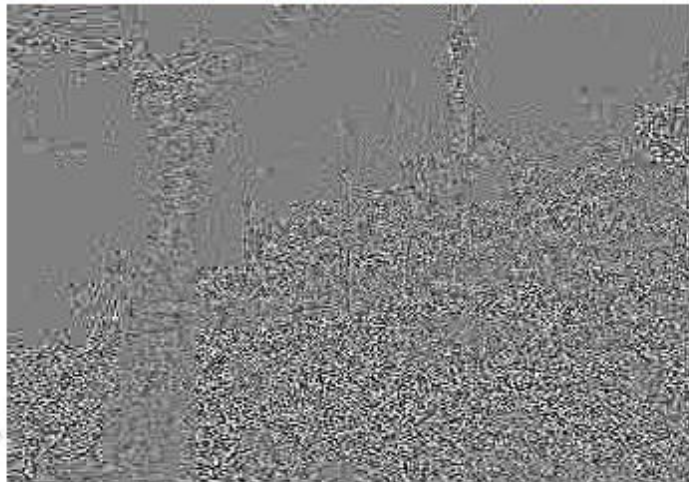
# General framework of watermarking



# Basic requirements for watermarking

- **Imperceptibility** (perceptual transparency)
- **Payload**
  - the amount of information that can be stored in a watermark
- **Robustness** (against different modifications - attacks)
- **Security** – Kerckhoff Principle
  - A system should be secure even if everything about the system, except the key, is public knowledge (the choice of the key is crucial)
- **Blind and non-blind detection** (Oblivious vs Non-oblivious)
  - Blind detection does not use the original, unmarked copy

# Invisible and robust watermark



# Watermarking – replacing LSBs

- Replace LSB with Pentagon's MSB



# Embedding methods

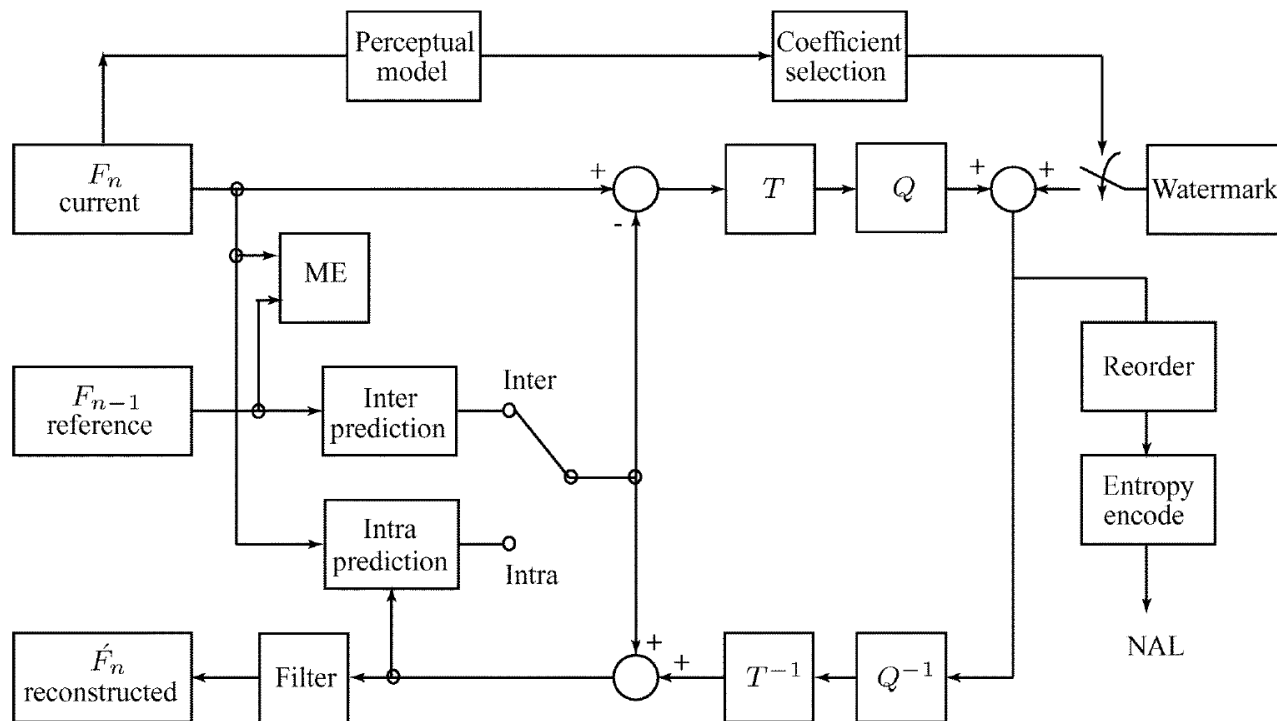
- In spatial domain (samples, pixels)
- In frequency domain (transform coefficients)
- In compressed domain (compressed stream)

Low

Complexity

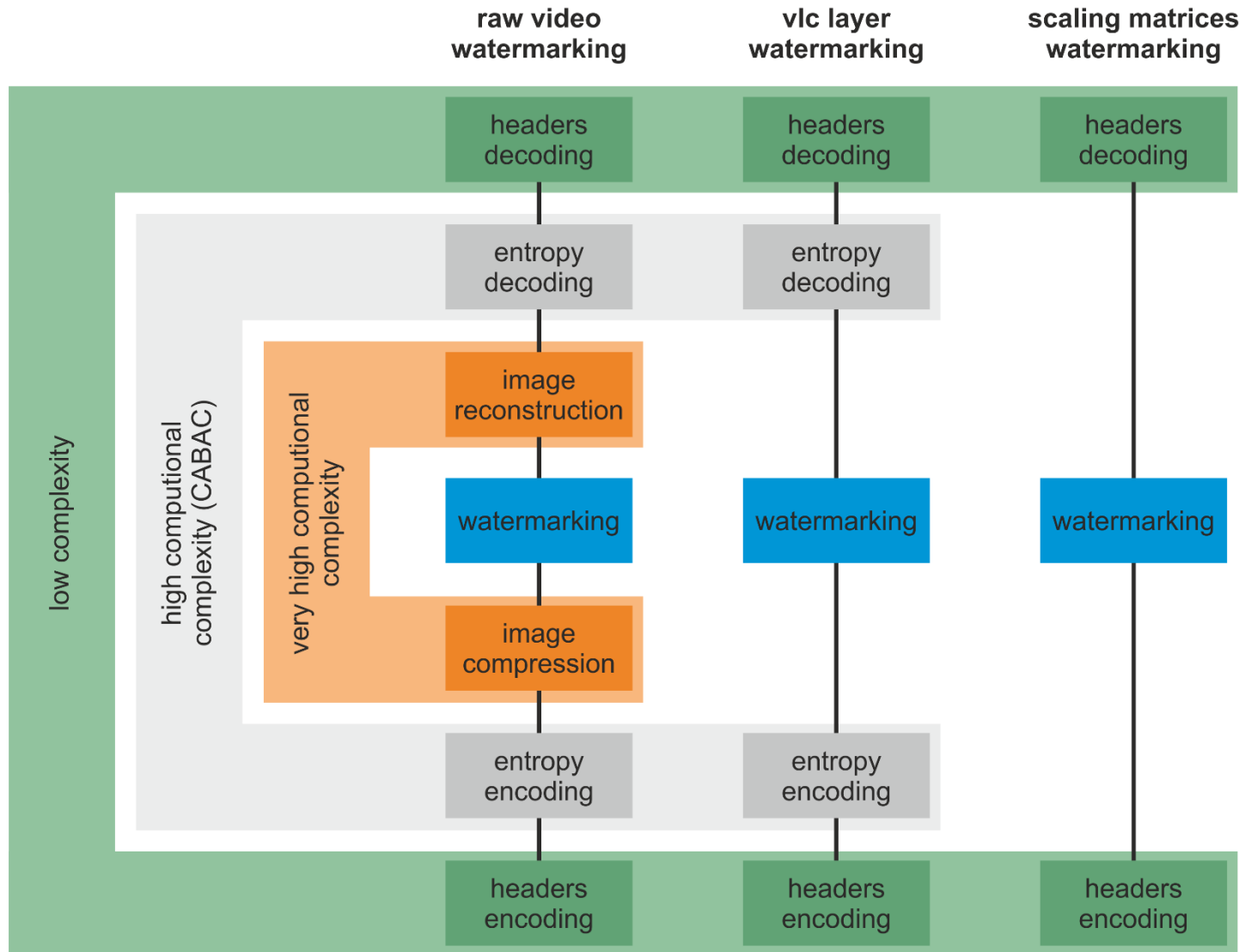
High

# Watermarking system for AVC - example



M. Noorkami, R. M. Mersereau, „A Framework for Robust Watermarking of H.264-Encoded Video With Controllable Detection Performance”, IEEE Transactions on Information Forensics and Security, vol. 2, no. 1, March 2007.

# Watermarking of compressed streams

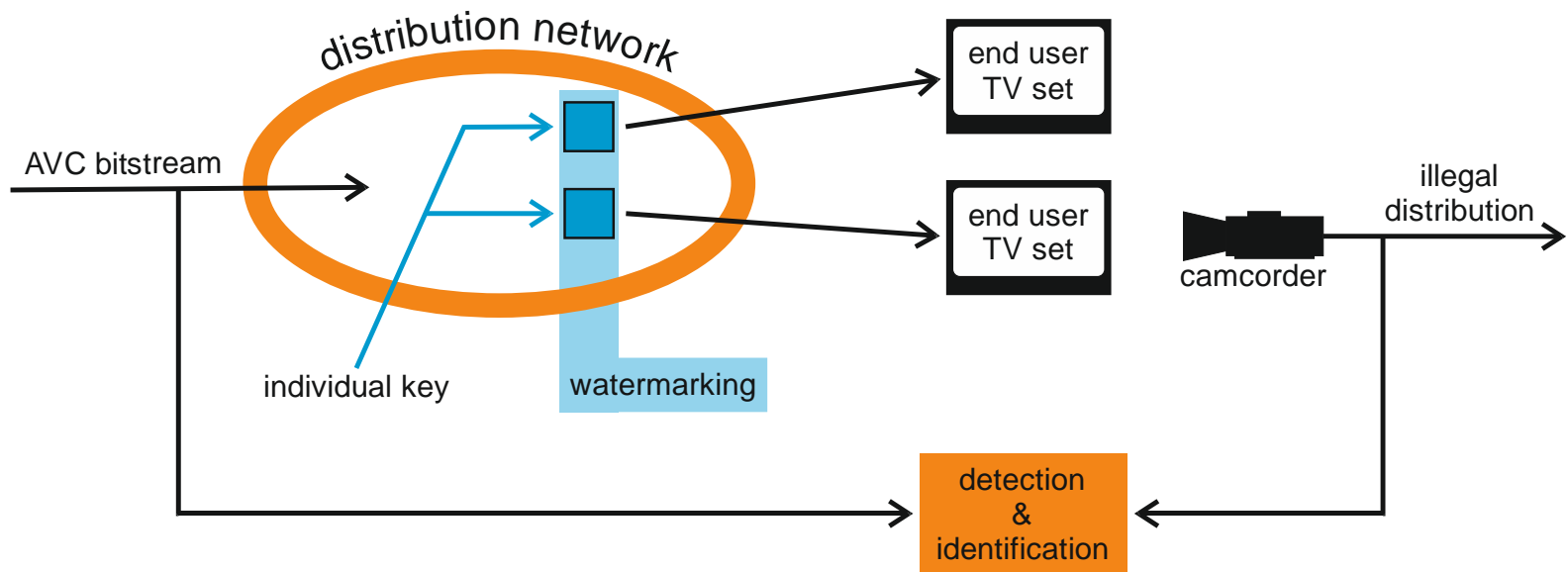


# Watermarking of compressed streams

	raw video watermarking	vlc layer watermarking	scaling matrices watermarking
+	<ul style="list-style-type: none"> <li>• access to each picture element</li> <li>• no watermark type restrictions</li> <li>• drift compensation</li> </ul>	<ul style="list-style-type: none"> <li>• no image reconstruction and recompression</li> </ul>	<ul style="list-style-type: none"> <li>• no image reconstruction and recompression</li> <li>• no slice data de- and encoding</li> </ul>
—	<ul style="list-style-type: none"> <li>• full de- and encoding</li> <li>• high computational power embedder required (uncompressed sequence processing)</li> </ul>	<ul style="list-style-type: none"> <li>• entropy de- and encoding (high complexity of CABAC)</li> <li>• access to some elements (coeffs, mv, etc.)</li> <li>• reduced drift control</li> </ul>	<ul style="list-style-type: none"> <li>• no local modifications</li> <li>• no drift compensation</li> </ul>

# System overview

- **Constrains:**
  - access to encoded bitstream only
  - separate watermarking of every video bitstream with individual key
  - low complexity real-time embedder
  - robustness against common attacks including camcording




# Proposed method

- Changing the quantization (scaling) matrices

Quantization (encoder side)

$$Y_Q(i, j) = \text{round} \left( \frac{Y(i, j)}{Q_S} \cdot \frac{16}{Q_T(i, j)} \right)$$

Quantization  
(scaling)  
matrix



Scaling (decoder side)

$$X(i, j) = \text{round} \left( Y_Q(i, j) \cdot Q_S \cdot \frac{Q_T(i, j)}{16} \right)$$

# Proposed method

- Modified transform coefficients for 4x4 and 8x8 block size:

	0	1	2	3
0	DC	AC (0,1)		
1	AC (1,0)			
2				
3				

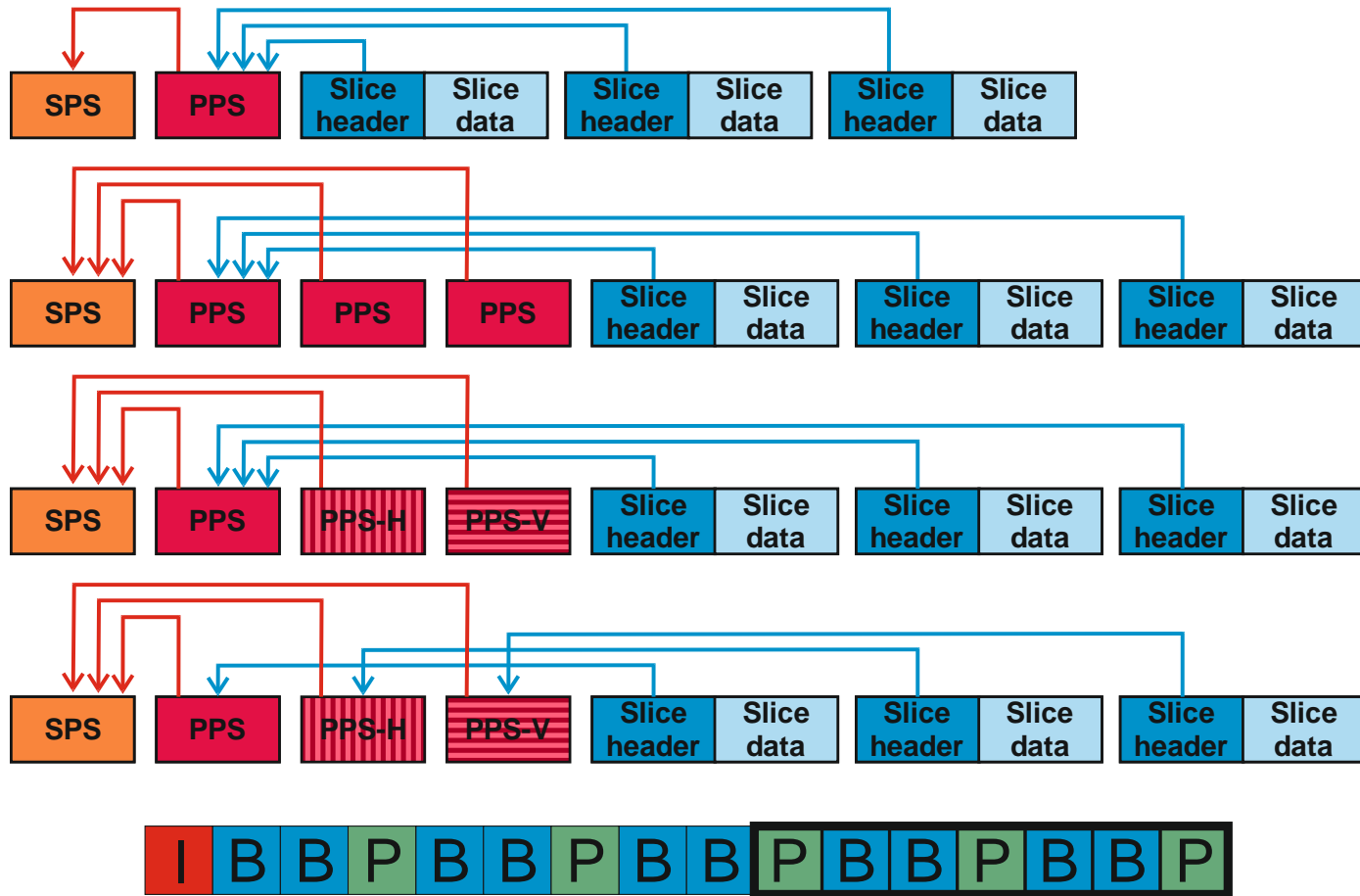
4x4

	0	1	2	3	4	5	6	7
0	DC		AC (0,2)	AC (0,3)				
1			AC (1,2)	AC (1,3)				
2	AC (2,0)	AC (2,1)						
3	AC (3,0)	AC (3,1)						
4								
5								
6								
7								

8x8

# Proposed method

- Bitstream modifications made during watermarking process (PPS-H and PPS-V contain modified quantization matrices)



# Profile issue

- In AVC (MPEG-4 part 10, H.264), the quantization (scaling) matrix transmission possible in the High profiles
- In HDTV broadcasts - the High profile mostly used
- Main profile - subset of the High profile tools
- Simple Main to High profile conversion:
  - *profile\_idc* in Sequence Parameter Set (SPS)
  - additional flags required in the High profile
- Standard HDTV decoder compatible with the High profile of MPEG-4 AVC/H.264

# Watermark detection

- The original and the investigated video sequence needed
- Both sequences must be temporally aligned, but spatial alignment is not critical
- The detector's input sequences (the original and the investigated) analyzed in spectral domain (the 8x8 transform as defined in MPEG-4 AVC/H.264)
- The averaged energy of each coefficient over 8x8 blocks in a frame estimated as follows:

$$\overline{E}_{i,j} = \frac{1}{N} \sum_k (a_{i,j}^k)^2$$



# Methodology

- Four different scenarios were tested to check robustness against most popular attacks:
  - Scenario 1: (attack simulation): Low-pass filtering, 10% image cropping and 10% image resizing
  - Scenario 2: Camcording using HD camera
  - Scenario 3: Camcording using HD camera and downscaling to SD resolution
  - Scenario 4: Camcording using HD camera and frame rate reduction (from 25 to 12.5 fps)
- Two different random bit streams (A and B) were used as the watermark payload.
- Five HDTV (1920x1080, 25 fps) video sequences - 10 min. length.
- x264 encoder, configured to produce the MPEG-4 AVC/H.264 High-profile-compliant bitstreams.

# Results

Sequence type	Payload bitstream	Properly detected bits [%] in scenario:			
		1.	2.	3.	4.
Soap opera 1	A	97.7	88.5	83.3	88.4
	B	97.4	87.6	82.0	87.8
Soap opera 2	A	98.4	88.5	88.5	88.5
	B	98.7	92.4	87.3	91.1
Historical novel	A	99.8	97.4	96.3	96.7
	B	99.9	99.6	98.7	99.2
Computer animated film	A	96.6	87.2	82.7	84.7
	B	97.0	87.7	82.8	86.0
War film	A	94.9	76.2	72.4	73.8
	B	95.4	75.0	73.9	74.6
<b>Average</b>	A	97.5	87.6	84.6	86.4
	B	97.7	88.5	84.9	87.7

# Results



# Summary

---

Advantages of the proposed method:

- Low computationally complex embedder
- Negligibly small bitstream increase
- Robustness against:
  - blurring
  - camcording
  - downscaling to SD
  - dawnsampling to lower frame rate
- Suitable for implementation on low processing power devices or systems