Ensuring security of H.264 videos by using watermarking

Marc Chaumont

April 22, 2011

Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Preamble

Outline

1. Preamble

2. H.264

3. Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)

4. Conclusion & Perspectives
Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Preamble

Slides may be downloaded at  http://www.lirmm.fr/~chaumont/Publications.html

e-mail: marc.chaumont@lirmm.fr
Where video compression is hidden in every days life?

A word of video compression

- Camera (Video surveillance, Smart Phone, ...),
- Streaming (YouTube, Television, ...),
- Storing (DVD, Blue-Ray, Hard-Disk, ...),
- Editing (Cinema, advertisement, entertainment).

→ Lots of people use videos.
Preamble

There is security requirements

The problem for right owners is the pirates...

Scientists should find solutions in order to dissuade users from pirating
Watermarking is a possible solution

Applications using watermarking:

<table>
<thead>
<tr>
<th>Related to security</th>
<th>Related to media enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>copyright identification</td>
<td>broadcast monitoring</td>
</tr>
<tr>
<td>traitor tracing (active fingerprinting)</td>
<td>device control</td>
</tr>
<tr>
<td>authentication</td>
<td>enrichment (functionalities and/or meta-datas)</td>
</tr>
<tr>
<td>copy control</td>
<td>with forward compatibility</td>
</tr>
<tr>
<td></td>
<td>improve compression performances</td>
</tr>
<tr>
<td></td>
<td>improve error recovery &amp; correction</td>
</tr>
</tbody>
</table>

In most of these applications, the watermarking should be robust.
What is robust watermarking?

General watermarking scheme

message → EMBEDING → marked → channel → attacked → EXTRACTION → message

message → host
Robustness illustration

original

watermarked

Robustness illustration: detection = Ok

watermarked

additive noise

Outline

1. Preamble

2. H.264

3. Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)

4. Conclusion & Perspectives
H.264 or MPEG-4 Part 10:

- **State-of-the-art** video coding standard,
- First version approved in 2003,
- Normalized by ITU-T and ISO/IEC organizations,
- **Up to 50% in bit rate savings** compared to MPEG-2 and MPEG4 Part 2 simple profile.


Visual example...

H.264 100Kbs

MPEG2 100Kbs
General coding scheme

H.264 General coding scheme

- Integer Transformation
- Quantization
- Entropy coding

INTRA or INTER prediction

Macroblock 16x16

+ - residue

Integer Transformation

Quantization

Entropy coding

0010101001 bitstream

control data

motion data
General coding scheme

Macroblock 16x16 → INTRA or INTER prediction → residue

Integer Transformation → Quantization → Entropy coding → 0010101001 bitstream

control data

motion data
General coding scheme

- **Macroblock** 16x16
- **INTRA or INTER prediction**
- **residue**
- **Integer Transformation**
- **Quantization**
- **Entropy coding**
- **bitstream** 0010101001
- **control data**
- **motion data**
Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

H.264

General coding scheme

Macroblock 16x16 → INTRA or INTER prediction

Integer Transformation → Residue

Quantization → Motion data

Entropy coding → 0010101001 bitstream
General coding scheme

Macroblock 16x16

INTRA or INTER prediction

residue

Integer Transformation

Quantization

Entropy coding

0010101001 bitstream

control data

motion data
Outline

1. Preamble
2. H.264
3. Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)
4. Conclusion & Perspectives
Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Watermarking
Robust video watermarking

Outline

1 Preamble

2 H.264

3 Watermarking
   • Robust video watermarking
   • Security of video watermarking
   • A practical security example: the traitor tracing (active fingerprinting)

4 Conclusion & Perspectives
### Few non-malicious attacks for a video

<table>
<thead>
<tr>
<th>Non-malicious attacks:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Photometric</td>
<td>Noise addition, DA/AD conversion</td>
</tr>
<tr>
<td></td>
<td>Gamma correction</td>
</tr>
<tr>
<td></td>
<td>Transcoding and video format conversion</td>
</tr>
<tr>
<td></td>
<td>Intra and inter-frames filtering</td>
</tr>
<tr>
<td></td>
<td>Chrominance resampling (4:4:4, 4:2:2, 4:2:0)</td>
</tr>
<tr>
<td>Spatial Desynchronization</td>
<td>Changes display formats (4/3, 16/9, 2.11/1)</td>
</tr>
<tr>
<td></td>
<td>Changes resolution (NTSC, PAL, SECAM)</td>
</tr>
<tr>
<td></td>
<td>Positional jitter</td>
</tr>
<tr>
<td></td>
<td>Hand-held camera recording (curved-bilinear transform)</td>
</tr>
<tr>
<td>Temporal Desynchronization</td>
<td>Changes of frame rate</td>
</tr>
<tr>
<td></td>
<td>Frame dropping / insertion</td>
</tr>
<tr>
<td></td>
<td>Frame decimation / duplication</td>
</tr>
<tr>
<td>Video editing</td>
<td>Cut-and-splice and cut-insert-splice</td>
</tr>
<tr>
<td></td>
<td>Fade-and-dissolve and wipe-and-matte</td>
</tr>
<tr>
<td></td>
<td>Graphic overlay (subtitles, logo)</td>
</tr>
</tbody>
</table>

---

Major approaches

Before compression
- images
  - SS [Cox et al., TIP’1997]
  - DPTC [Miller et al., TIP’2004]
  - P-QIM [Li and Cox, TIFS’2007]
  - …

Sequence of images
- Temporal watermarking
  - [Haitsma and Kalker, ICIP’2001]
  - [Chen et al., IWDW’2009]
- 3D DFT
  - [Deguillaume et al., SPIE’1999]
- On-off keying (Extended BA)
  - [Xie et al., MM&Sec2008]
  - …

Inside H.264 structure

Before quantization
- Luma modification:
  - [Golikeri et al., JEI’2007]
- Motion vectors modification:
  - [Zhang et al., SCG’2001]
- GOP structure modification:
  - [Linnartz and Talstra, ESRCS’1998]
  - …

During Entropy coding

During encoding process
- [Mobasseri and Raikar, SPIE’2007]
- [Zou and Bloom, SPIE’2009]
- …

In an already
H.264 encoded
bitstream
- [Shahid et al.,
  EUSIPCO’2009]
- [Noorkami and Mersereau,
  TIFS’2008]
  - …
- [Hartung and Girod,
  Signal Processing 1998]
- [Gong and Lu, ISM’2008]
  - …
Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Watermarking
Robust video watermarking

Inside H.264

Before compression

images

SS [Cox et al., TIP’1997]
DPTC [Miller et al., TIP’2004]
P-QIM [Li and Cox, TIFS’2007]
...

sequence
of images

Temporal watermarking
[Haitsma and Kalker,ICIP’2001]
[Chen et al., IWDW’2009]

3D DFT
[Deguillaume et al., SPIE’1999]

On-off keying (Extended BA)
[Xie et al., MM&Sec2008]
...

Before quantization

Luma modification:
[Golikeri et al., JEI’2007]

Motion vectors modification:
[Zhang et al., SCGIP’2001]

GOP structure modification:
[Linnartz and Talstra, ESRCS’1998]
...

Inside H.264 structure

After quantization

During encoding process

[Shahid et al.,
EUSIPCO’2009]
[Noorkami and Mersereau,
TIFS’2008]
...

During Entropy coding

[Mobasseri and Raikar, SPIE’2007]
[Zou and Bloom, SPIE’2009]
...

In an already
H.264 encoded
bitstream

[Heydt et al.
Signal Processing 1998]
[Gong and Lu, ISM’2008]
...

...
Brief conclusion about robust video watermarking

Good news

There are good solutions robust to photometric attacks **INSIDE H.264** (or a similar codec).

Bad news

Most of the solutions (all?) **INSIDE H.264** (or a similar codec) are **not robust** (or not enough robust) to **temporal and spatial desynchronizations**.

→ What about security?
Outline

1. Preamble
2. H.264
3. Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)
4. Conclusion & Perspectives
Definition

The classical framework of security:

Kerckhoffs’s framework

The embedding and extracting algorithms are known by the attacker and the attacker owns observations. The only secret parameter is the key.

Security attack

A security attack is an attack for which secrets parameters or secret informations are obtained.

Security subject addresses those technical points:

- Analysis and creation of secure algorithm,
- Analysis and creation of security attack.

Security of few images schemes

Security addresses the problem of recovering secret parameters.

<table>
<thead>
<tr>
<th>Images</th>
<th>Proposed attacks</th>
</tr>
</thead>
</table>


## Video collusion attack

**Inter** video collusion (not specific to video): Collusion with several videos

<table>
<thead>
<tr>
<th></th>
<th>Collusion type I</th>
<th>Collusion type II</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyright application</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>(same watermark in ≠ videos)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traitor tracing application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(≠ watermarks in the same videos)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Intra** video collusion (specific to video): collusion with just 1 video

<table>
<thead>
<tr>
<th></th>
<th>Collusion type I</th>
<th>Collusion type II</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same watermark in ≠ frames of the video</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>≠ watermarks in each frame of the video (and thus in static scenes)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

→ main security “danger” is Intra video collusion.

---

Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Watermarking
A practical security example: the traitor tracing (active fingerprinting)

Outline

1 Preamble

2 H.264

3 Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)

4 Conclusion & Perspectives
Traitor tracing concept
Example of watermarking for security:
traitor tracing application

An investigation experiment:


- The best probabilistic code (coming from cryptography community): The Tardos code.
- A video watermarking technique inside H.264, before quantization, taking into account RD optimization, robust to photometric attacks, and real time.
Ensuring security of H.264 videos by using watermarking - Marc Chaumont - SPIE’2011

Watermarking
A practical security example: the traitor tracing (active fingerprinting)

Example of watermarking for security:
Shahid, Chaumont and Puech, ICIP’2010

100 users maximum
20 colluders maximum
Probability accusing an innocent $10^{-3}$
User ID (codeword) on 92 104 bits

10 bits / frame

Intra CIF 352x288
25 fps
92 104 bits
$\approx 6$ minutes

Macroblocks hiding the same bit

Spread Spectrum embedding
(DCs coefficients modification)
Collusion attacks

\( f_k \): a video frame from a colluder \( k \).  
\( C \): the set of colluders.  
\( K \): the number of colluders.

<table>
<thead>
<tr>
<th>Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_{\text{min}} = \min { f_k }_{k \in C} )</td>
<td>Minimum watermark value</td>
</tr>
<tr>
<td>( f_{\text{max}} = \max { f_k }_{k \in C} )</td>
<td>Maximum watermark value</td>
</tr>
<tr>
<td>( f_{\text{avg}} = \sum_{k \in C} \frac{f_k}{K} )</td>
<td>Average watermark value</td>
</tr>
<tr>
<td>( f_{\text{median}} = \text{median} { f_k }_{k \in C} )</td>
<td>Median watermark value</td>
</tr>
<tr>
<td>( f_{\text{minmax}} = \frac{f_{\text{min}} + f_{\text{max}}}{2} )</td>
<td>Min-max watermark value</td>
</tr>
<tr>
<td>( f_{\text{modNeg}} = f_{\text{min}} + f_{\text{max}} - f_{\text{median}} )</td>
<td>Modified negative watermark value</td>
</tr>
</tbody>
</table>

'bus', 'city', 'foreman', 'football', 'soccer', 'harbour', 'ice' and 'mobile', have been concatenated and repeated 4 times.
## Detection of the colluders

<table>
<thead>
<tr>
<th>$K$</th>
<th>No. of colluders detected for attacks</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>avg</td>
<td>min</td>
<td>max</td>
<td>median</td>
<td>minmax</td>
<td>modNeg</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>16</td>
<td>15</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>18</td>
<td>18</td>
<td>18</td>
<td>19</td>
<td>18</td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>
Visual evaluation
An interesting practical scheme,
but the watermarking scheme is not enough secure,
and the algorithm is not robust to spatial and temporal desynchronization.

Another interesting approach (outside H.264):


There is still lots of work...
Outline

1. Preamble

2. H.264

3. Watermarking
   - Robust video watermarking
   - Security of video watermarking
   - A practical security example: the traitor tracing (active fingerprinting)

4. Conclusion & Perspectives
Conclusion and perspectives

- Lots of possible ways to do watermarking inside H.264 (depends on application)

- **If desynchronization (spatial & temporal) robustness** is a requirement
  ⇒ Very few algorithms; still an open problem.

- **If security** is a requirement (but not desynchronization (spatial & temporal) robustness)
  ⇒ Very few algorithms; still an open problem

- **If desynchronization (spatial & temporal) robustness & security** are requirements
  ⇒ The Graal quest!
End

Slides may be downloaded at: http://www.lirmm.fr/~chaumont/Publications.html

e-mail: marc.chaumont@lirmm.fr
References:

**Spread Spectrum:**

[Cox et al., TIP’1997]


**DPTC:**

[Miller et al., TIP’2004]


**Percetpual-QIM:**

[Li and Cox, TIFS’2007]

References:

**Temporal watermarking:**

[Haitsma and Kalker, ICIP’2001]


[Chen et al., IWDW’2009]


**3D DFT:**

[Deguillaume et al., SPIE’1999]


**On-off keying:**

[Xie et al., MM&Sec2008]

References:

**Luma modification:**

[Golikeri et al., JEI’2007]


**Motion vector modification:**

[Zhang et al., SCGIP’2001]


**GOP structure modification:**

[Linnartz and Talstra, ESRCS’1998]

References:

[Shahid et al. EUSIPCO’2009]

[Noorkami and Mersereau, TIFS’2008]

[Hartung and Girod, Signal Processing 1998]

[Gong and Lu, ISM’2008]
References:

[Mobasseri and Raikar, SPIE'2007]

[Zou and Bloom, SPIE'2009]
References:

[Bas and Westfeld, MM&Sec’2009]

[Xie et al., SPIE’2010]

[Bas et Doërr, MM&Sec’2008]

[Mathon et al., AT’2009]

[Pérez-Freire et Pérez-González, IH’ 2007]