Ensuring security of H.264 videos by using watermarking

Marc Chaumont

April 22, 2011

"Mobile Multimedia/Image Processing, Security, and Applications 2011", Part of SPIE'2011, Defense, Security, and Sensing, 25 - 29 April 2011 Orlando, USA.

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

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

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.

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

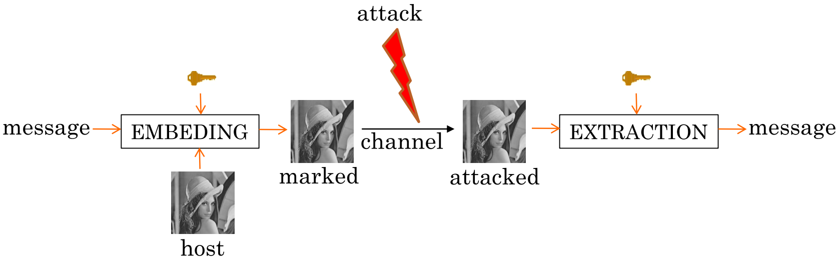
Applications using watermarking:

Related to security	Related to media enhancement
copyright identification	broadcast monitoring
traitor tracing (active fingerprinting)	device control
authentication	enrichment (functionalities and/or meta-datas) with forward compatibility
copy control	improve compression performances
	improve error recovery & correction

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

What is robust watermarking?

General watermarking scheme



Robustness illustration

original

watermarked

"Broken Arrows", Teddy Furon and Patrick Bas, EURASIP Journal on Information Security, 2008.

Robustness illustration: detection = Ok

watermarked

additive noise

"Broken Arrows", Teddy Furon and Patrick Bas, EURASIP Journal on Information Security, 2008.

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

What is H.264/AVC?

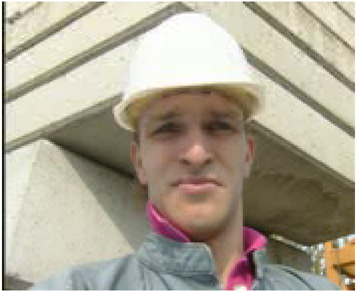
H.264 or MPEG-4 Part 10:

- **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.

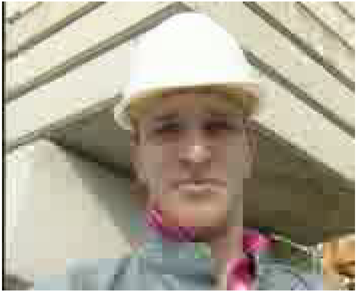
"Draft ITU-T Recommendation and Final Draft International Standard of Joint Video Specification (ITU-T Rec. H.264 ISO/IEC 14496-10 AVC)," Tech. Rep., Joint Video Team (JVT), Doc. JVT-G050, March 2003.

I. Richardson, "H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia", 2003.

Visual example...

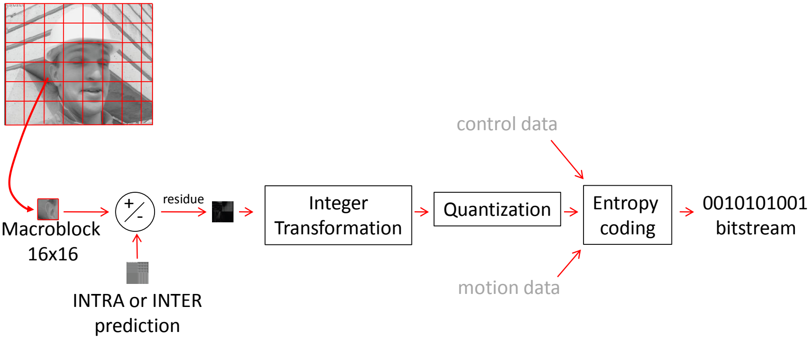


H.264 100Kbs

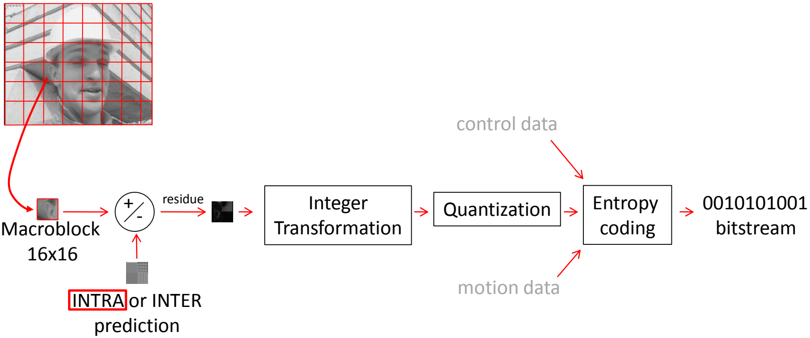


MPEG2 100Kbs

General coding scheme



General coding scheme



Macroblock 16x16

+ / -

residue

INTRA or INTER prediction

Integer Transformation

Quantization

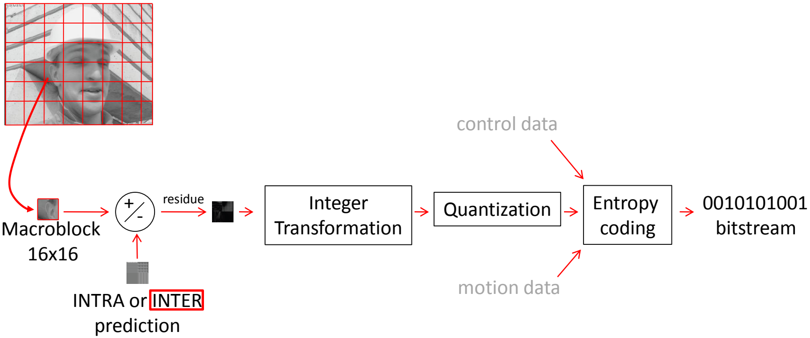
Entropy coding

control data

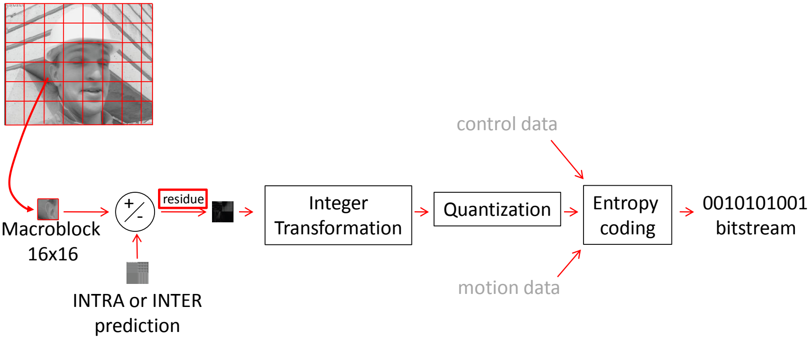
motion data

0010101001 bitstream

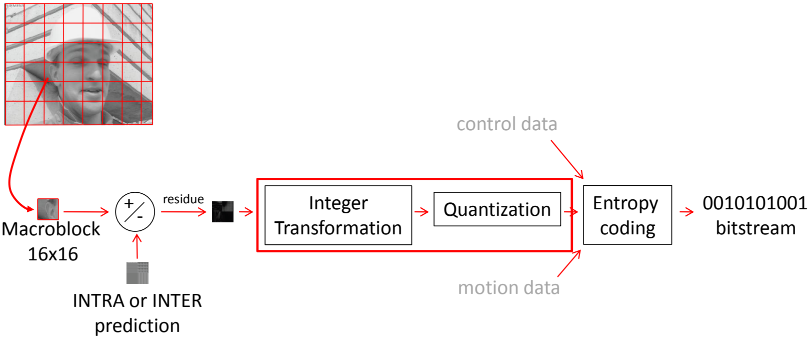
General coding scheme



General coding scheme



General coding scheme



Macroblock 16x16

+/-

residue

INTRA or INTER prediction

Integer Transformation

Quantization

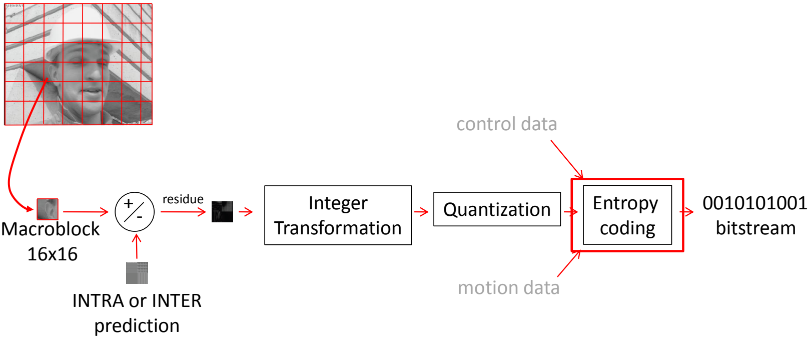
control data

motion data

Entropy coding

0010101001 bitstream

General coding scheme



Macroblock 16x16

+ / -

residue

INTRA or INTER prediction

Integer Transformation

Quantization

control data

Entropy coding

motion data

0010101001 bitstream

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

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

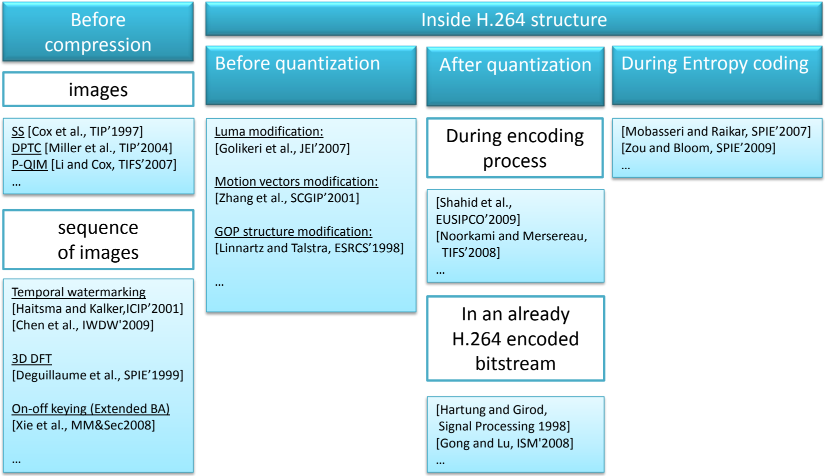
Few non-malicious attacks for a video

Non-malicious attacks:

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

"Security issue and collusion attacks in video watermarking", PhD Thesis, G. Doërr, Supervised by J.-L. Dugelay, University of Nice-Sophia Antipolis, France, june 2005.

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., SCGIP'2001]

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

…

After quantization

During encoding process

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

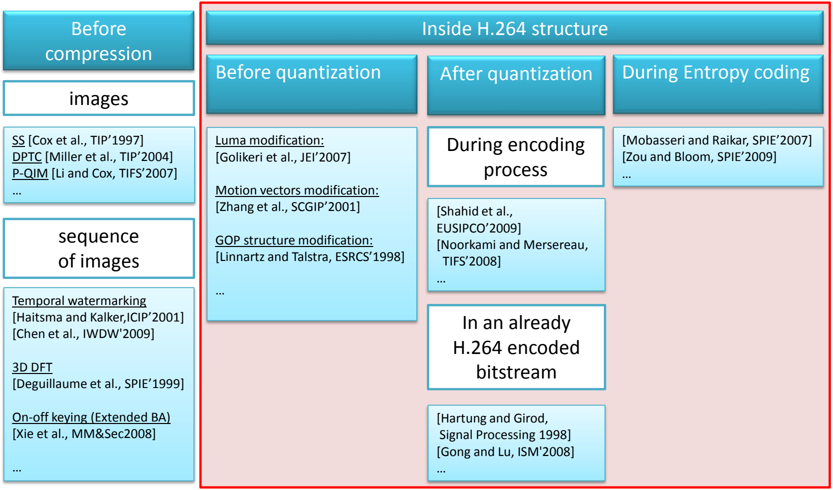
In an already H.264 encoded bitstream

[Hartung and Girod, Signal Processing 1998]
[Gong and Lu, ISM'2008]
…

During Entropy coding

[Mobasseri and Raikar, SPIE'2007]
[Zou and Bloom, SPIE'2009]
…

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]

…

Inside H.264 structure

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]

…

After quantization

During encoding process

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

In an already H.264 encoded bitstream

[Hartung and Girod, Signal Processing 1998]
[Gong and Lu, ISM'2008]
…

During Entropy coding

[Mobasseri and Raikar, SPIE'2007]
[Zou and Bloom, SPIE'2009]
…

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.

F. Cayre, C. Fontaine, T. Furon, "Watermarking Security: Theory and Practice", IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3976-3987, 2005.

Security of few images schemes

Security addresses the problem of recovering secret parameters.

Images	Proposed attacks
Spread Spectrum	"Comparison of secure spread-spectrum modulations applied to still image watermarking" B. Mathon, P. Bas P, F. Cayre F, and B. Macq. Annals of Telecommunication, 2009.
Broken Arrows	"Two Key Estimation Techniques for the Broken-Arrows Watermarking Scheme", P. Bas and A. Westfeld, MM&Sec'2009. Counter Attack : "Better security levels for 'Broken Arrows' ", F. Xie, T. Furon, and C. Fontaine, SPIE'2010.
DPTC	"Evaluation of an Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes".P Bas and G. Doërr, MM&Sec'2008.
Quantized based	"Exploiting security holes in lattice data hiding", L. Perez-Freire and F. Perez-Gonzalez. IH'07.

Video collusion attack

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

	Collusion type I	Collusion type II
Copyright application (same watermark in ≠ videos)	√	
Traitor tracing application (≠ watermarks in the same videos)		√

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

	Collusion type I	Collusion type II
Same watermark in ≠ frames of the video	√	
≠ watermarks in each frame of the video (and thus in static scenes)		√

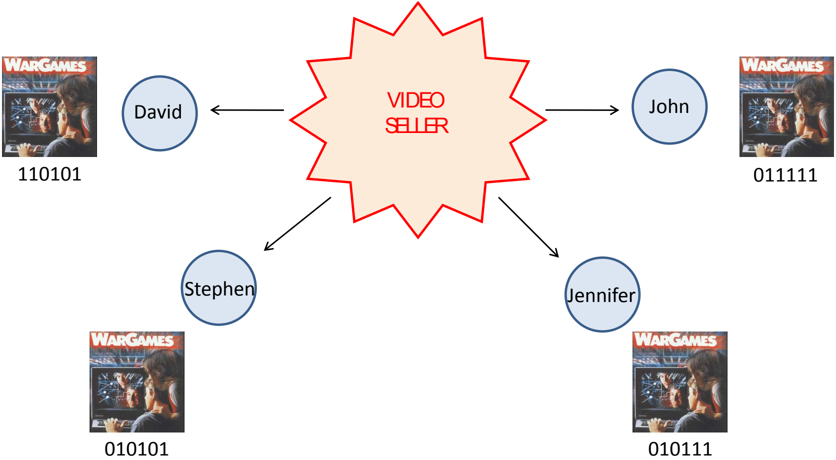
→ main security "danger" is Intra video collusion.

G. Doërr, J.-L. Dugelay, "A guide tour of video watermarking", Signal Processing: Image Communication 18 (2003) 263-282.

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

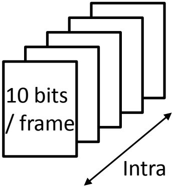
An investigation experiment:

Z. Shahid, M. Chaumont and W. Puech, "Spread Spectrum-Based Watermarking for Tardos Code-Based Fingerprinting of H.264/AVC Video", ICIP'2010, IEEE International Conference on Image Processing, Hong-Kong, China, 26-29 September, 2010, 4 pages.

- 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.

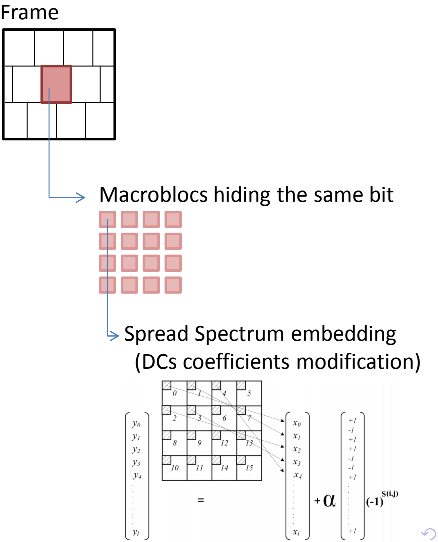
Example of watermarking for security: Shahid, Chaumont and Puech, ICIP'2010

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



Intra
CIF 352x288
25 fps

92 104 bits
≃ 6 minutes



Collusion attacks

f_k: a video frame from a colluder k.
$\mathcal{C}$: the set of colluders.
K: the number of colluders.

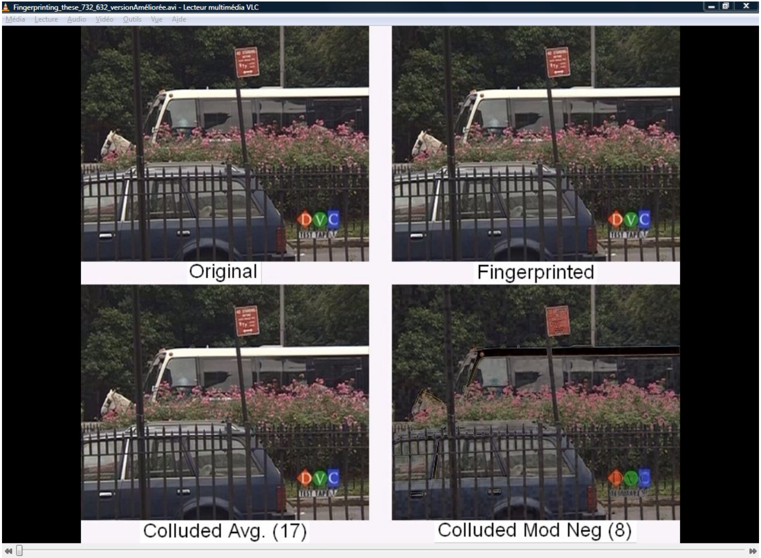
$f_{min} = \min\{f_k\}_{k \in \mathcal{C}}$	$f_{max} = \max\{f_k\}_{k \in \mathcal{C}}$
$f_{avg} = \sum_{k \in C} \frac{f_k}{K}$	$f_{median} = median\{f_k\}_{k \in \mathcal{C}}$
$f_{minmax} = \frac{f_{min}+f_{max}}{2}$	$f_{modNeg} = f_{min} + f_{max} - f_{median}$

'bus', 'city', 'foreman', 'football', 'soccer', 'harbour', 'ice' and 'mobile', have been concatenated and repeated 4 times.

Detection of the colluders

	No. of colluders detected for attacks					
K	avg	min	max	median	minmax	modNeg
2	2	2	2	2	2	2
5	5	5	5	5	5	5
8	8	8	8	8	8	6
11	11	10	10	10	10	7
14	14	13	13	13	13	9
17	16	15	16	16	16	10
20	18	18	18	19	18	11

Visual evaluation


Fingerprinting_these_732_632_versionAméliorée.avi - Lecteur multimédia VLC
Média Lecture Audio Vidéo Outils Vue Aide
Original
Fingerprinted
Colluded Avg. (17)
Colluded Mod Neg (8)

Shahid, Chaumont and Puech, ICIP'2010; remarks

- An interesting practical scheme,
- but the watermarking scheme is not enough secure,
- and the algorithm is not robust to spatial and temporal desynchronizations.

Another interesting approach (outside H.264):

F. Xie, T. Furon, C. Fontaine, "On-Off Keying Modulation and Tardos Fingerprinting", MM & Sec'08, September 22-23, 2008, Oxford, United Kingdom.

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]

I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing 6, 1673-1687 (1997).

DPTC:

[Miller et al., TIP'2004]

M.L. Miller, G. J. Doërr and J. Cox, "Applying Informed Coding and Embedding to Design a Robust, High capacity Watermark", IEEE Trans. On Image Processing, 13, 6, 792-807, June 2004.

Percetpual-QIM:

[Li and Cox, TIFS'2007]

Q. Li and I.J. Cox, "Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking", IEEE Transactions on Information Forensics and Security, 2, 2, 2007, p. 127-139.

—

References:

Temporal watermarking:

[Haitsma and Kalker, ICIP'2001]

Haitsma L., Kalker T., "A Watermarking Scheme for Digital Cinema", Proceedings of ICIP, vol. 1, Thessaloniki, Greece, p. 587-489, octobre 2001.

[Chen et al., IWDW'2009]

C. Chen, J. Ni, and J. Huang, "Temporal Statistic Based Video Watermarking Scheme Robust against Geometric Attacks and Frame Dropping", IWDW'2009, Proceedings of the 8th International Workshop on Digital Watermarking, Guildford, UK, p. 81-95, 2009.

3D DFT:

[Deguillaume et al., SPIE'1999]

F. Deguillaume, G. Csurka, J. O'Ruanaidh, and T. Pun, "Robust 3D DFT Video Watermarking," Security and Watermarking of Multimedia Contents 3657, 113-124, SPIE'1999.

On-off keying:

[Xie et al., MM&Sec2008]

F. Xie, T. Furon, C. Fontaine, "On-Off Keying Modulation and Tardos Fingerprinting", MM&Sec'08, September 22-23, 2008, Oxford, United Kingdom.

References:

Luma modification:

[Golikeri et al., JEI'2007]

A. Golikeri, P. Nasiopoulos, and Z. Wang, "Robust Digital Video Watermarking Scheme for H.264 Advanced Video Coding Standard," Journal of Electronic Imaging 16(4), 2007.

Motion vector modification:

[Zhang et al., SCGIP'2001]

J. Zhang, J. Li, L. Zhang, "Video Watermark Technique in Motion Vector", Proc. of XIV Symposium on Computer Graphics and Image Processing, pp.179-182, Oct.2001.

GOP structure modification:

[Linnartz and Talstra, ESRCS'1998]

Linnartz J.-P. M. G., Talstra J., "MPEG PTY-Marks : Cheap Detection of Embedded Copyright Data in DVD-Video", Proceedings of ESORICS, p. 221-240, 1998.

—

References:

[Shahid et al. EUSIPCO'2009]

Z. Shahid, P. Meuel, M. Chaumont and W. Puech, "Considering the Reconstruction Loop for Watermarking of Intra and Inter Frames of H.264/AVC", EUSIPCO'2009, The 17th European Signal Processing Conference, Glasgow, Scotland, 24-28 August, 2009 (an extended version has been submitted to Journal of Electronic Imaging 2010).

[Noorkami and Mersereau, TIFS'2008]

M. Noorkami and R. Mersereau, "Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase," IEEE Transactions on Information Forensics and Security, 3, 441-455 (2008).

—

[Hartung and Girod, Signal Processing 1998]

F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Process., vol. 66, no. 3, pp. 283-301, May 1998.

[Gong and Lu, ISM'2008]

X. Gong and H. Lu., "Towards Fast and Robust Watermarking Scheme for H.264 Video". In Proc. IEEE International Symposium on Multimedia, pages 649-653, 2008.

—

References:

[Mobasseri and Raikar, SPIE'2007]

B.G. Mobasseri and Y.N. Raikar. "Authentication of H.264 Streams by Direct Watermarking of CAVLC Blocks". In Security, Steganography, and Watermarking of Multimedia Contents IX, SPIE'2007.

[Zou and Bloom, SPIE'2009]

D. Zou and J.A. Bloom, "H.264/AVC Substitution Watermarking: A CAVLC Example", Media Forensics and Security, Proc. of SPIE-IS&T Electronic Imaging, SPIE Vol. 7254, 2009.

—

References:

[Bas and Westfeld, MM&Sec'2009]

"Two Key Estimation Techniques for the Broken-Arrows Watermarking Scheme", P. Bas and A. Westfeld, 11th ACM workshop on Multimedia and Security, MM&Sec'2009, September 07-08, 2009, Princeton, USA.

[Xie et al., SPIE'2010]

F. Xie, T. Furon, and C. Fontaine, "Better security levels for 'Broken Arrows' ", , in Proc. IS&T/SPIE Electronic Imaging, Media Forensics and Security XII, vol. 7541, San Jose, CA, Jan. 2010.

[Bas et Doërr, MM&Sec'2008]

P. Bas and G. Doërr, "Evaluation of an Optimal Watermark Tampering Attack Against Dirty Paper Trellis Schemes". In: 10th ACM workshop on Multimedia and Security, MM&Sec'2008, Oxford, United Kingdom (September 2008) 227-232.

[Mathon et al., AT'2009]

"Comparison of secure spread-spectrum modulations applied to still image watermarking" B. Mathon, P. Bas P, F. Cayre F, and B. Macq. Annals of Telecommunication, 2009.

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

"Exploiting security holes in lattice data hiding", L. Perez-Freire, and F. Perez-Gonzalez. In Information Hiding, IH'07, Lecture Notes in Computer Science, Saint-Malo, France, 11-13 June 2007. Springer-Verlag.