Protocolli Buyer-Seller resistenti ad attacchi di collusione per la distribuzione sicura in rete di contenuti video

Borsista: Dasara Shullani
Tutor: Alessandro Piva

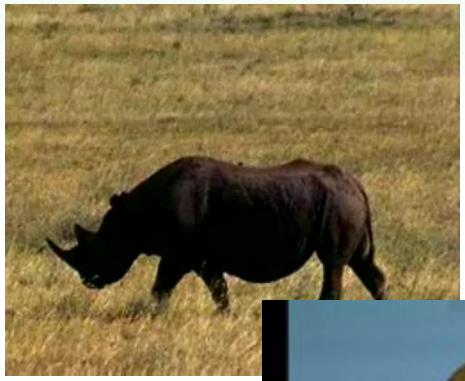
UNIVERSITÀ
DEGLI STUDI
FIRENZE
DINFO
DIPARTIMENTO DI
INGEGNERIA
DELL'INFORMAZIONE

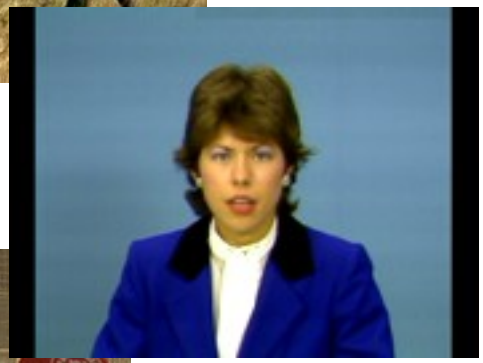
7° Borsisti Day

20/01/2016
Roma – Consortium GARR

Il progetto iniziale

- Studiare gli standard di compressione video
- Sfruttare la marchiatura digitale ai fini di proteggere i contenuti video
- Progettare un algoritmo di marchiatura robusto a manipolazioni
- Fornire un implementazione scalabile





L'attività di ricerca

- **Trimestre I** — Maggio 2015
  (a) Codec video
  (b) H.264 vs H.265
  (c) Analisi di percettività
- **Trimestre II** — Agosto 2015
  (a) Strumenti di analisi
  (b) Intra saliency H.264
- **Trimestre III** — Novembre 2015
  (a) Intra saliency H.265
  (b) Algoritmo di watermarking
  (c) Test di robustezza
- **Trimestre IV** — Febbraio 2016
  (a) Inter saliency H.265
  (b) Algoritmo completo

Codec video

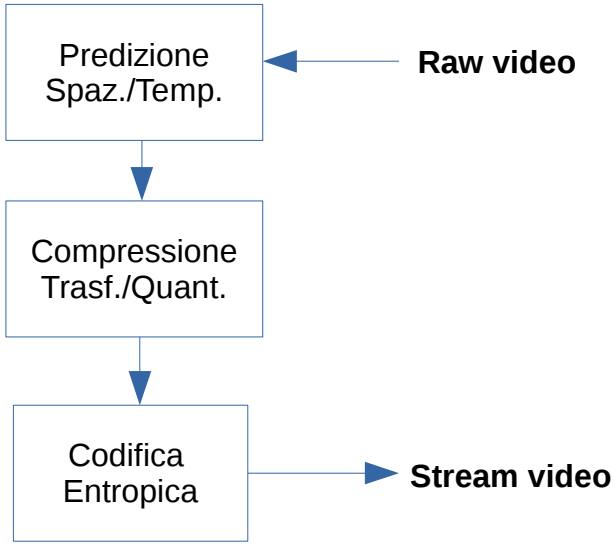
video HD di 10 minuti occupa

~42 GB

Header	Body		
Metadati	Video stream .h265	Audio stream .aac	...

AVI, MP4, MKV, ...

H.264, H.265, VP8, ...



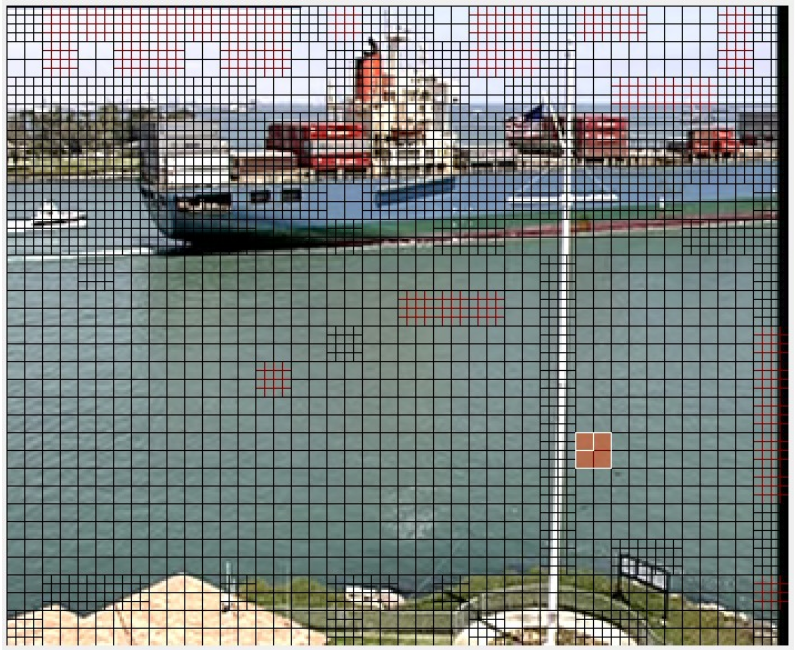
Borse di Studio
Orio Carlini
Consortium GARR

H.264 vs H.265

UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

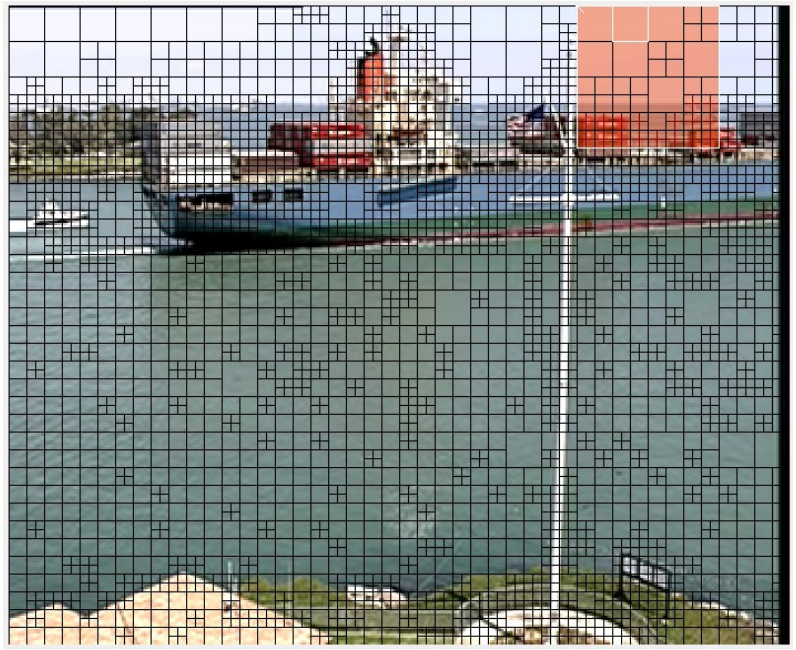
Borse di Studio Orio Carlini Consortium GARR

H.264 vs H.265



H.264/MPEG-4 Part 10 o **AVC**

- 2003 stesura della prima versione
- Difussissimo sul web e std Blu-Ray Disc
- Analisi a macroblocchi di dimensione 16x16 px



H.265/MPEG-H Part 2 o **HEVC**

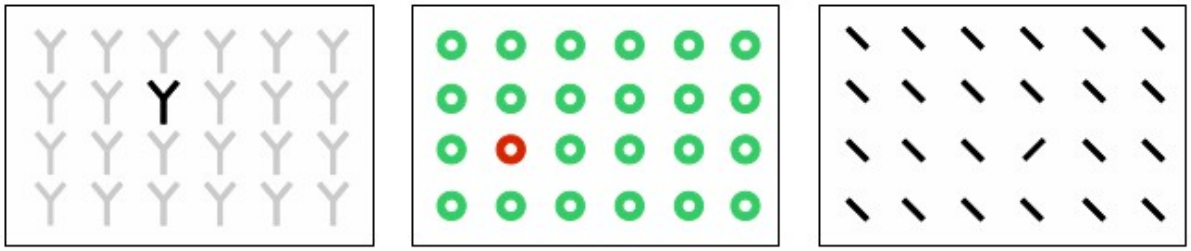
- 2013 stesura della prima versione
- Raddoppia rapporto di compressione rispetto a H.264, e supporta ultra definizione fino a 8K
- Analisi del frame in Coding Unit da 64x64 px

UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Analisi di percettività

La salienza:
un oggetto si definisce visivamente saliente se si distingue visivamente dal suo vicinato catturando l'attenzione dell'occhio umano.

In letteratura la percettività si analizza tipicamente tramite maschere di varianza ottenute nel dominio spaziale.



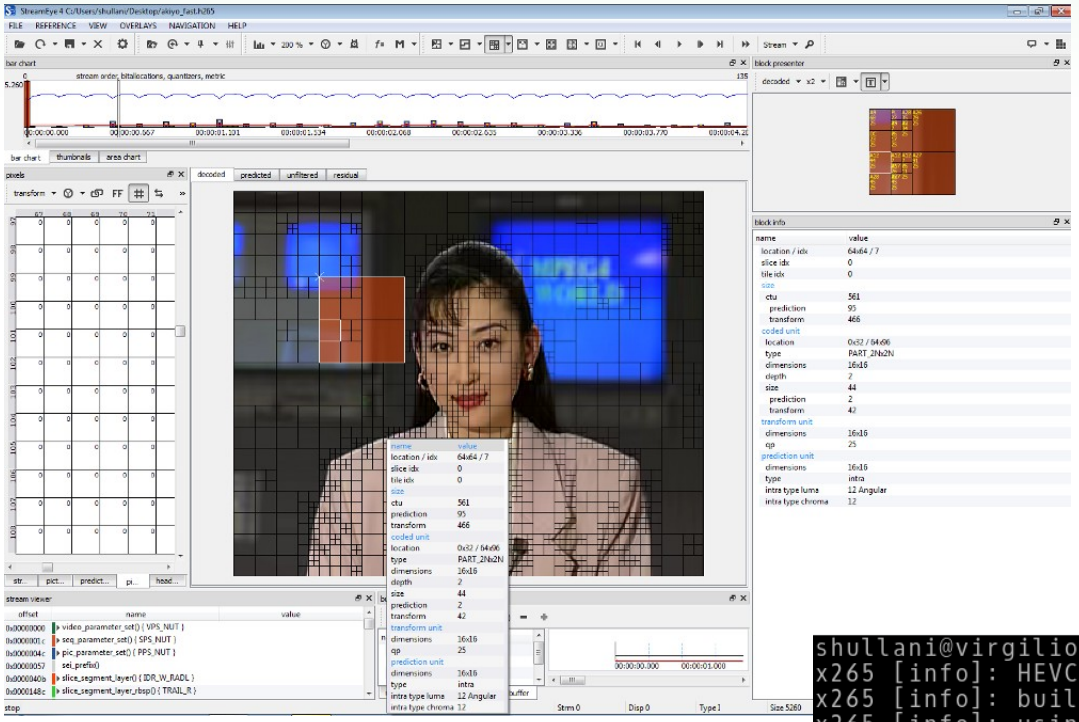
SOLO NEL DOMINIO COMPRESSO

In H.265:
- Intra frame – modi, residui e partizionamento
- Inter frame – vettori di moto, residui e partizionamento

L'attività di ricerca

- **Trimestre I** — Maggio 2015
  (a) Codec video
  (b) H.264 vs H.265
  (c) Analisi di percettività
- **Trimestre II** — Agosto 2015
  (a) Strumenti di analisi
  (b) Intra saliency H.264
- **Trimestre III** — Novembre 2015
  (a) Intra saliency H.265
  (b) Algoritmo di watermarking
  (c) Test di robustezza
- **Trimestre IV** — Febbraio 2016
  (a) Inter saliency H.265
  (b) Algoritmo completo

Strumenti di analisi



FFMPEG e x265

- Licenza GPL
- Disponibile su molteplici piattaforme
- Codice sorgente a disposizione

StreamEye v4

- GUI intuitiva
- Proprietà di Elecard, in licenza a 2000 euro
- Microsoft Windows
- Assenza di command line
- Customer care e documentazione quasi assente

X265

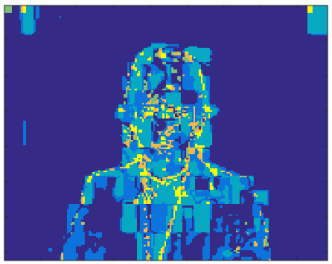
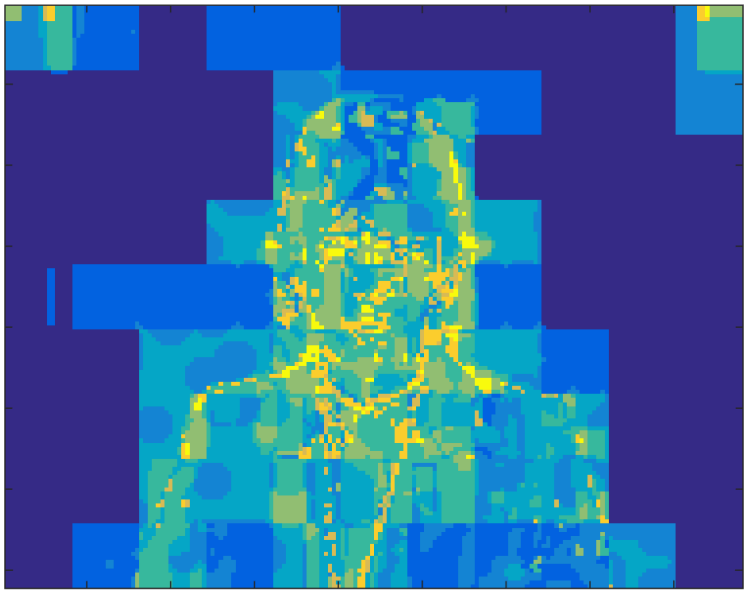
```
shullani@virgilio:~/Scrivania$ x265 --version
x265 [info]: HEVC encoder version 1.6+185-dd456de98c23
x265 [info]: build info [Linux][GCC 4.8.2][64 bit] 8bpp
x265 [info]: using cpu capabilities: MMX2 SSE2Fast SSSE3 SSE4.2 AVX
```

FFMPEG

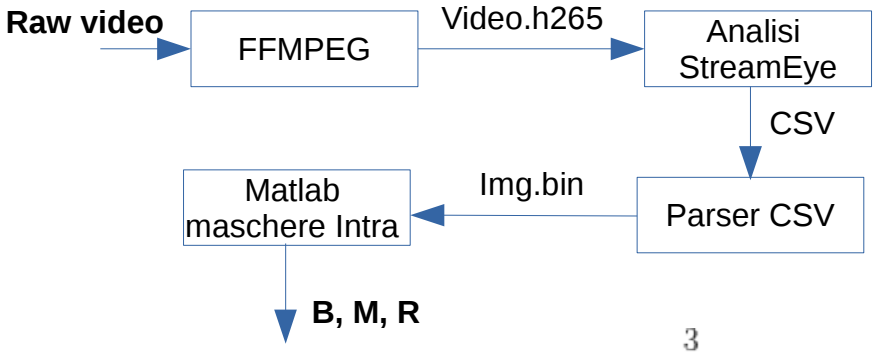
```
shullani@virgilio:~/Scrivania$ ffmpeg -version
ffmpeg version N-77455-g4707497 Copyright (c) 2000-2015 the FFmpeg developers
built with gcc 4.8 (Ubuntu 4.8.4-2ubuntu1~14.04)
configuration: --extra-libs=-ldl --prefix=/opt/ffmpeg --mandir=/usr/share/man --enable-avresampl
e --disable-debug --enable-nonfree --enable-gpl --enable-version3 --enable-libopencore-amrnb --e
nable-libopencore-amrwb --disable-decoder=amrnb --disable-decoder=amrwb --enable-libpulse --enab
le-libdcadec --enable-libfreetype --enable-libx264 --enable-libx265 --enable-libfdk-aac --enable
-libvorbis --enable-libmp3lame --enable-libopus --enable-libvpx --enable-libspeex --enable-libas
s --enable-avisynth --enable-libsoxr --enable-libxvid --enable-libvo-aacenc --enable-libvidstab
libavutil      55. 11.100 / 55. 11.100
libavcodec     57. 20.100 / 57. 20.100
libavformat    57. 20.100 / 57. 20.100
libavdevice    57.  0.100 / 57.  0.100
libavfilter     6. 21.101 /  6. 21.101
libavresample   3.  0.  0 /  3.  0.  0
libswscale      4.  0.100 /  4.  0.100
libswresample   2.  0.101 /  2.  0.101
libpostproc    54.  0.100 / 54.  0.100
```

Intra saliency H.264



- Mappa dei blocchi – 3 livelli di suddivisione
- Mappa dei modi – 8 direzioni angolari di predizione spaziale
- Mappa dei residui – differenze con la predizione spaziale dei modi



$$I_{mask} = w_b \cdot B_{mask} + w_m \cdot M_{mask} + \sum_{i=1}^{3} w_i \cdot R^i_{mask}$$

L'attività di ricerca

- **Trimestre I**
  (a) Codec video
  (b) H.264 vs H.265
  (c) Analisi di percettività

- **Trimestre II**
  (a) Strumenti di analisi
  (b) Intra saliency H.264

- **Trimestre III**
  (a) Intra saliency H.265
  (b) Algoritmo di watermarking
  (c) Test di robustezza

- **Trimestre IV**
  (a) Inter saliency H.265
  (b) Algoritmo completo

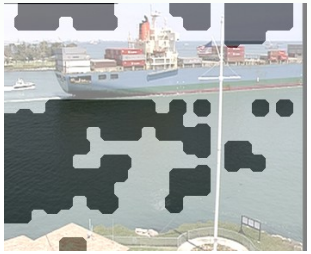
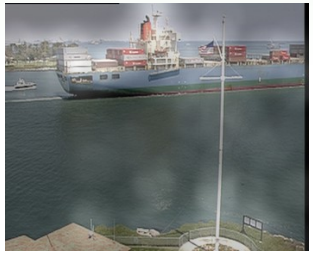
Maggio 2015

Agosto 2015

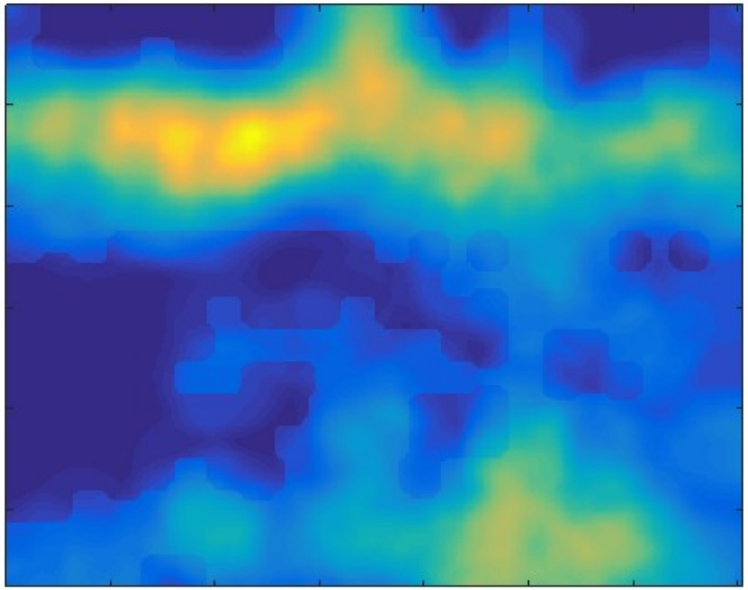
Novembre 2015

Febbraio 2016

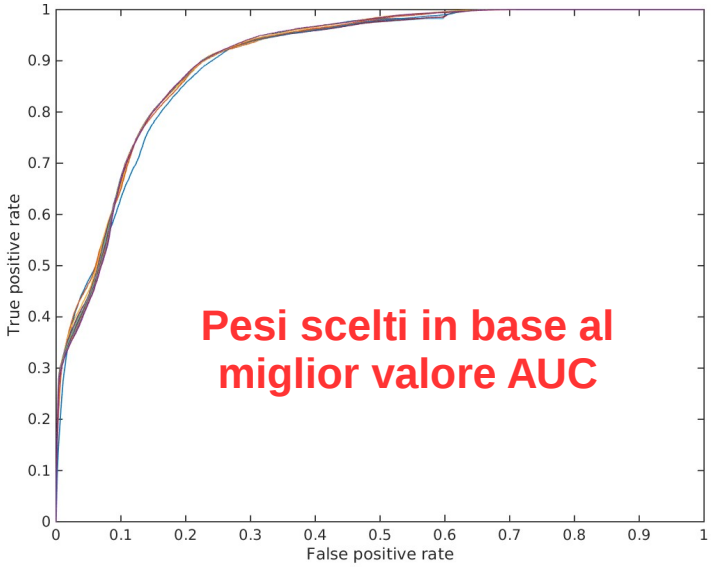
Intra saliency H.265


- Mappa dei blocchi – 5 livelli di suddivisione da 64x64 a 4x4
- Mappa dei modi – 36 direzioni angolari di predizione spaziale
- Mappa dei residui – differenze con la predizione spaziale dei modi



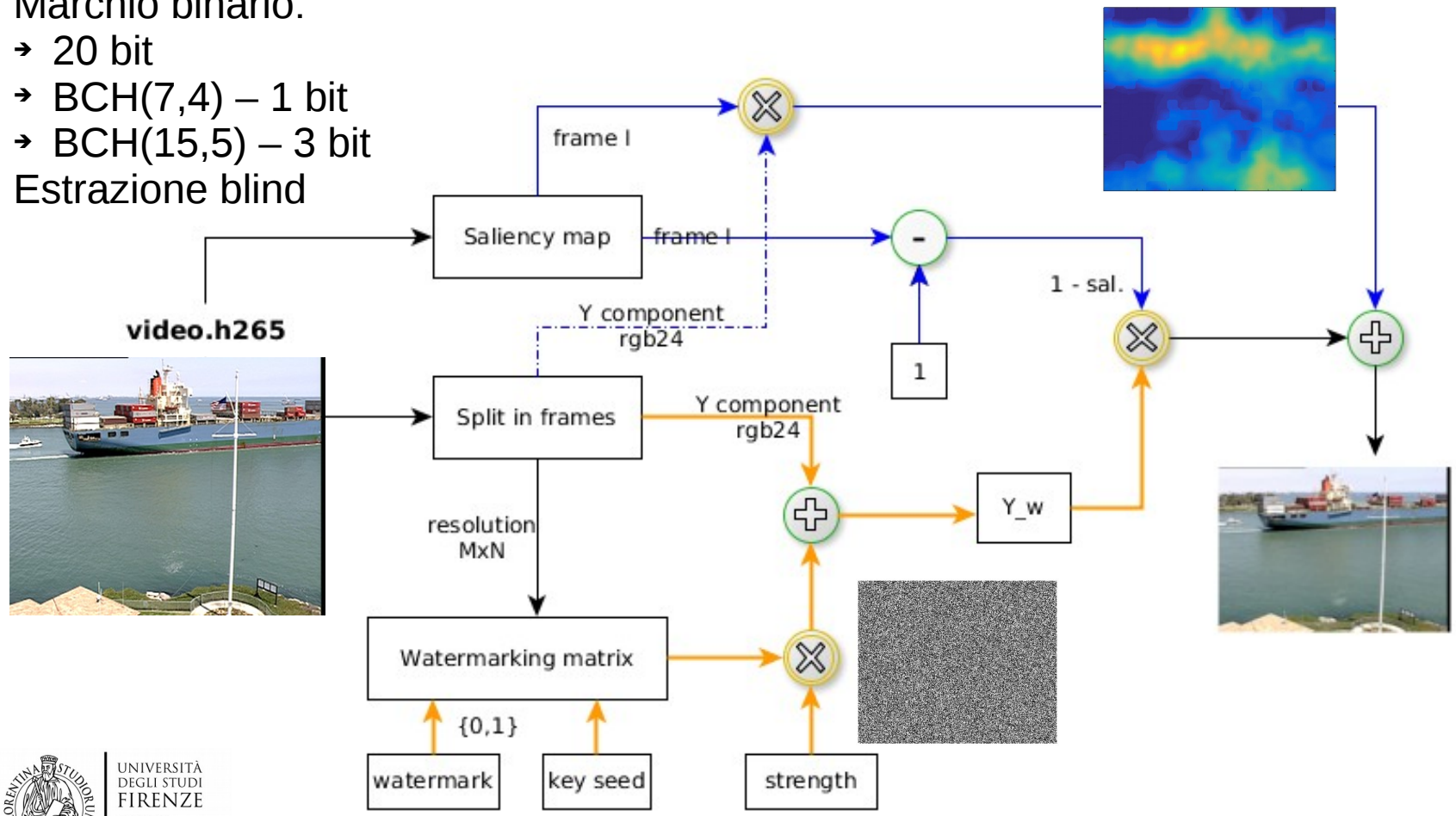
$$I_{mask} = w_b \cdot B_{mask} + w_m \cdot M_{mask} + \sum_{i=1}^{3} w_i \cdot R^i_{mask}$$



Pesi scelti in base al miglior valore AUC

Algoritmo di watermarking

- Approccio spaziale SSP
- Manipolazione della componente di luminanza di ciascun frame
- Marchio binario:
  - 20 bit
  - BCH(7,4) – 1 bit
  - BCH(15,5) – 3 bit
- Estrazione blind




B20, S=5


BCH(7,4), S=3

Test di robustezza

- Analisi di robustezza media eseguita su 11 video provenienti da dataset MIT con risoluzione full HD
- Transcodifica e ricodifica realizzate tramite FFMPEG
- Preset – da ultrafast a placebo con fattore di quantizzazione di default 23

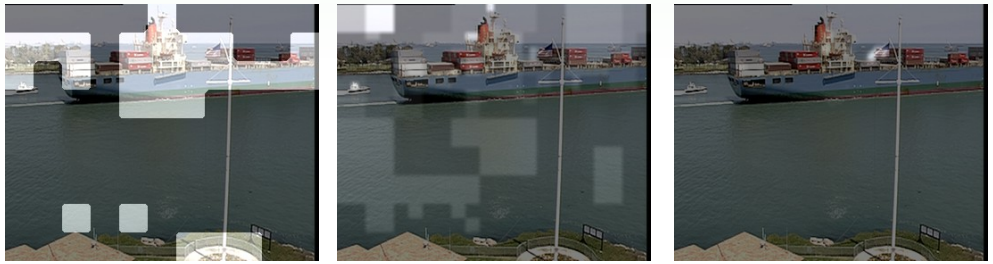
B20, S=5 PSNR=40dB	H.264 transcodifica	H.265 ricodifica	
#bit errati estratti	< 1 bit	< 1 bit	Qp – 10, 20, 30
	~ 5 bit	~ 6 bit	Qp – 40, 50
	0 bit	< 1 bit	Preset

BCH(7,4) S=3 PSNR=44dB	H.264 transcodifica	H.265 ricodifica	
#bit errati estratti	0 bit	0 bit	Qp – 10, 20, 30
	< 1 bit	< 1 bit	Qp – 40, 50
	0 bit	0 bit	Preset

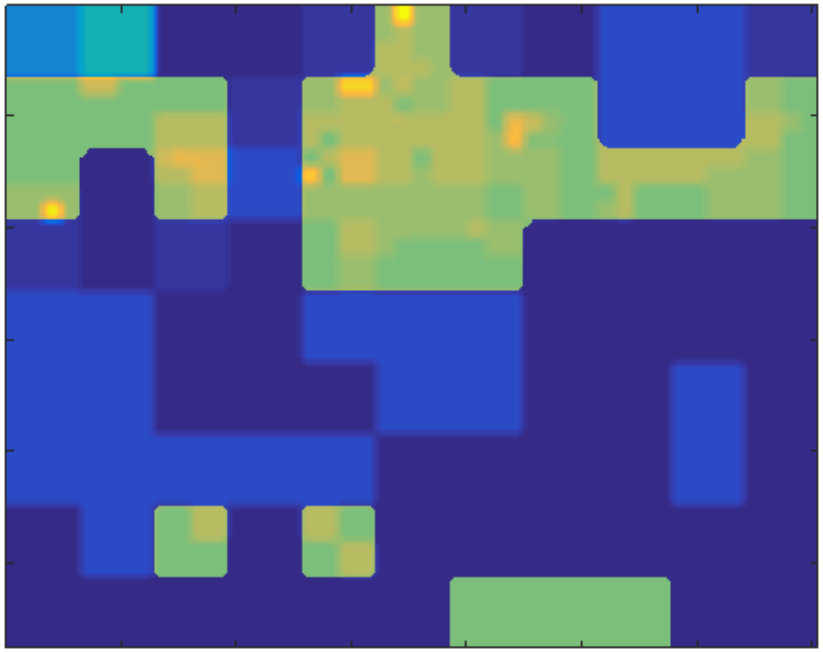
L'attività di ricerca

- **Trimestre I** — Maggio 2015
  (a) Codec video
  (b) H.264 vs H.265
  (c) Analisi di percettività
- **Trimestre II** — Agosto 2015
  (a) Strumenti di analisi
  (b) Intra saliency H.264
- **Trimestre III** — Novembre 2015
  (a) Intra saliency H.265
  (b) Algoritmo di watermarking
  (c) Test di robustezza
- **Trimestre IV** — Febbraio 2016
  (a) Inter saliency H.265
  (b) Algoritmo completo

Inter saliency H.265



- Mappa dei blocchi
- Mappa dei MV – intensità dei vettori di moto
- Mappa dei residui – differenze con la predizione temporale dei vettori di moto



- Maschera inter ottenuta pesando opportunamente le tre mappe inter
- La scelta dei pesi necessita di ulteriore tuning ma tiene in considerazione il SSIM index con riferimento al frame originale

Borse di Studio Orio Carlini Consortium GARR

Algoritmo completo

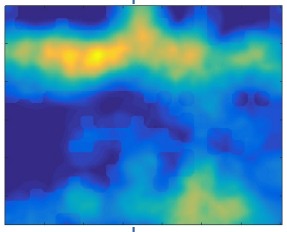
FFMPEG compressione

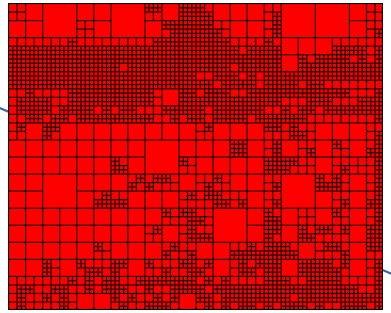
```
Input #0, yuv4mpegpipe, from 'container_cif.y4m':
  Duration: 00:00:10.01, start: 0.000000, bitrate: 36460 kb/s
    Stream #0:0: Video: rawvideo (I420 / 0x30323449), yuv420p, 352x288, SA
3, 29.97 fps, 29.97 tbr, 29.97 tbn, 29.97 tbc
x265 [info]: HEVC encoder version 1.8+1-5dcc9d3a928c400b
x265 [info]: build info [Linux][GCC 5.2.1][64 bit] 8bit
x265 [info]: using cpu capabilities: MMX2 SSE2Fast SSSE3 SSE4.1 Cache64
x265 [info]: Main profile, Level-2 (Main tier)
x265 [info]: Thread pool created using 2 threads
x265 [info]: frame threads / pool features       : 1 / wpp(5 rows)
x265 [info]: Coding QT: max CU size, min CU size : 64 / 8
x265 [info]: Residual QT: max TU size, max depth : 32 / 1 inter / 1 intra
x265 [info]: ME / range / subpel / merge         : hex / 57 / 2 / 2
x265 [info]: Keyframe min / max / scenecut       : 25 / 250 / 40
x265 [info]: Lookahead / bframes / badapt        : 20 / 4 / 2
x265 [info]: b-pyramid / weightp / weightb       : 1 / 1 / 0
x265 [info]: References / ref-limit  cu / depth  : 3 / 0 / 0
x265 [info]: AQ: mode / str / qg-size / cu-tree  : 1 / 1.0 / 32 / 1
x265 [info]: Rate Control / qCompress            : CRF-5.0 / 0.60
x265 [info]: tools: rd=3 psy-rd=0.30 signhide tmvp strong-intra-smoothing
x265 [info]: tools: deblock sao
Output #0, rawvideo, to 'container_crf5.h265':
  Metadata:
    encoder         : Lavf56.40.101
    Stream #0:0: Video: hevc (libx265), yuv420p, 352x288 [SAR 128:117 DAR
.97 fps, 29.97 tbn, 29.97 tbc
    Metadata:
      encoder         : Lavc56.60.100 libx265
```

Analisi StreamEye

	A	B
1	name	value
2	cu location	0x0
3	cu slice\tile idx	0\0
4	cu size total\prediction\transform	14603\375\14187
5	cu type\location\dimension\depth	PART_2Nx2N\0x0\8x8\3
6	cu size total\prediction\transform	229\6\223
7	tu dimensions\qp	8x8\6
8	pu intra dimension\luma_type\chroma_type	8x8\0 Planar\34
9	tu dimensions\qp	8x8\6
10	pu intra dimension\luma_type\chroma_type	8x8\8 Angular\0
11	tu dimensions\qp	16x16\6
12	pu intra dimension\luma_type\chroma_type	16x16\0 Planar\34
13	tu dimensions\qp	8x8\6
14	pu intra dimension\luma_type\chroma_type	8x8\11 Angular\1
15	tu dimensions\qp	8x8\6
16	pu intra dimension\luma_type\chroma_type	8x8\0 Planar\10
17	tu dimensions\qp	8x8\6
18	pu intra dimension\luma_type\chroma_type	8x8\0 Planar\34
19	tu dimensions\qp	8x8\6
20	pu intra dimension\luma_type\chroma_type	8x8\2 Angular\0
21	tu dimensions\qp	8x8\6
22	pu intra dimension\luma_type\chroma_type	8x8\14 Angular\0
23	tu dimensions\qp	8x8\6
24	pu intra dimension\luma_type\chroma_type	8x8\8 Angular\1
25	tu dimensions\qp	8x8\6
26	pu intra dimension\luma_type\chroma_type	8x8\0 Planar\10
27	tu dimensions\qp	8x8\6

Matlab maschere Intra/Inter



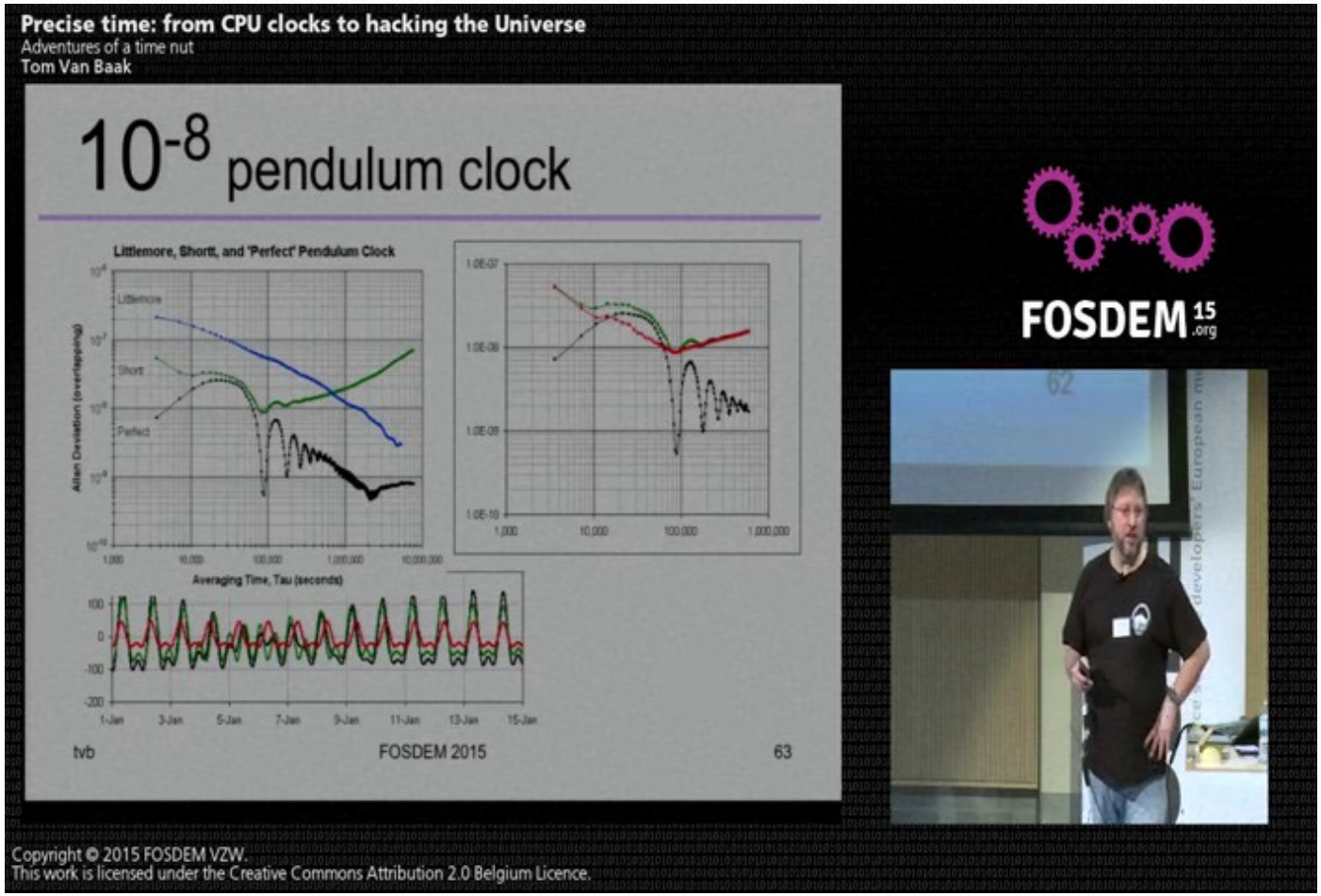


Parser StreamEye

Matlab algoritmo di marchiatura

UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Un esempio


Precise time: from CPU clocks to hacking the Universe
Adventures of a time nut
Tom Van Baak
10-8 pendulum clock
Littlemore, Shortt, and 'Perfect' Pendulum Clock
Allan Deviation (overlapping)
Averaging Time, Tau (seconds)
tvb
FOSDEM 2015
63
FOSDEM 15 .org
Copyright © 2015 FOSDEM VZW.
This work is licensed under the Creative Commons Attribution 2.0 Belgium Licence.

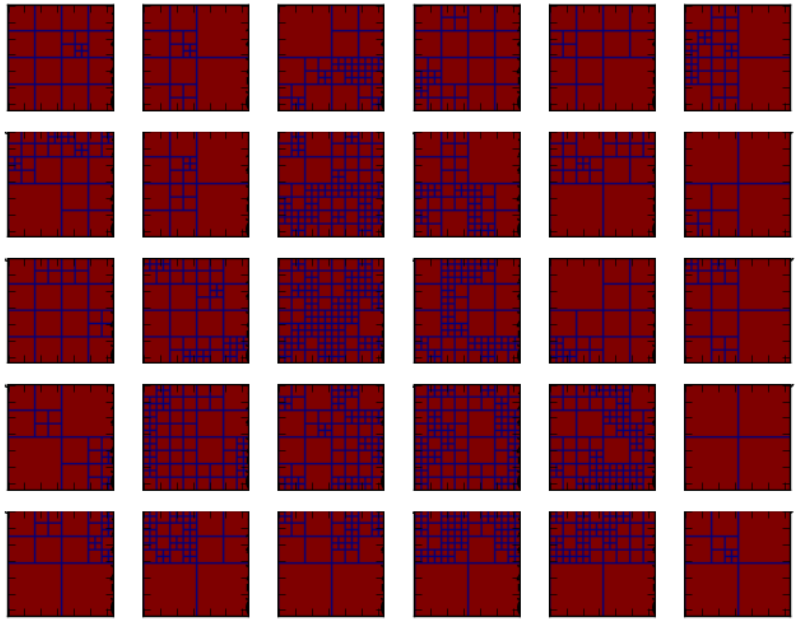
Conclusioni

- Know how in materia di H.265/H.264 codec video
- Implementato algoritmo di marchiatura che sfrutta la percettività ottenuta dalle maschere di salienza per la protezione del contenuto video
- Si riescono a nascondere in un secondo di video 100 bit utilizzando BCH(7,4) oppure 500 bit in caso di B20
- Analisi di robustezza sull'algoritmo complessivo comprendendo attacchi di compressione sia in transcodifica che ricodifica.
- tempo di elaborazione ~4H per 100 frame in fullHD

Problemi aperti

ctu	@0x23dd640	x265::CUData &
m_absIdxInCTU	0	uint32_t
m_cbf	@0x23dd718	uint8_t *[3]
m_chromaFormat	1	uint32_t
m_chromaIntraDir	36	uint8_t
m_cuAbove	0x0	x265::CUData *
m_cuAboveLeft	0x0	x265::CUData *
m_cuAboveRight	0x0	x265::CUData *
m_cuAddr	0	uint32_t
m_cuDepth	<1000 items>	uint8_t *
[0]	2	uint8_t
[1]	2	uint8_t
[2]	2	uint8_t
[3]	2	uint8_t
[4]	2	uint8_t
[5]	2	uint8_t
[6]	2	uint8_t
[7]	2	uint8_t
[8]	2	uint8_t
[9]	2	uint8_t
[10]	2	uint8_t
[11]	2	uint8_t
[12]	2	uint8_t
[13]	2	uint8_t
[14]	2	uint8_t
[15]	2	uint8_t
[16]	2	uint8_t

- Estrazione delle caratteristiche del frame fondato su software proprietario e problematico
- Applicativi Microsoft Windows dipendenti
- Approccio di marchiatura baseline che sfrutta il dominio spaziale
- La marchiatura necessita di ulteriore decodifica/codifica per poter nascondere il marchio
- Costo di eleborazione elevato



Estensioni future

Trimestre I – Studiare e modificare libx265 al fine di poter accedere alle specifiche di codifica video in maniera efficiente
Trimestre II – Algoritmo di marchiatura innovativo che opera nel dominio compresso tramite libx265 per nascondere un marchio durante la fase di codifica video, sfruttando la maschera di percettività ad oggi ottenuta
Trimestre III – Testing e conseguenti modifiche del algoritmo di marchiatura a fronte di manipolazione esterne
Trimestre IV – Adattamento dell'algoritmo ad essere scalabile e multipiattaforma

Pubblicazione del lavoro svolto
Ricerca *Scopus* <15 articoli su data hiding HEVC

Riferimenti

Riferimenti e link:

- https://media.xiph.org/video/derf/
- http://saliency.mit.edu/datasets.html
- Sze, Vivienne, Madhukar Budagavi, and Gary J. Sullivan. High Efficiency Video Coding (HEVC). Springer, 2014.
- http://www.elecard.com/en/products/professional/analysis/streameye4.html
- http://x265.org/
- https://www.ffmpeg.org/
- https://github.com/AlDanial/cloc
- https://video.fosdem.org/2015/main_track-time/

Pubblicazioni:

Bianchi, Tiziano, Alessandro Piva, and Dasara Shullani.
"Anticollusion solutions for asymmetric fingerprinting protocols based on client side embedding." EURASIP Journal on Information Security 2015.1 (2015): 1-17.

Borse di Studio
Orio Carlini
Consortium GARR

Vi ringrazio per l'attenzione!

… Domande?

UNIVERSITÀ DEGLI STUDI FIRENZE
DINFO
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE