Blind motion-compensated video watermarking

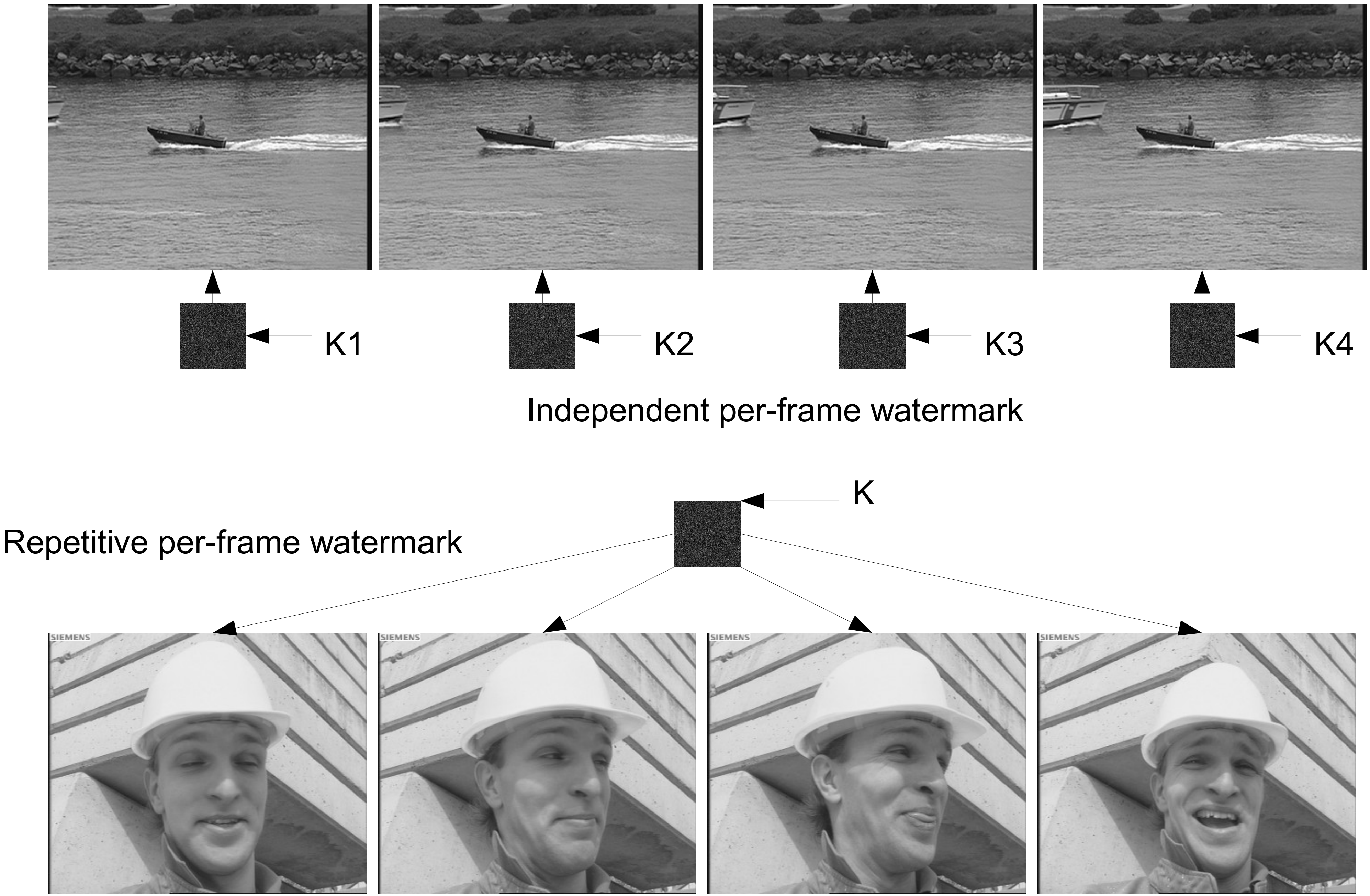
Peter Meerwald, Andreas Uhl

June 24, 2008

Outline

- Video watermarking
- Interframe Attacks
- Motion-compensation temporal filtering
- Blind MC watermarking
- Results

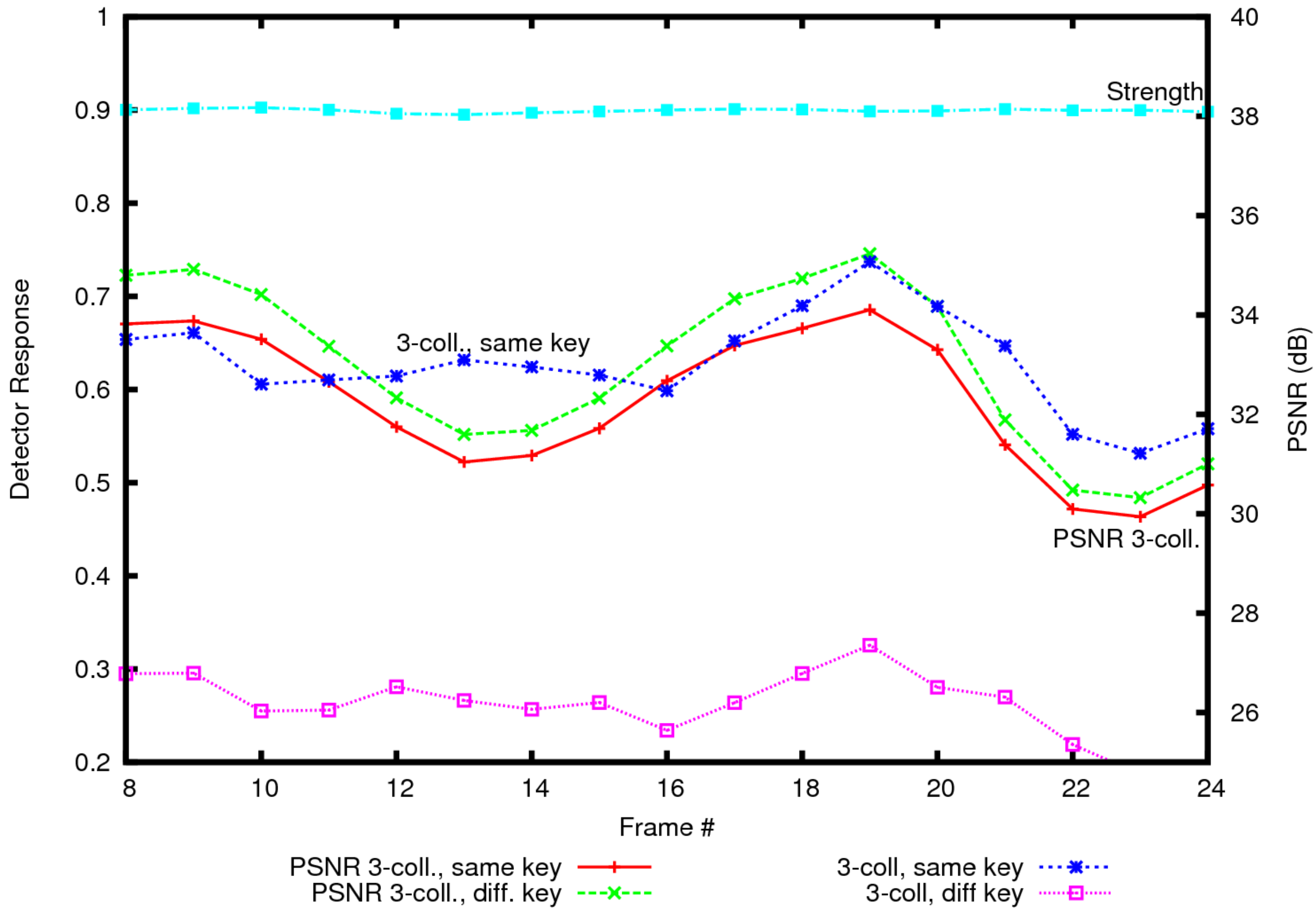
Video watermarking



Inter-frame watermark attacks

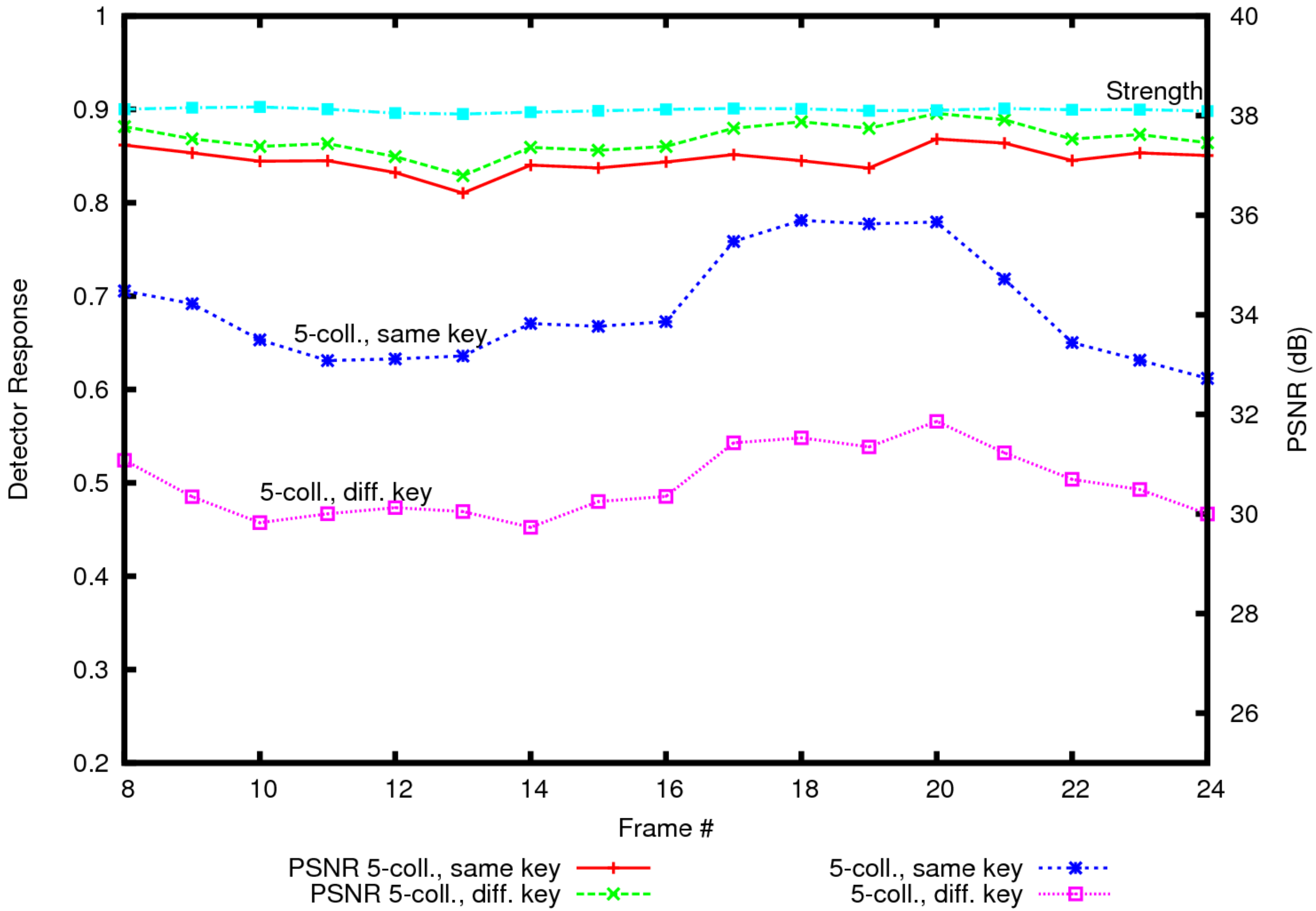
- Exploit correlation of the host signal
  - Against independent (uncorrelated) watermark
  - Frame Temporal Filtering (FTF)
  - Extension: Motion-compensated FTF
- Exploit correlation of the watermark
  - Estimate watermark from uncorrelated frames
  - Watermark Estimation and Remodulation (WER) Attack

FTF



Foreman sequence

MC-FTF



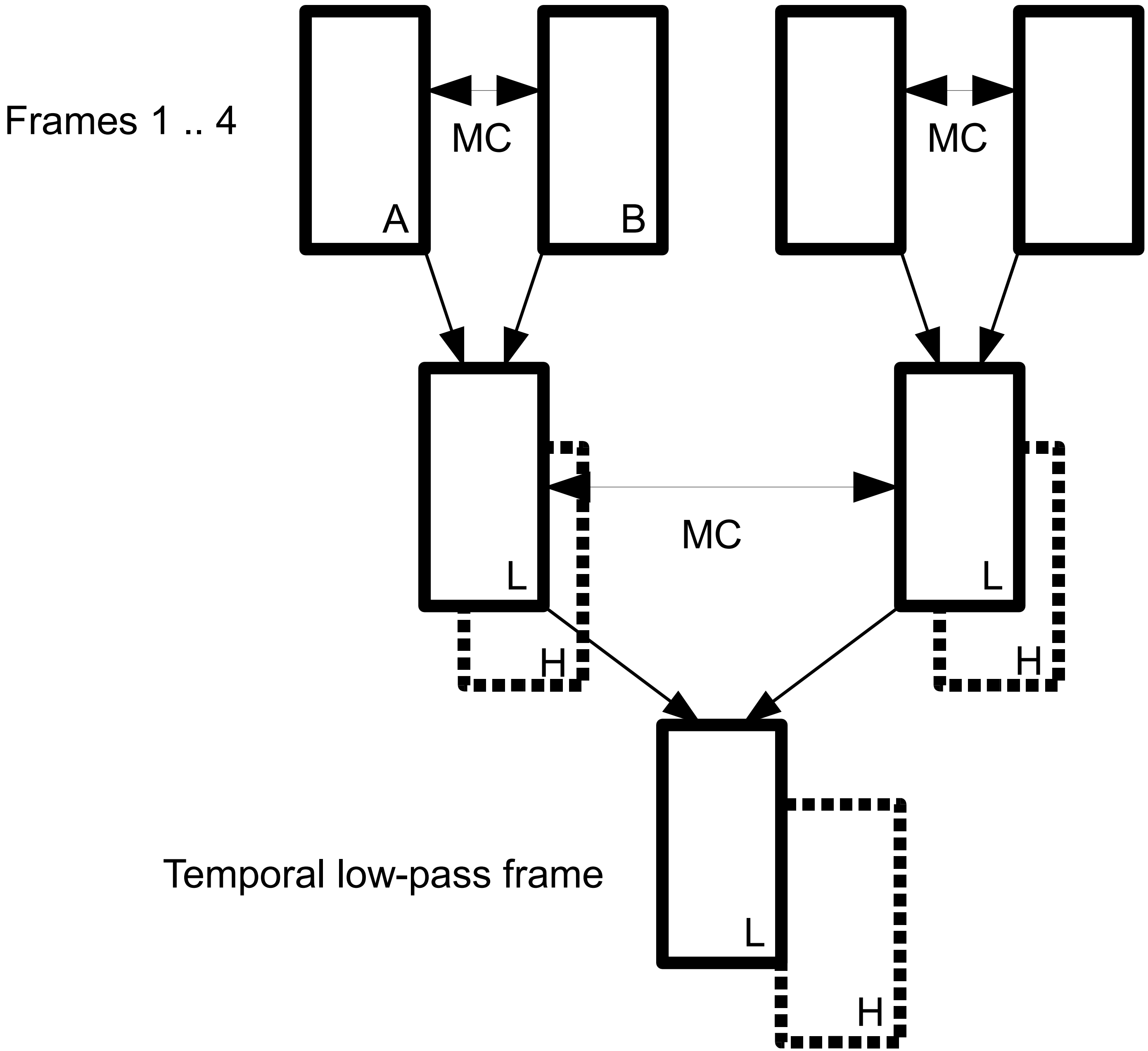
non-blind DWT watermarking scheme
MC: block size 8, search range 16

Foreman sequence

Motion-coherent watermarking

- Countermeasure: [Doerr03c]
  - Watermark of two frames should be as correlated as host signal
- Implementation choices:
  - Frame registration [Doerr04b]
  - Spatial correlation technique via anchor points [Su05a]
  - Motion-compensated temporal transform [Pankajakshan06a]

Temporal filtering



Haar Filter as Lifting Steps

Decomposition

$$H[n] = B[n] - A[n]$$

$$L[n] = A[n] + \frac{1}{2}H[n]$$

Reconstruction

$$A[n] = L[n] - \frac{1}{2}H[n]$$

$$B[n] = H[n] + A[n]$$

Motion-compensated Temporal Filtering

- Motion Estimation (ME) connects related pixels between frame A and B
- Can apply filtering along motion trajectories

Decomposition

$$H[n] = B[n] - A[M_{A\rightarrow B}(n)]$$

$$L[n] = A[n] + \frac{1}{2}H[M_{B\rightarrow A}(n)]$$

Reconstruction

$$A[n] = L[n] - \frac{1}{2}H[M_{B\rightarrow A}(n)]$$

$$B[n] = H[n] + A[M_{A\rightarrow B}(n)]$$

Temporal low-pass frames

No motion compensation

Left

Middle

Right

Haar temporal filter
CIF, first 16 frames, block size 8, search range 16

Non-blind motion-compensated watermarking

- MC-TF, 4 decomposition levels
- add additive spread-spectrum <u>watermark on temporal low-pass</u> approximation
- non-blind detector (can refer to original host signal)
  - can cancel host signal, does not interfere with detection
  - has <u>accurate motion information</u>
  - use normalized linear correlation (assume attack is AWGN)

[Pankajakshan06a]

Blind motion-compensated watermarking

- MC-TF, 4 decomposition levels
- spatial 8x8 block DCT on temporal low-pass approximation
- select 18 mid-frequency channels, rejects part of the host interference; models host with Generalized Gaussian distribution [Hernandez00a]
- estimate motion from received host signal

Experiments

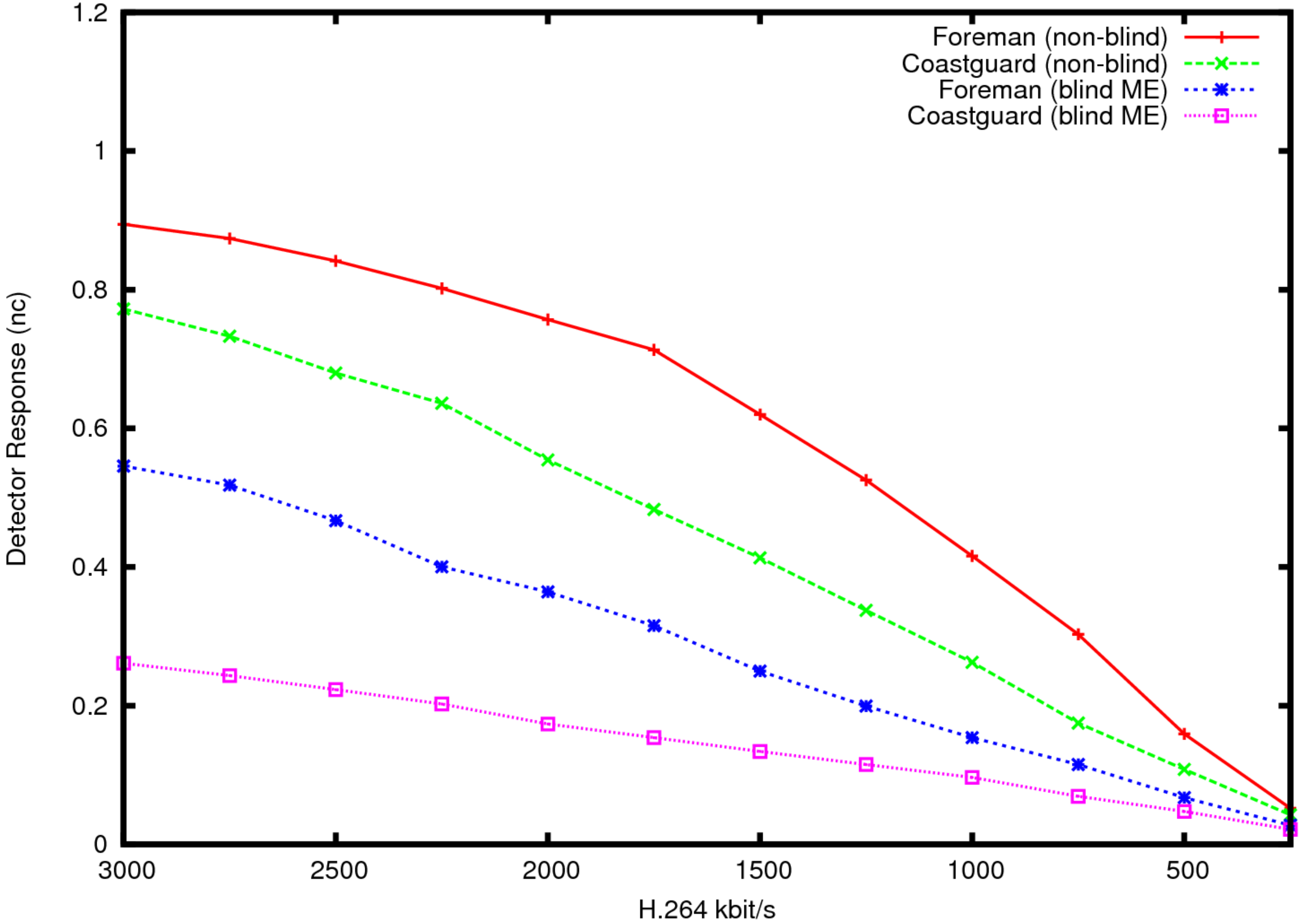
- Blind ME from watermarked video (38 dB PSNR)
- How does compression attack affect motion estimation?
  - compare blind with non-blind scheme
- Assess FTF and MC-FTF attack

Blind ME

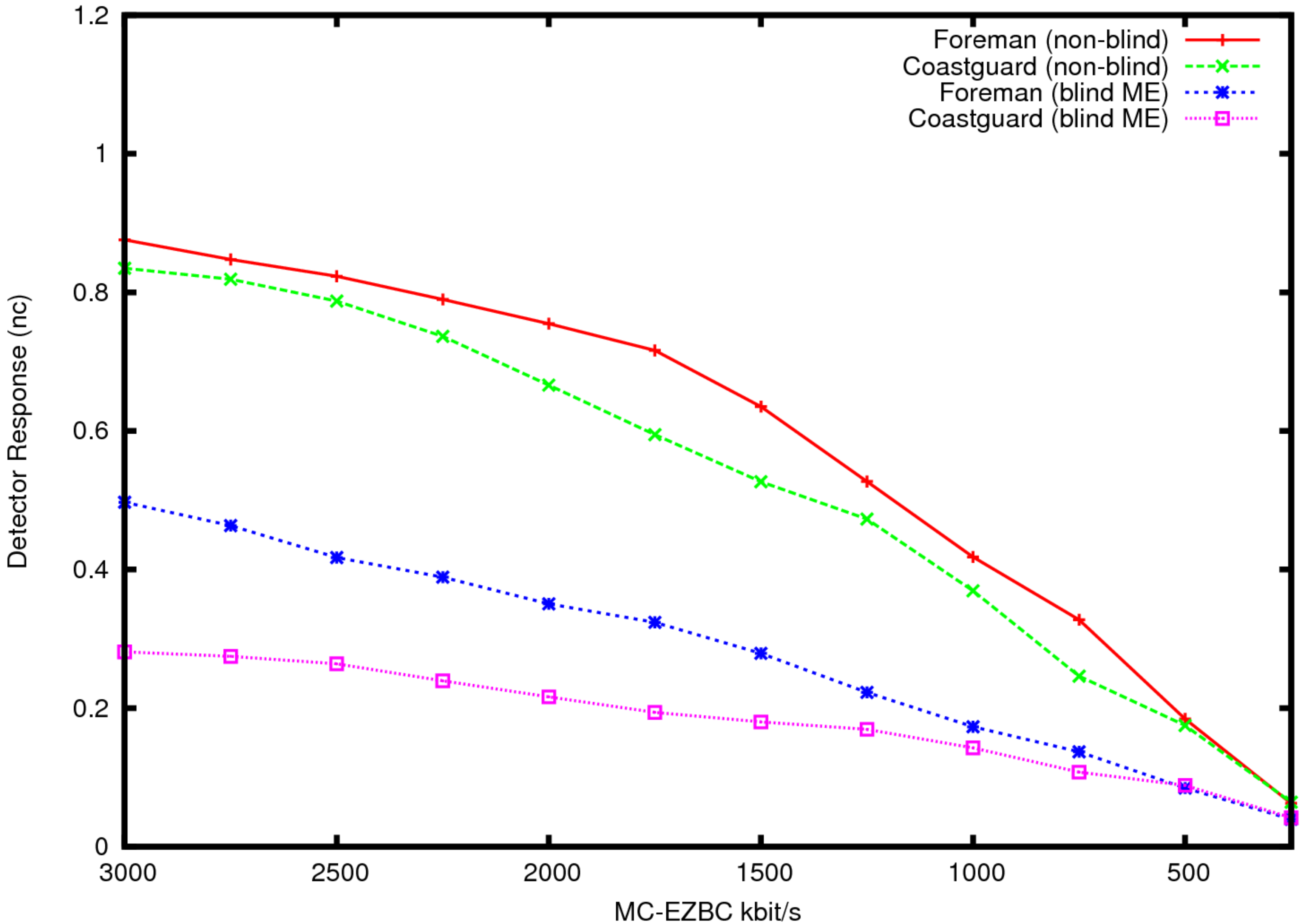
Sequence	Non blind	Blind ME			
		SR 16, L 4	SR 32, L 4	SR 16, L 3	SR 32, L 3
Foreman	1.00	0.80	0.79	0.90	0.89
Coastguard	1.00	0.48	0.45	0.63	0.60
Akiyo	1.00	0.98	0.98	0.99	0.99
Mobile	1.00	0.34	0.29	0.45	0.38
Stefan	1.00	0.47	0.47	0.64	0.61

PSNR: ~38 dB

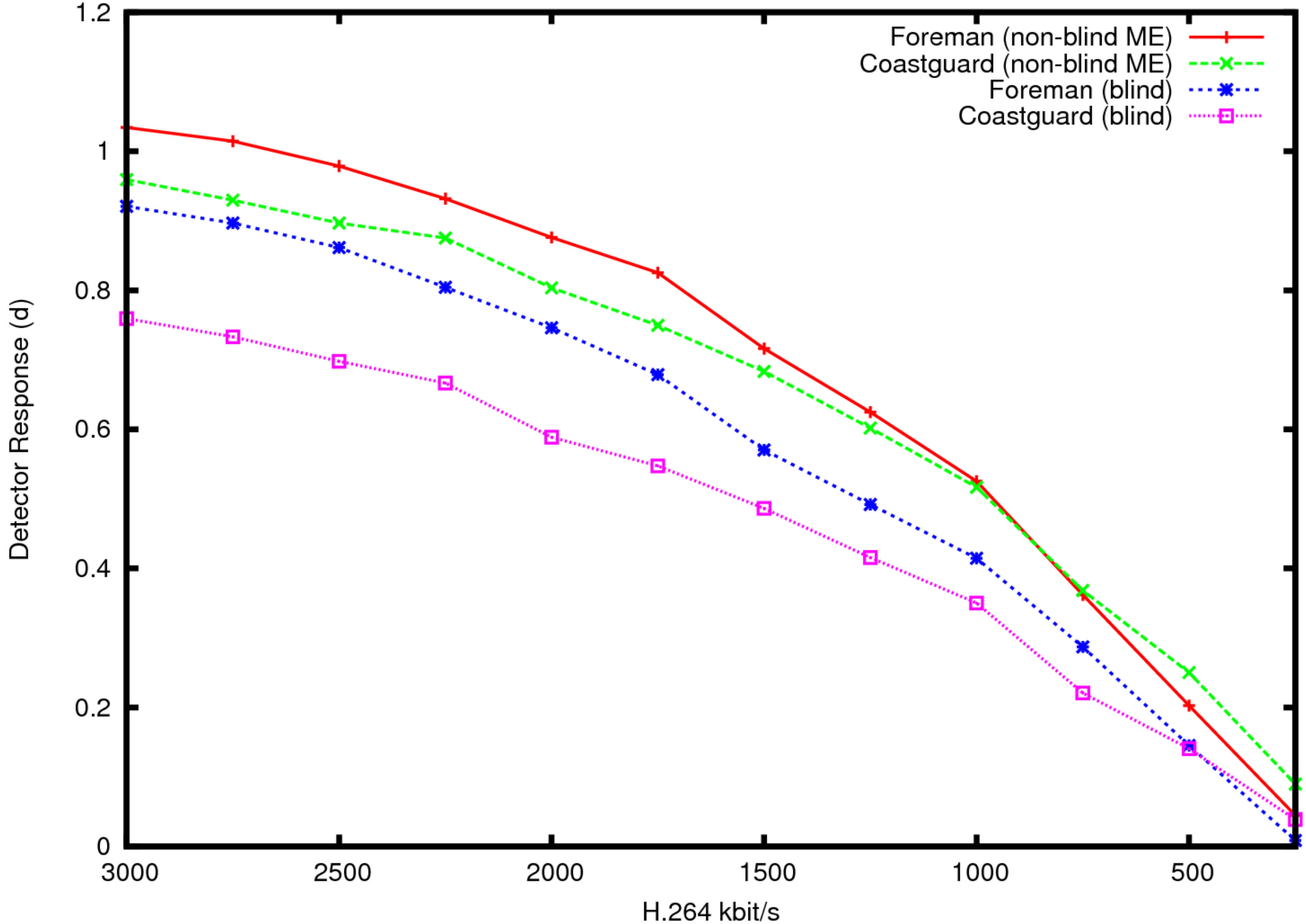
Non-blind scheme / H.264



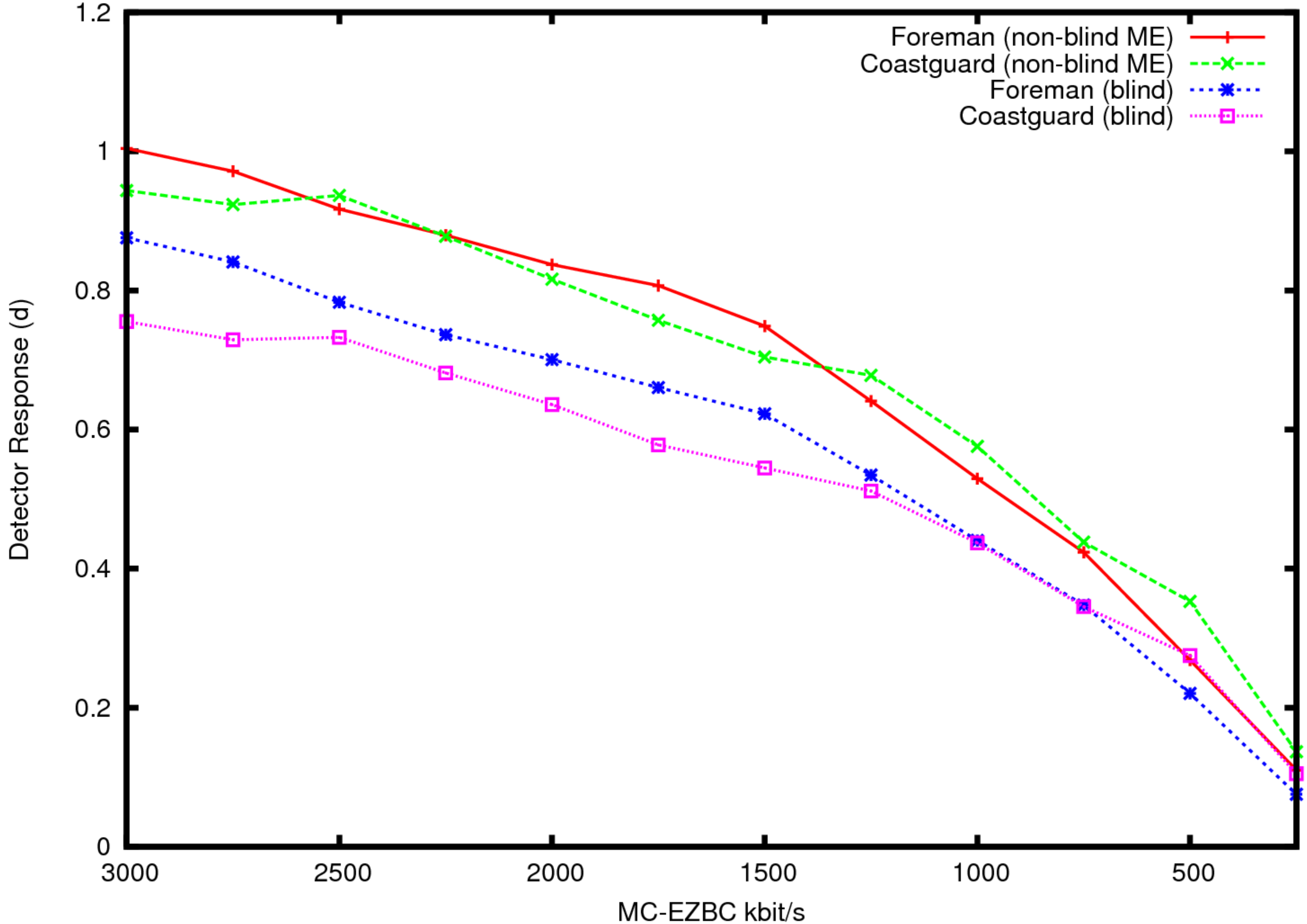
Non-blind scheme / MC-EZBC



Blind scheme / H.264



Blind scheme / MC-EZBC



MC-FTF Attack

MC-FTF Attack (window size 7)					
Repetitive WM		Independent WM		Motion-coherent WM	
PSNR (dB)	d	PSNR (dB)	d	PSNR (dB)	d
36.96	0.79	37.96	0.60	36.92	0.86
33.47	0.51	33.84	0.38	33.12	0.68
38.25	1.12	41.33	0.75	38.36	0.96
28.53	0.69	29.01	0.52	28.58	0.76
30.06	0.63	31.02	0.53	30.26	0.79

Conclusion

- Blind motion-compensated watermarking seems feasible
- Motion-coherent watermark can be detected in temporal-low pass and per-frame
- Integration with (scalable) video codecs based on MC-TF possible
- Further work
  - can motion estimation be explicitly attacked?
  - WER attack

References

- [Doerr03c] G. Doerr et al., New Intra-Video Collusion Attack Using Mosaicing, ICME'03
- [Doerr04b] G. Doerr et al., Secure Background Watermarking Based on Video Mosaicing, EI'04
- [Su05a] K. Su et al, Statistical Invisibility for Collusion-resistant Digital Video Watermarking, IEEE Tr. MM, vol. 7, n. 1, 2005
- [Pankajakshan06a] V. Pankajakshan et al., Motion-compensated inter-frame collusion attack on video watermarking and a countermeasure, IEE Proc. IS, vol. 153, n. 2, 2006
- [Hernandez00a] J. Hernandez et al., DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure, IEEE Tr. IP, vol. 9, n. 1, 2000