Feature Point-Based 3D Mesh Watermarking that Withstands the Cropping Attack

M. Montañola Sales[1], R. Darazi[1], J. Giard[1], P. Rondão Alface[2] and B. Macq[1]

[1] Univeristé Catholique de Louvain (ICTEAM)

Belgium

[2] Alcatel-Lucent Bell Labs

Belgium

Outline

- Introduction
  - Digital watermarking
  - Industrial applications
  - 3D Triangle Meshes
- State-of-the-Art
- QIM-based 3D Mesh Watermarking
  - STDM
  - Perceptual Model
- Re-synchronization with Feature Point Detection (Prongs)
- Robust 3D Watermarking Scheme with Side Information
- Conclusions

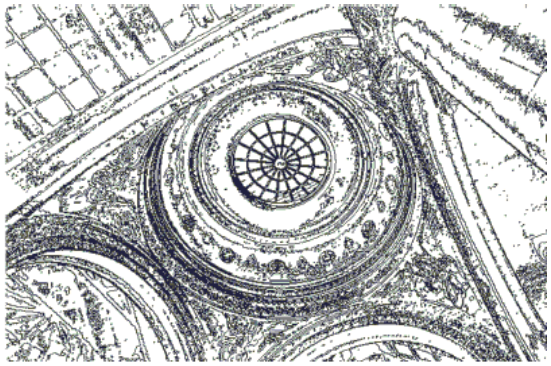
Digital Watermarking

- The robust hiding of a message within another signal (e.g. an image, a piece of music, a video, …)

Original content

Message

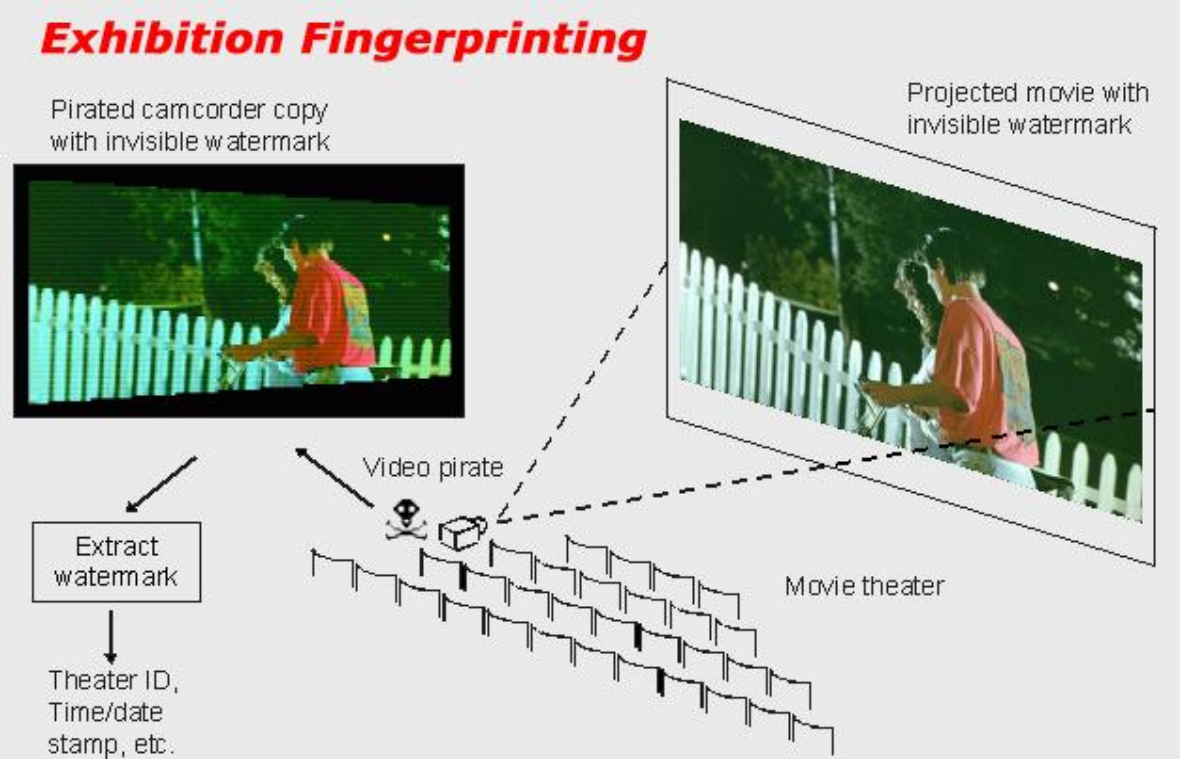
01001000 (H)
01100101 (e)
01101100 (l)
01101100 (l)
01101111 (o)



Watermarked content

Digital Watermarking

- Industrial applications
  - ***Copyright protection***
  - Authentication
  - Content monitoring
  - Content enrichment (data hiding)



Industrial applications

- Trend towards 3D content-based applications

3D videoconference

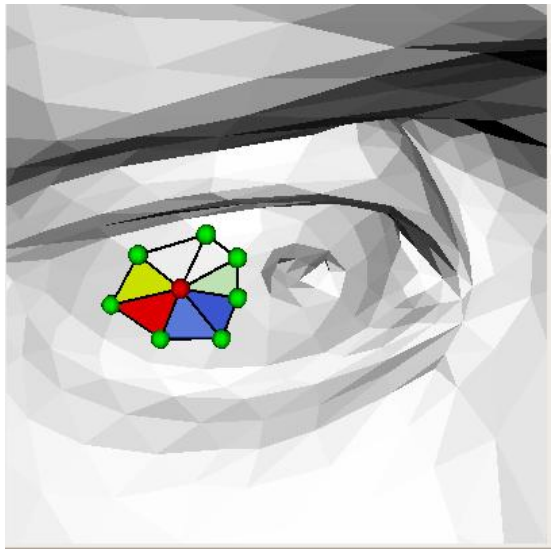
Smartphones

3D cinema

Video games

Home entertainment

3D Triangle Meshes



Geometry:

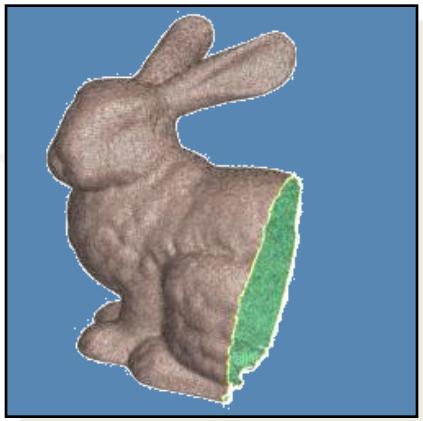
x	y	z	p_{id}
0.033	0.025	-0.067	4048
0.034	0.027	-0.068	4057
0.031	0.027	-0.067	8900

Connectivity:

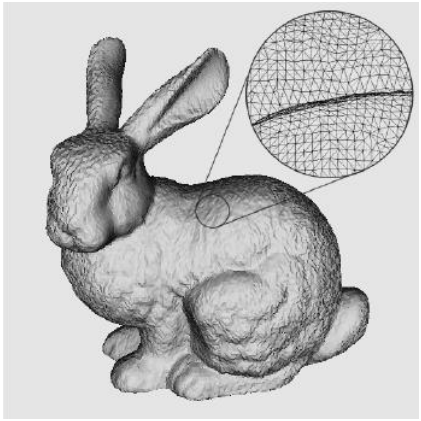
p_1	p_2	p_3	t_{id}
4048	4057	8900	12005
4057	4048	8910	12006

3D Watermarking Attacks

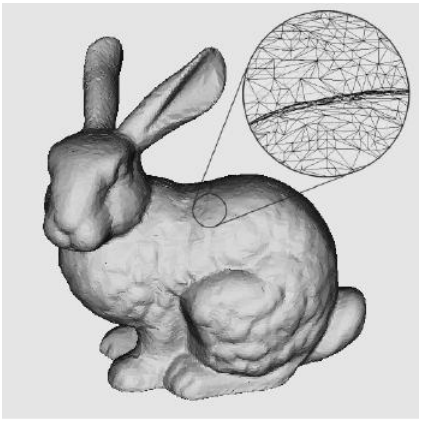
Cropping



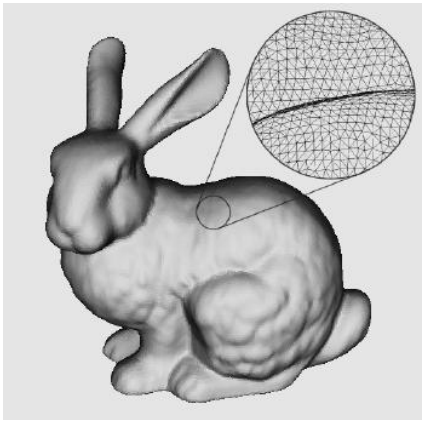
noise



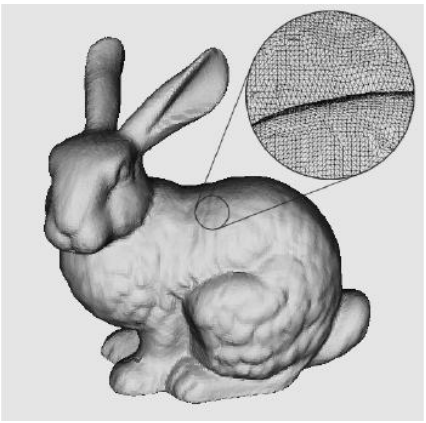
Decimation



Smoothing



Subdivision



State-of-the-Art

- Blind robust 3D watermarking techniques
  - J.W. Cho, M.S. Kim, R. Prost, H.Y. Chung, and H.Y. Jung. Robust watermarking on polygonal meshes using distribution of vertex norms. In Proc. of IWWM'05, volume LNCS 3304 of Lecture Notes in Computer Science, Siena, Italy, pages 283–293, 2005.
  - S. Zafeiriou, A. Tefas, and I. Pitas. Blind robust watermarking schemes for copyright protection of 3d mesh objects. IEEE Trans. Vis. Comput. Graph., 11(5):596–607, 2005.
  - No robust against cropping
- P. Rondão Alface. Perception and Re-Synchronization Issues for the Watermarking of 3D Shapes. PhD thesis, Université Catholique de Louvain, 2006.

- Combination: STDM + Re-synchronization with Feature Point Detection

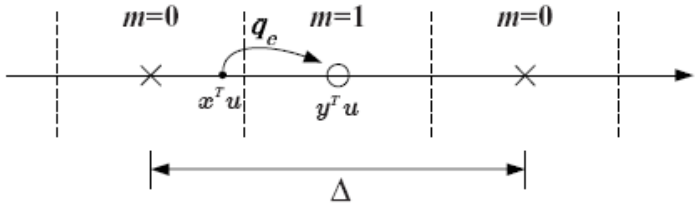
QIM-based 3D Watermarking

R. Darazi, R. Hu and B. Macq. *Applying Spread Transform Dither Modulation for 3D-Mesh Watermarking by using Perceptual Models*. Communications and Remote Sensing laboratory, Université Catholique de Louvain, 2010.

- **QIM**
  - Host data **x** quantized by scalar, uniform quantizers using DM
  - Δ controls the **x** signal alteration
  - High robustness to noising and smoothing

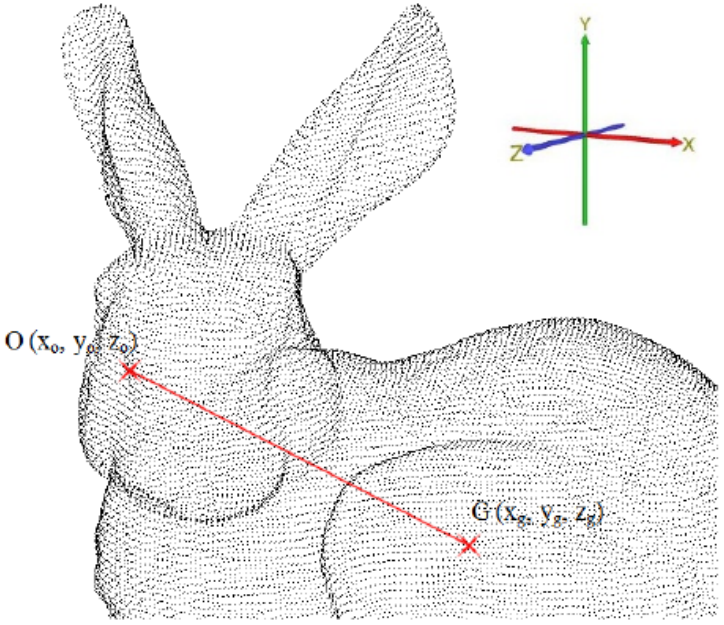
$$Q_i(\boldsymbol{x}) = Q_\Delta(\boldsymbol{x} - \boldsymbol{d}_i) + \boldsymbol{d}_i, \quad \forall i \in \{0,1\}$$

$$d_0 = \frac{-\Delta}{4}, \quad d_1 = \frac{\Delta}{4}$$



- **STDM**
  - Random transformation by projecting **x** onto a random vector, $\boldsymbol{u}$

- High resistance to noising and smoothing
- Robust against RST attacks
- Limitations:
  - No resistance to cropping, re-ordering, re-sampling attacks
  - Extraction depends on the points and order used in the embedding
  - Cropping makes impossible the recover of the center of gravity (cog)



Perceptual Model

R. Darazi, R. Hu and B. Macq. *Applying Spread Transform Dither Modulation for 3D-Mesh Watermarking by using Perceptual Models*. Communications and Remote Sensing laboratory, Université Catholique de Louvain, 2010.

- Improve perceptual quality

$$[p'] = [v][p]$$

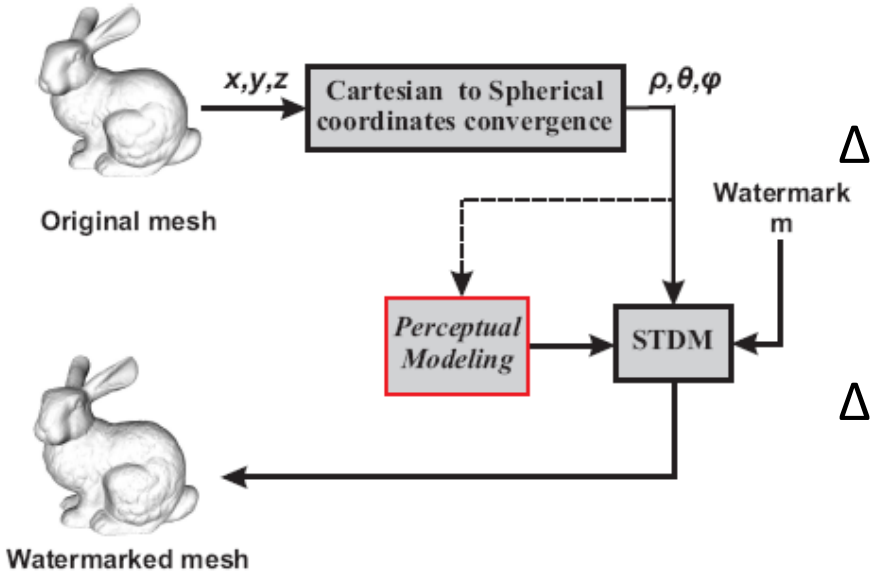
$$\begin{bmatrix} v(1) \\ v(2) \\ . \\ . \\ v(n) \end{bmatrix} = \begin{bmatrix} Curvature(P_1) * Roughness(P_1) \\ Curvature(P_2) * Roughness(P_2) \\ . \\ . \\ Curvature(P_n) * Roughness(P_n) \end{bmatrix}$$

  - ***p*** is modulated with a masking vector $\boldsymbol{v}$
- Curvature:

$$Curvature(P_0) = \left| \sum_{P \epsilon V(P_0)} \frac{\overline{PP_0}\, \overline{N_{P0}}}{|\overline{PP_0}|} \right|$$

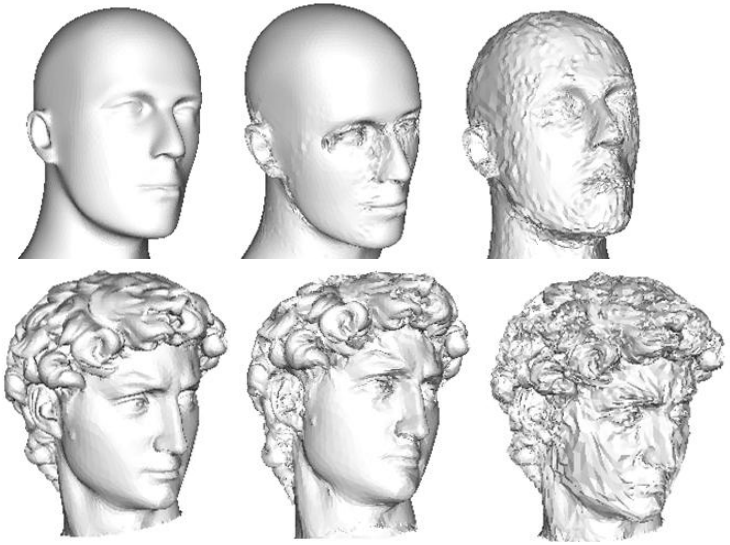
- Roughness:

$$Roughness(P_0) = Variance_{P \epsilon V(P_0)}(|\overline{PP_c}|)$$



Δ = 0.1

Δ = 0.3

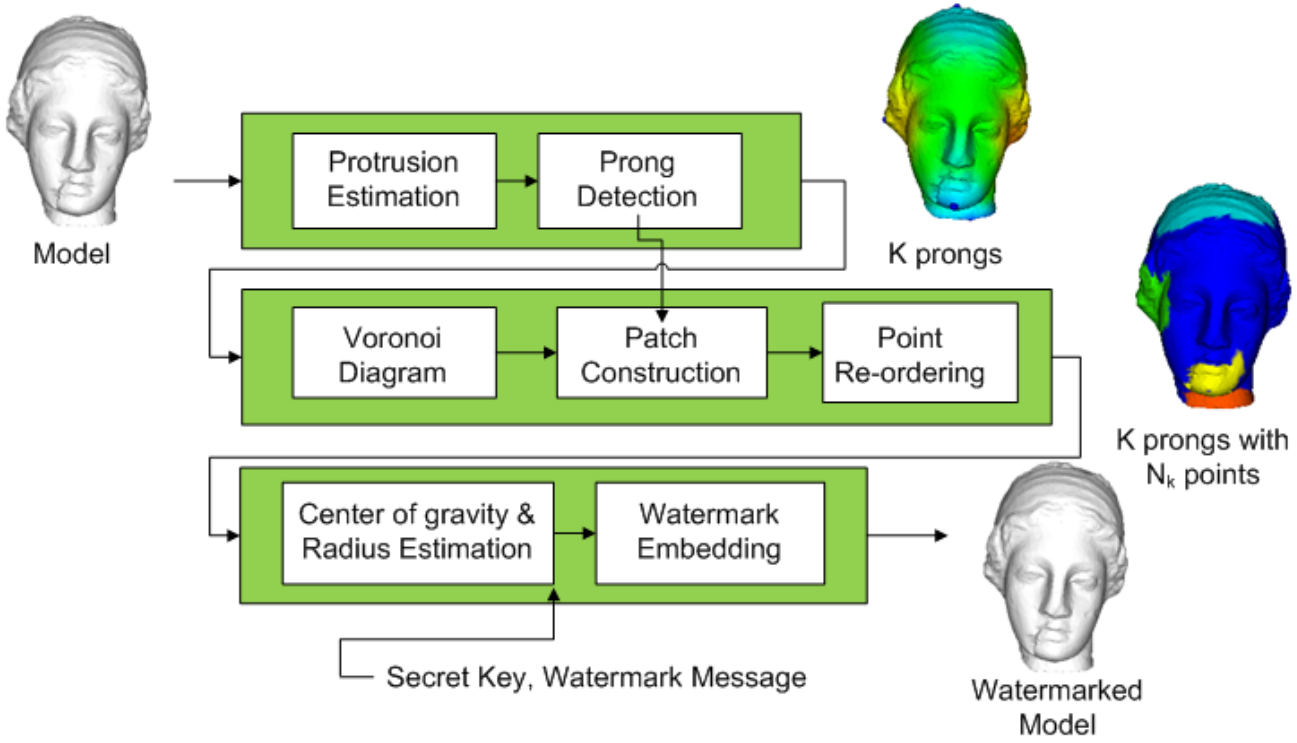


Original With PM Without PM

Proposed Watermarking Scheme

- Scheme:

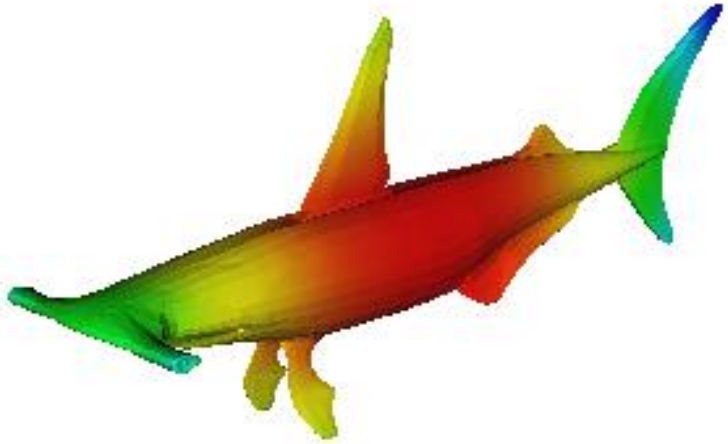
1. Protrusion function and detection of **prongs**
2. Geodesic Voronoi Segmentation
3. Neighborhood definition
4. Local Spatial Watermarking QIM-based



P. Rondão Alface. *Perception and Re-Synchronization Issues for the Watermarking of 3D Shapes*. PhD thesis, Université Catholique de Louvain, 2006.

Step 1: Finding prongs

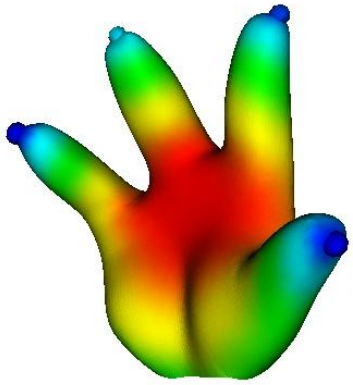
- Idea: *How to resist cropping and re-ordering attacks?*

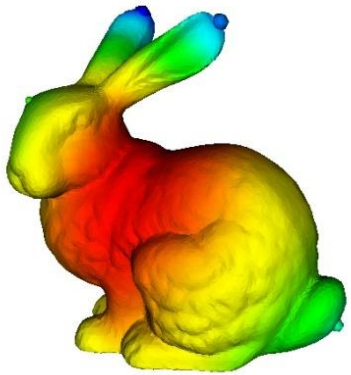


- Local spatial wm using **prongs**
- Protrusion function

$$\mu(v) = \int_{p \in S} g(v,p)^2 dS$$

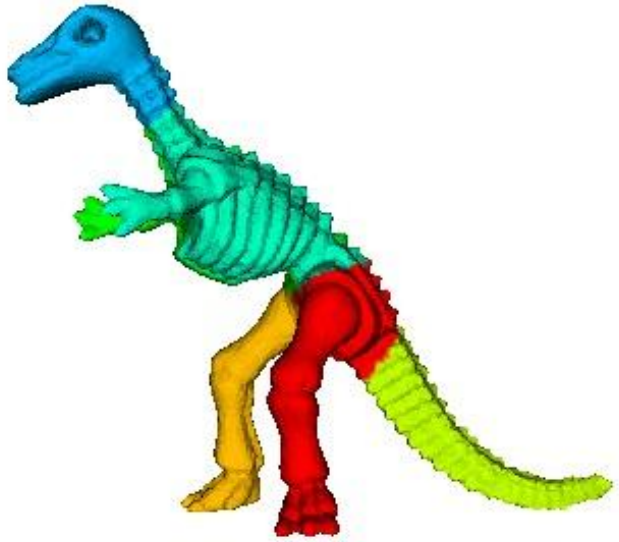
- Finding prongs:
  - Local max of the protrusion
    - Protrusion(p)>Protrusion(p_i) with p_i in the n-nearest neighbors
    - P is not on a boundary

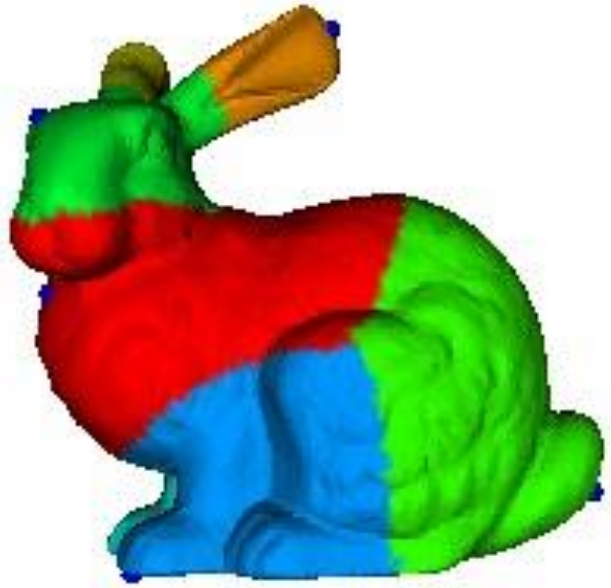




Step 2: Voronoi Segmentation

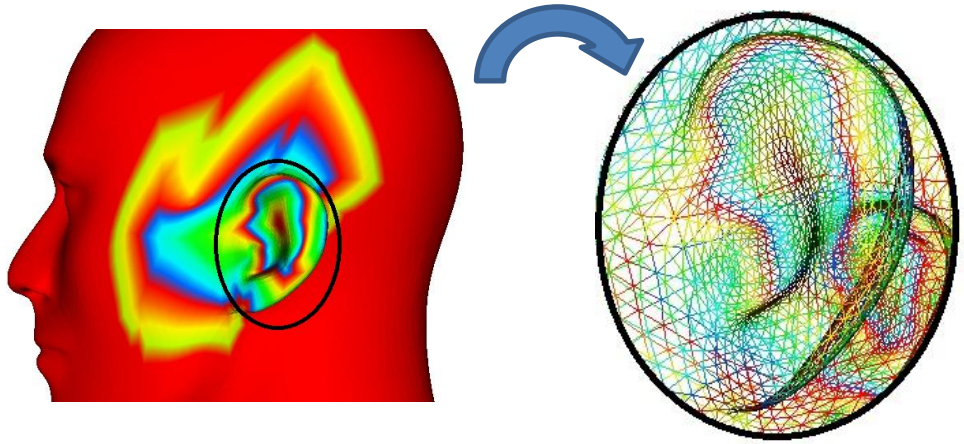
- Voronoi Mesh Segmentation
  - Number of regions vs. Number of points available to embed
  - Neighborhoods contained inside Voronoi Region

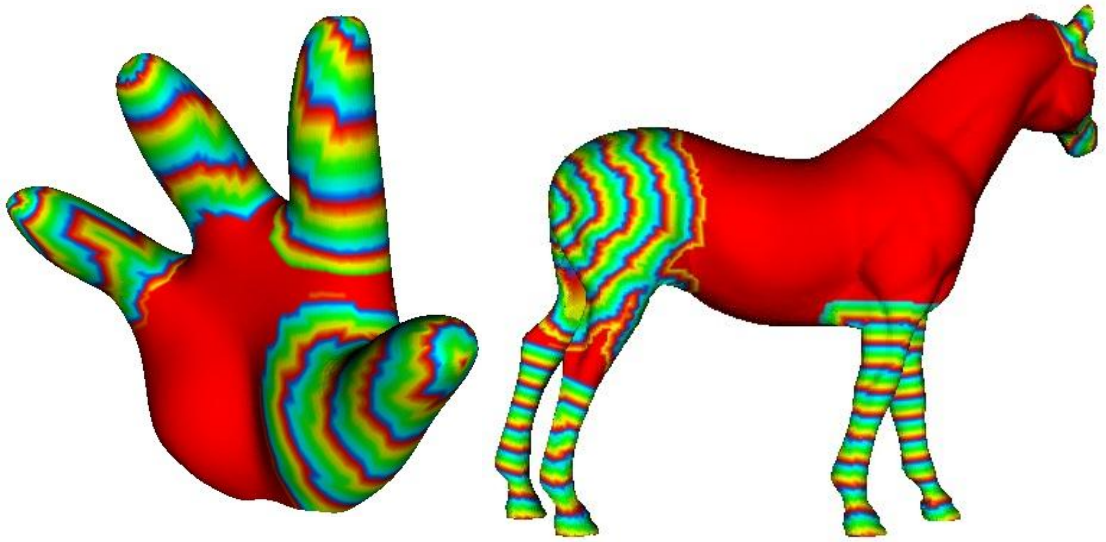




Step 3: Neighborhood definition

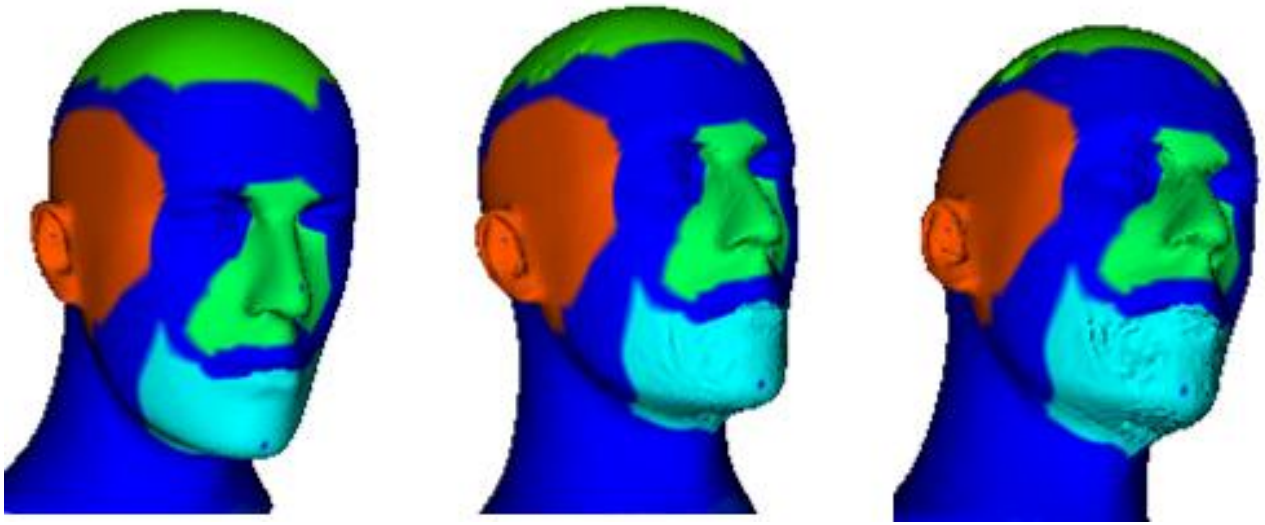
- Defining a local neighborhood for embedding
  - Rings circle centered on the prong with radius R
  - R is definded by Voronoi boundaries or wm length





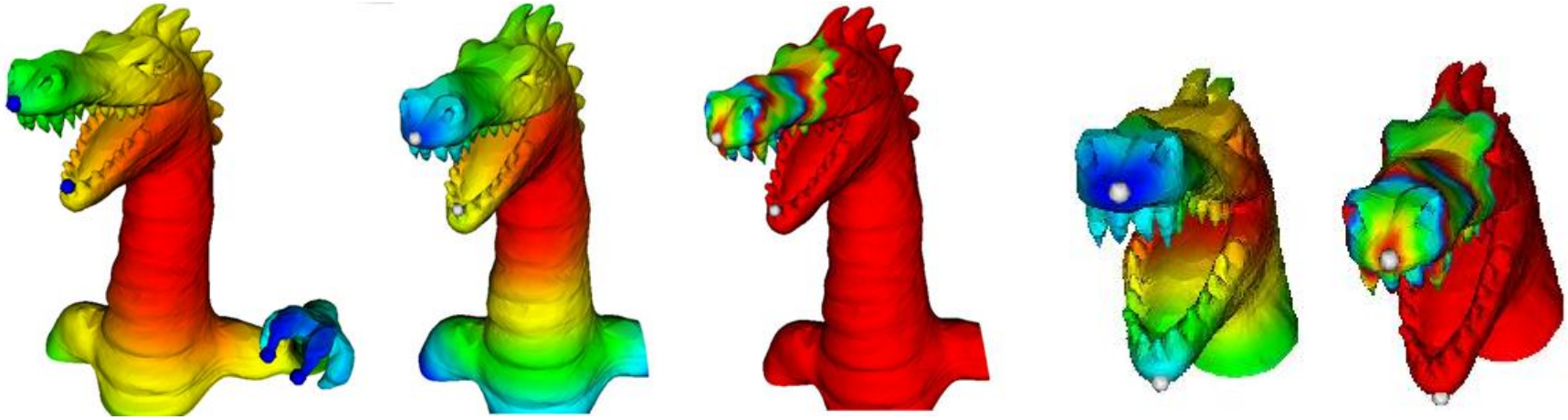
Step 4: Local Watermarking

- Patch watermarking
  - Ordering defined by geodesic distances in each ring
  - R is definded by Voronoi boundaries or wm length



Proposed Watermarking Scheme

- Robust against RST attacks
- Robustness against re-ordering
  - Order defined by geodesic distances in each ring of a patch
- Robustness against cropping
  - If the cut is far enough from prongs



Original Model
4 prongs

2 correct prongs
BER=0. BER=0

2 prongs. 1 correct prong
BER=0. BER≠0

Proposed Watermarking Scheme

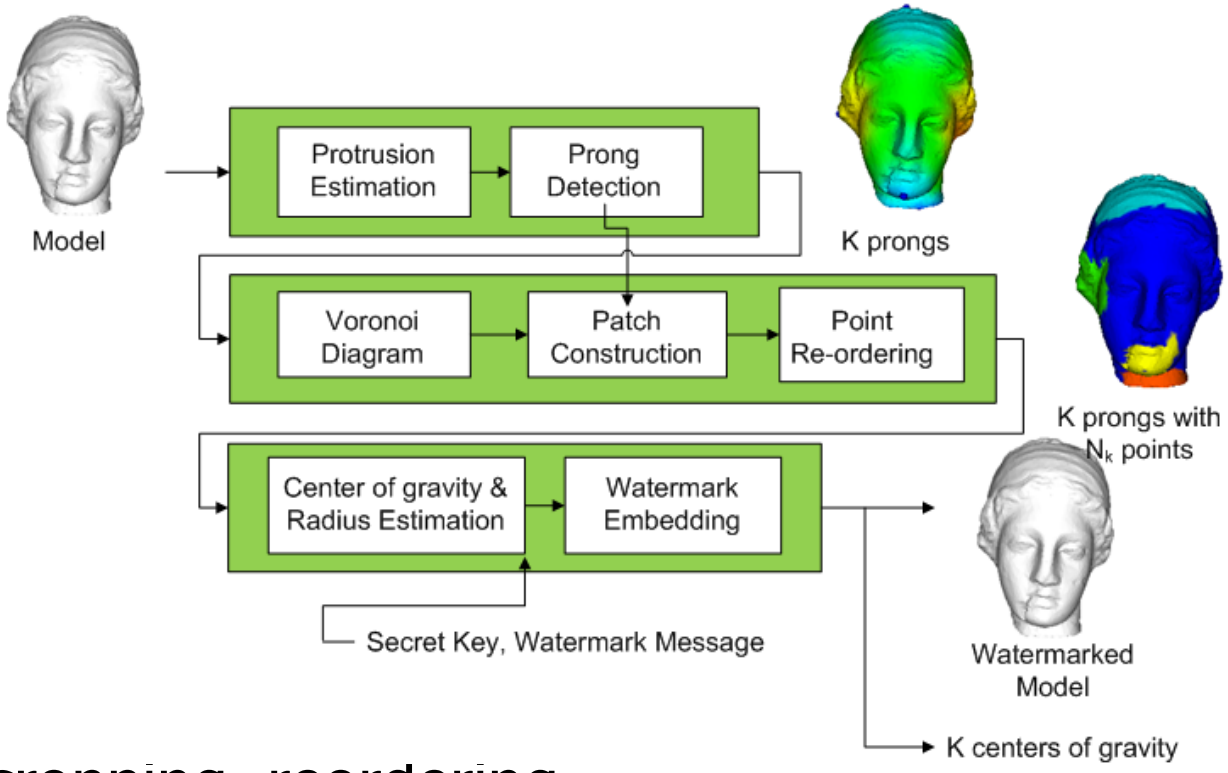
Results

- Robust against RST attacks
- Robust against cropping if crop far enough from prongs
- Robust against re-ordering
- Limitations:
  - No resistance to noising and smoothing attacks as compared to the watermarking scheme in the whole mesh
    - Cog of each patch is not well recovered
    - Ordering by geodesical distances is not properly assigned in decoding
  - Non resistant to re-sampling (embed and decoding relied to specific points of the mesh)
  - Capacity constrained by the size of the smaller patch

Models vs. Attacks	Noise	Smoothing	RST	Re-ordering	Cropping
Hammerhead	NO	NO	OK	OK	OK
Bunny	NO	NO	OK	OK	OK
Dinosaur	NO	NO	OK	OK	OK

Robust 3D Watermarking Scheme with Side-Information

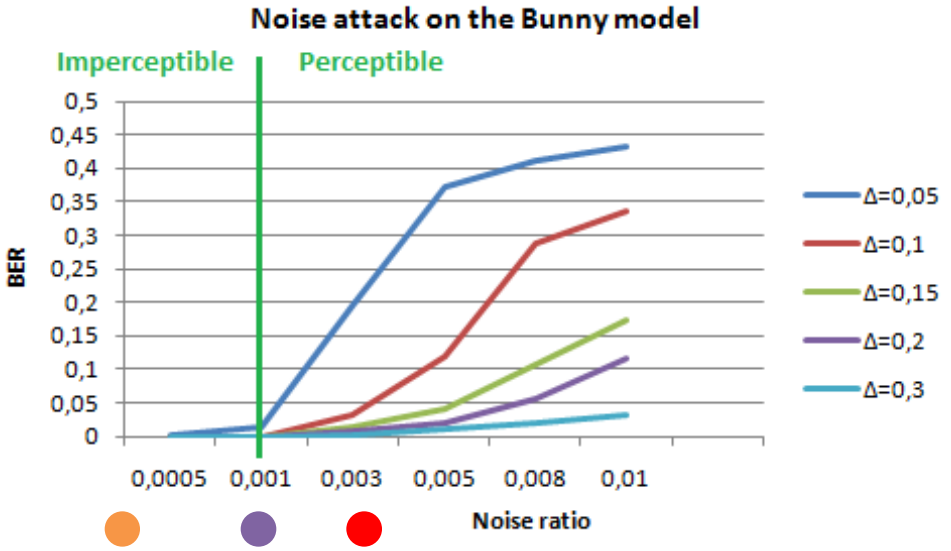
- Idea: *Build a wm. Scheme robust against noising and smoothing*
- Cog patches as side-information
- New scheme:

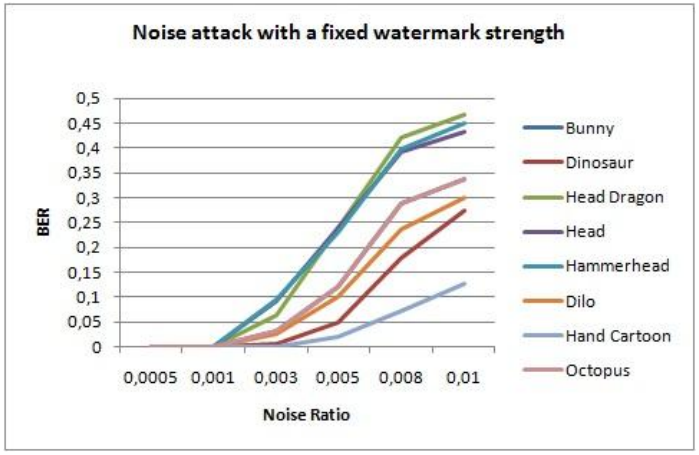


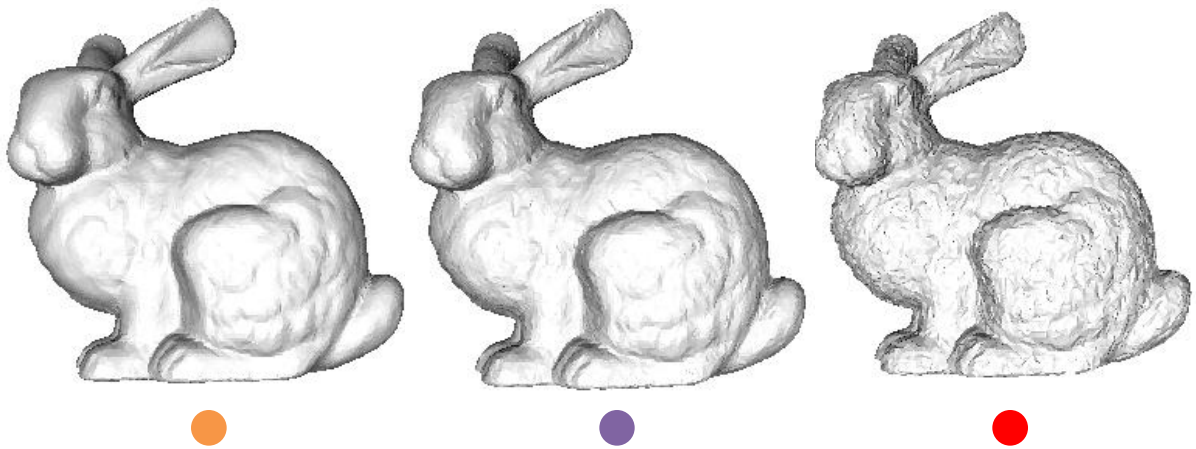
- Robust against cropping, reordering

Robust 3D Watermarking Scheme with Side-Information

- Robustness against noise addition
  - Watermark retrieved for NR values no perceptible
  - Perception depends on each mesh feature







Robust 3D Watermarking Scheme with Side-Information

- Robustness against noise addition
  - Minimal Δ for different NR values

MODEL	Δ	MSDM	PRONGS	CAPACITY	NR	BER	PERCEPTION
	0.1	0.113	6	4032/14007	0.001	0	Imperceptible
					0.003	0.031	Perceptible
					0.005	0.120	Perceptible
					0.008	0.288	Perceptible
	0.1	0.127	6	8064/14070	0.001	0	Imperceptible
					0.003	0.004	Perceptible
					0.005	0.050	Perceptible
					0.008	0.180	Perceptible
	0.1	0.046	6	3328/19119	0.001	0	Imperceptible
					0.003	0.062	Perceptible
					0.005	0.241	Perceptible
	0.05	0.065	6	6400/11703	0.0005	0	Imperceptible
					0.001	0.035	Perceptible
					0.003	0.296	Perceptible

Robust 3D Watermarking Scheme with Side-Information

Results

- Robust against cropping if crop far enough from prongs
- Robust against re-ordering
- Robust against noising and smoothing in cases of interest
- RST attacks
- Limitations:
  - Non resistant to re-sampling (embed and decoding relied to specific points of the mesh)
  - BER correctness correlated with number of insertions in the patch

Models vs. Attacks	Noise	Smoothing	RST	Re-ordering	Cropping
Head	0.1%	0.05%	OK	OK	OK
Bunny	0.3%	0.1%	OK	OK	OK
Dinosaur	0.3%	0.1%	OK	OK	OK

Conclusions

- 3D wm. Scheme combining:
  - QIM-based 3D watermarking
  - Prong features for re-synchronization
  - Perceptual visual mask
- Succesful extension
  - Compared to QIM, improved robustness against re-ordering, cropping. Noise and smoothing resistance is silightly reduced
  - Compared to feature-based re-syncrhonization, better resistance to noise and smoothing.
  - Side information is necessary for optimal results.
- Future work:
  - Extension of the Visual Mask to other features
  - How to resist against re-sampling attacks?
  - Security of side information

Thank you!

Questions?