Anti-cropping Blind Resynchronization for 3D Watermarking

Xavier Rolland-Nevière Gwenaël Doërr Pierre Alliez

Technicolor R&D France

Inria Sophia-Antipolis – Méditerranée

IEEE ICASSP 2015

1. Introduction
2. 3D Landmarks Creation
3. Synchronization Patterns
4. Performances
5. Conclusion

Context

3D assets

- Routinely used in movies, video games, and scientific simulations
- Complex, valuable and copyrighted

Piracy threats

- 3D models/animations leakage
- 3D scanners/printers

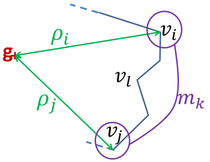
Enduring challenges in 3D watermarking (for traitor tracing)

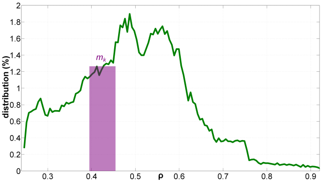
1. Transforms for 3D mesh: correlated coefficients, causality issues
2. Perceptual modeling: geometry vs. rendering fidelity, complexity
3. Resynchonization: robustness trade-off against cropping / noise addition
4. Security: accessible watermark carriers

Radial-based 3D Watermarking

Baseline principle

Encode watermark information in the distribution of radial distances ρ_i between the center of mass **g** and the vertices v_i [Cho et al., 2007]





Embedding process

1. Compute the radial distances ρ_i
2. Compute the histogram $\mathrm{hist}(\boldsymbol{\rho})$ and the average μ_k of each bin
3. Compute a target average value $\mu_k \lessgtr \tau_k$ to encode a bit m_k of the watermark payload
4. Modify v_i position so that corresponding bin averages μ_k matches the target values

Reference implementation

- Quadratic programming framework [Rolland-Nevière et al., 2014]

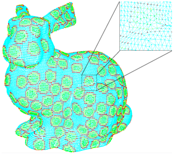
3D Cropping Attack

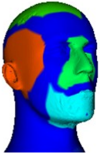
Watermark desynchronization

Loss of $\mathbf{g}, \min(\boldsymbol{\rho}), \max(\boldsymbol{\rho}) \implies$ critical impairment of $\mathrm{hist}(\boldsymbol{\rho})$

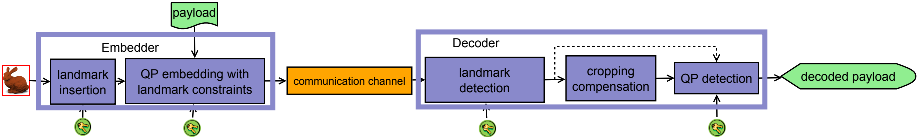
Countermeasures

1. Invariant watermark carrier
   ☹ *Sensitivity to noise*
2. (Implicit) resynchronization
   ☹ *Instability, content dependency*
3. Pilot sequences (?)





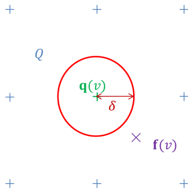
Proposed approach



3D Landmark Vertices

Landmark definition

- **f**: vector field $\mathcal{M} \rightarrow \mathbb{R}^2$
  1. Fitting parametric model of paraboloid to $\mathcal{N}_2(v)$
  2. Derive RST-resilient 2D vertex signature
- $\mathcal{Q}$: 2D quantization lattice
- $\mathbf{q}(v) \in \mathcal{Q}$: quantization point closest to $\mathbf{f}(v)$
- v is a landmark $\iff \|\mathbf{f}(v) - \mathbf{q}(v)\| < \delta$



Landmark creation

Move vertices $v_i \in \mathcal{N}_2(v)$ in a local neighborhood to

- *Minimize* the squared error distortion
- While satisfying the *constraint*: $\|\mathbf{f}(v) - \mathbf{q}(v)\| < \delta$

Non-interference: non-overlapping neighborhoods for multiple landmarks

Detection of Landmark Vertices

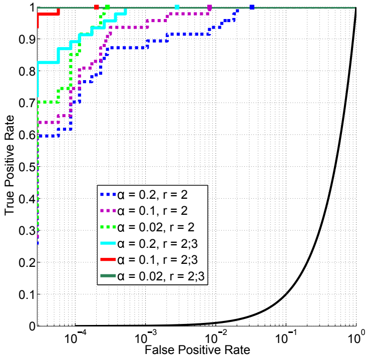
Blind retrieval

1. Fast signature estimation for all vertices (4s for 35k vertices)
2. Detection problem: binary classification (threshold at δ)

Limitation: false positives due to the low dimension (2D) of the signature

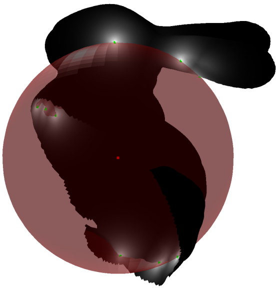
Mitigation strategies

1. Strengthen the landmark constraint, i.e. reduce the threshold δ
2. Increase the dimensionality of the signature $\mathbf{f}(v)$
   - Complex neighborhood modeling
   - Nested signatures $\mathcal{N}_2(v) \longrightarrow (\mathcal{N}_2(v), \mathcal{N}_3(v))$



α: normalized δ w.r.t. $\mathcal{Q}$

Center of Mass Recovery



Watermark embedding

1. Create a pattern of landmarks to recover $\mathbf{g}$
   - Select a non-overlapping set of vertices $\mathcal{L}$ near a sphere $\mathcal{S}(\mathbf{g}, r)$ (heuristics)
   - Project vertices of $\mathcal{L}$ onto $\mathcal{S}$
   - Turn vertices of $\mathcal{L}$ into landmarks
2. Embed payload with radial 3D watermarking (add constraints to preserve landmarks)

Watermark extraction

1. Recover the center of mass
   - Retrieve a set $\hat{\mathcal{L}}$ of candidate landmarks
   - Compute an estimate $\hat{\mathbf{g}}_{\hat{\mathcal{L}}} \equiv \mathbf{g}$ using robust sphere fitting (RANSAC)
2. Radial 3D watermark extraction using $\hat{\mathbf{g}}_{\hat{\mathcal{L}}}$ (instead of $\hat{\mathbf{g}}$)

Low landmark/fitting scores $\implies$ automatic resynchronization bypass

Full Resynchronization

Objective: transmit $(\mathbf{g}, \min(\boldsymbol{\rho}), \max(\boldsymbol{\rho}))$ to fully recover $\mathrm{hist}(\boldsymbol{\rho})$
Proposal: embed two synchronization patterns $\mathcal{S}_1(\mathbf{g}, r_1)$ and $\mathcal{S}_2(\mathbf{g}, r_2)$

Watermark embedder

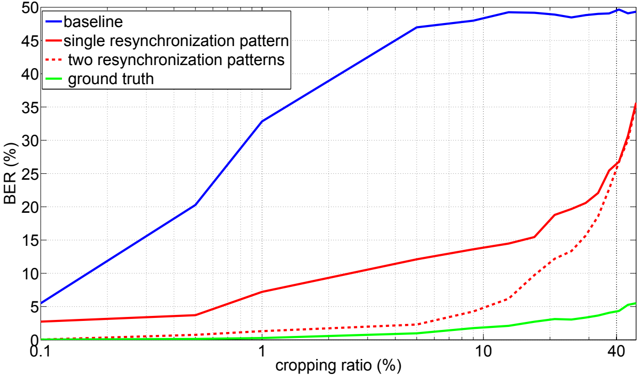
1. Define two sets of landmarks $(\mathcal{L}_1, \mathcal{L}_2)$ using alternate quantizers, e.g. QIM
2. Define (r_1, r_2) as preset linear combination of $(\min(\boldsymbol{\rho}), \max(\boldsymbol{\rho}))$

Vertex assignment: 90% payload vs. 10% resynchronization

Watermark decoder

1. Recover the geometrical parameters of both synchronization patterns
   - Isolate candidate landmarks for both quantizers used during embedding
   - Compute $\hat{\mathbf{g}}_{\hat{\mathcal{L}}}$ and $\hat{r}$ after RANSAC sphere fitting for both sets of landmarks
2. Radial 3D watermark extraction using $\hat{\mathbf{g}}_{\hat{\mathcal{L}}_1}, \hat{\mathbf{g}}_{\hat{\mathcal{L}}_2}, \hat{r}_1, \hat{r}_2$
   (when confidence is sufficient)

Benchmarking Against Cropping



Remarks

- Resynchronization robust to combined rigid transform and cropping (in contrast with 'ground truth')
- Baselines with/without resynchronization equally robust against valumetric attacks, simplification, etc.

Wrapping Up

Conclusion

1. New resynchronization paradigm illustrated with radial 3D watermarking
2. Significant gain in robustness against cropping
   … while preserving performances against standalone noise addition

Research outlook

1. Robustness against combined cropping-noise attacks
2. Investigate alternate models for local neighborhoods
3. Security of landmark resynchronization (QIM attacks, geometric attacks)
4. Extension to other types of content, e.g. 2D landmarks for still images

Bibliography

Cho, J.-W., Prost, R., and Jung, H.-Y. (2007).
An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms.
IEEE Transactions on Signal Processing, 55(1):142–155.

Rolland-Nevière, X., Doërr, G., and Alliez, P. (2014).
Triangle surface mesh watermarking based on a constrained optimization framework.
IEEE Transactions on Information Forensics and Security, 9(9):1491–1501.