A FORMAT-COMPLIANT SELECTIVE SECRET 3D OBJECT SHARING SCHEME BASED ON SHAMIR'S SCHEME

Sébastien Beugnon[1,2], William Puech[1] and Jean-Pierre Pedeboy[2]

[1] LIRMM, CNRS, Univ. Montpellier, France

[2] STRATEGIES, Rungis, France

{sebastien.beugnon, william.puech}@lirmm.fr

INTRODUCTION

Multimedia security **allows** users to **protect** content from illegal access by **preserving** the **format compliance**.

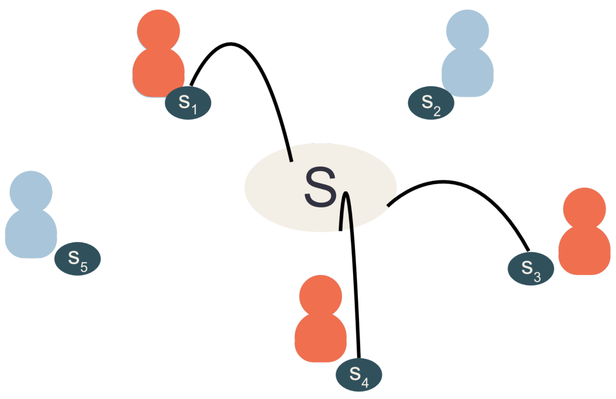
3D selective encryption allows owners to distribute protected 3D contents **as they see fit** to transmit to third-parties [1].

The **need** to **share** 3D content in a **secure** manner has arisen in recent **collaborative** and cloud-based environments, such as **3D workflows**.

We propose a **selective secret 3D object sharing scheme based on Shamir's Secret Sharing scheme** to protect 3D content and share low quality 3D objects as shares.

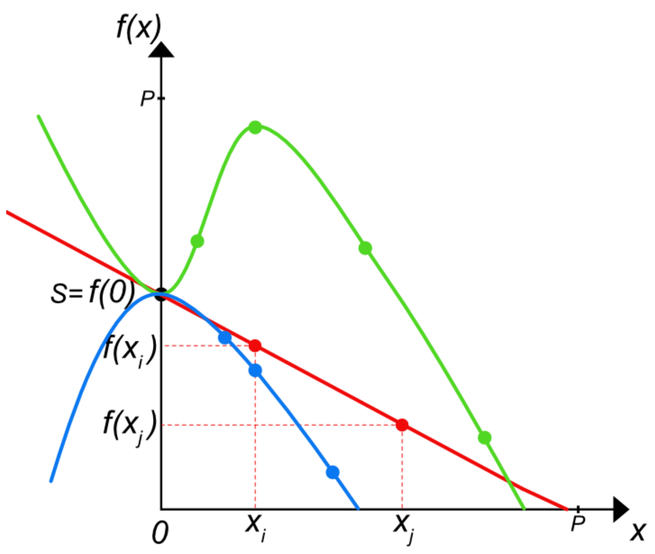
SECRET SHARING

- Keyless approach.
- (*k, n*)- threshold scheme.
- Share a secret among *n* users.
- Reconstruct secret with *k* users (among the *n)*.

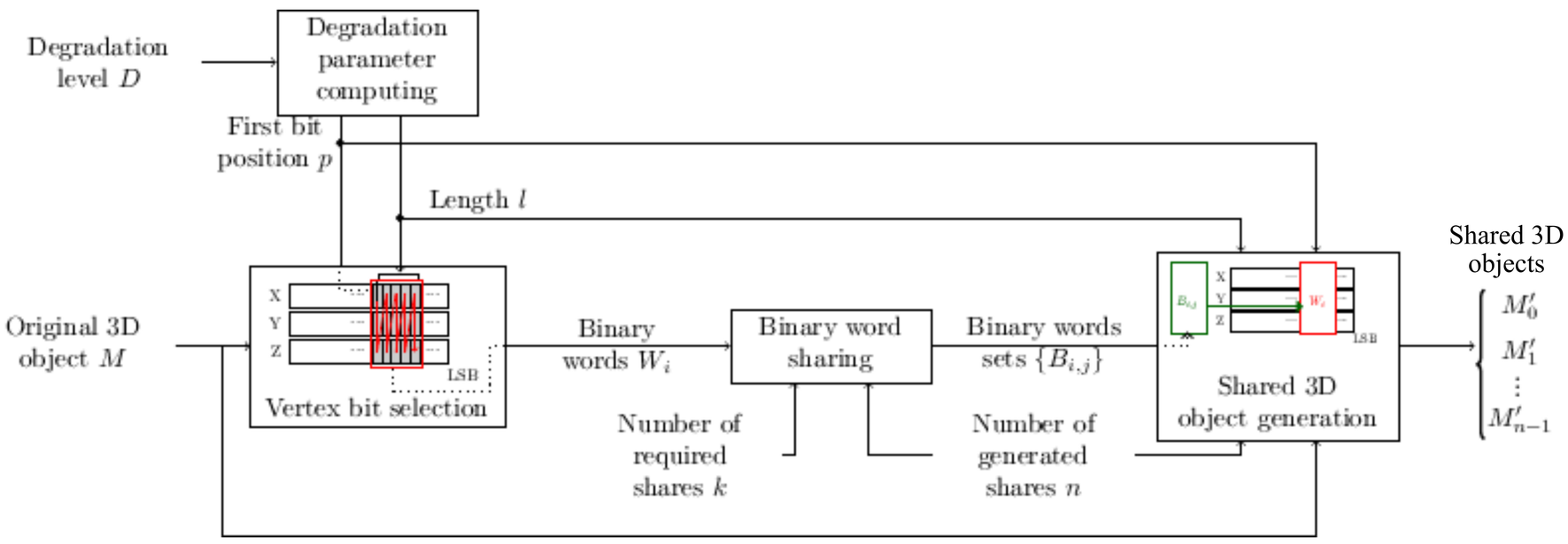


SHAMIR'S SCHEME

- First scheme in 1979 [2].
- Secret is defined on finite field.
- Shares can be considered as **2D points**.
- The secret is reconstructed using a polynomial interpolation (Lagrange's interpolation).

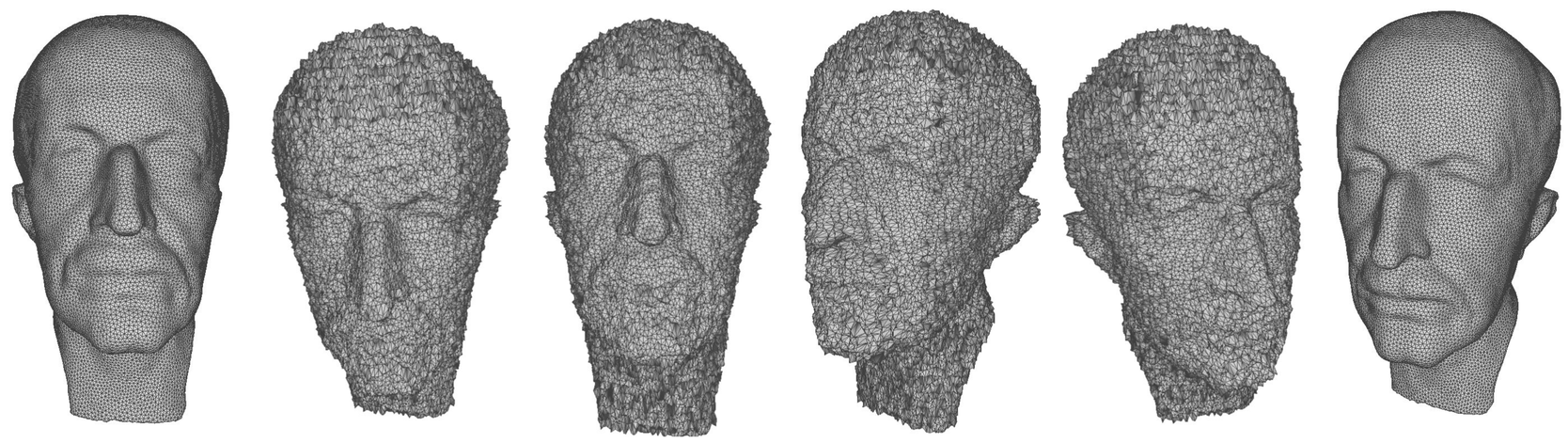


OVERVIEW OF THE METHOD



Degradation level *D* parameters: *p* between 0 and 22, *l* between 1 and (*p*+1).

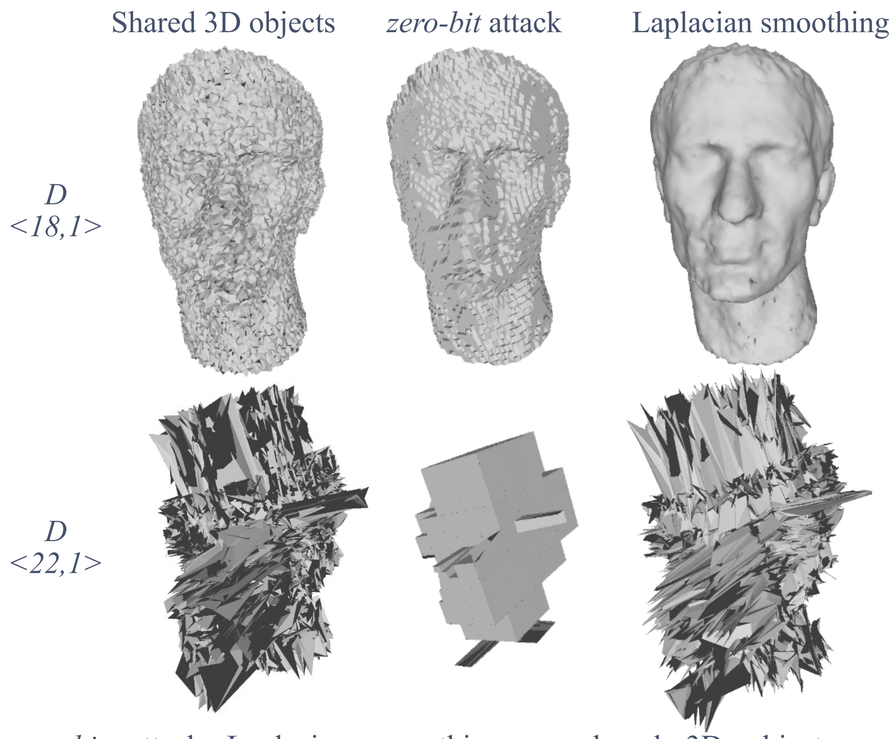
EXPERIMENTAL RESULTS



Original 3D object | *Shared 3D object* M'_0 | *Shared 3D object* M'_1 | *Shared 3D object* M'_2 | *Shared 3D object* M'_3 | *Reconstructed 3D object*

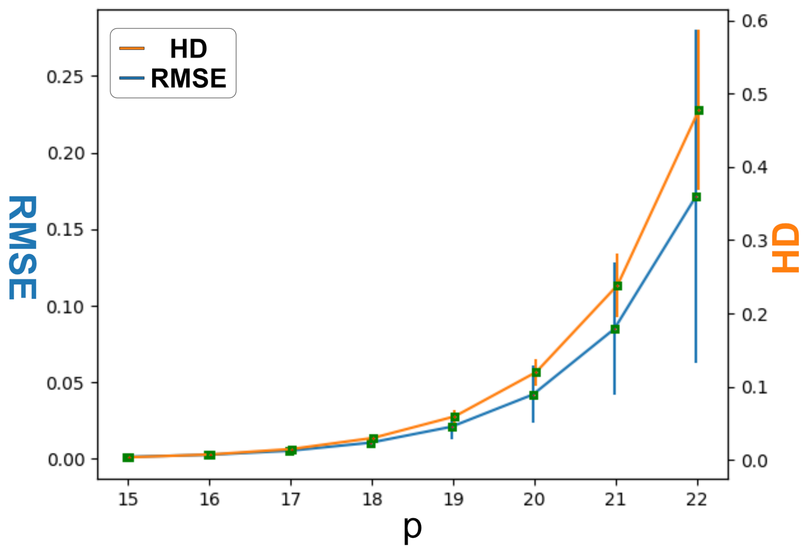
Sharing experiment with parameters *k=3*, *n=4* and *D=<18,19>*.

GEOMETRIC ATTACKS



zero-bit attack Laplacian smoothing on shared 3D objects depending on the degradation level *D=<18, 1>* and *D=<22,1>*.

EVALUATION



Mean and standard deviation of the RMSE and the Hausdorff Distance on the Princeton mesh segmentation dataset [3] as a function of the degradation level (*D=<p, p+1>*).

COMPARISON

Scheme	[4]	[5]	[6]	[7]	[8]	**Proposed**
Meaningful	✗	✗	✗	✓	✓	✓
Lossless	✗	✗	✓	✓	✗	✓
Multiple	✗	✓	✓	✗	✓	✗
Non expansive	✓	✗	✓	✗	✗	✓
Format-compliant	✗	✗	✓	✓	✓	✓
Selective	✗	✗	✗	✗	✗	✓

Comparison of our scheme with previous work.

CONCLUSION

- We proposed a efficient **format-compliant selective secret 3D object sharing** scheme based on Shamir's scheme. We share a 3D object and *n* low and controllable quality shared 3D objects distributed to users which can reconstruct the secret 3D object **perfectly** with *k* of them.
- We introduced the **first selective** secret 3D object sharing scheme which **allows** users to define the **level of degradation** assigned to the shared 3D objects before the sharing step.
- Experimental results show the feasibility of our scheme and the robustness against geometric attacks.
- Future work will concentrate on adding new features to our secret 3D object sharing scheme, for example **hierarchical** aspect in order to control the access to 3D content depending on the hierarchy among users in collaborative 3D workflows.

REFERENCES

[1] S. Beugnon, W. Puech and J.-P. Pedeboy, "Format-compliant selective encryption of 3D objects", *2018 IEEE ICME*, 2018.

[2] A. Shamir, "How to share a secret", *Communications of the ACM*, 1979.

[3] X. Chen, A. Golovinskiy and T. Funkhouser, "A benchmark for 3D mesh segmentation", *ACM TOG*, 2009.

[4] E. Elsheh and A. B. Hamza, "Secret sharing approaches for 3D object encryption", *Expert Systems with Applications,* 2011.

[5] L. J. Anbarasi and GS. A. Mala, "Verifiable multi secret sharing scheme for 3D models", *International Arab Journal of I.T., 2015.*

[6] A. Martín del Rey, "A multi-secret sharing scheme for 3D solid objetcs", *Expert Systems with Applications*, 2015.

[7] Y.-Y. Tsai, "A secret 3D model sharing scheme with reversible data hiding based on space subdivision", *3D Research*, 2016.

[8] S.-S. Lee, Y.-J. Huang, and J.-C. Lin, "Protection of 3D models using cross recovery", *Multimedia Tools and Applications*, 2017.