Improving Robustness of Watermarking Techniques for 3D Models

Jaden Nierop

J.A.Nierop@student.tudelft.nl

1. Background

Digital watermarking allows for:

- Verification of the authenticity.
- Verification of the identity of the owner of digital content.

A digital watermark:

- is an embedded secret in the digital content.
- should be hard to destroy without ruining the content in the process.

Watermarking 3D meshes is hard because:

- mesh topology is arbitrary and can be complex. [1]
- Many possible complex attacks on the watermark. [1]

2. Research Question

How can introducing mesh regularization steps before watermark insertion and extraction make geometry based 3D mesh watermarking techniques more robust against randomization of points attacks?

3. Method

To investigate the effects that the addition of mesh regularization steps has on geometry based watermarking techniques we implement a geometry based watermarking technique proposed by O. Benedens in [2]. We evaluate the performance of this watermarking technique against a randomization of points attacks with and without the addition of mesh regularization steps.

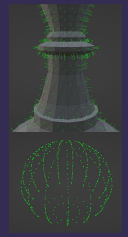
The randomization of points attack displaces every vertex of the watermarked mesh a given distance in random directions to attempt to destroy the watermark.

The watermarking algorithm and randomization of points attack are implemented in Python while the mesh regularization steps are applied using a 3D modeling software called Blender.

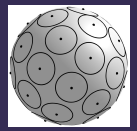
Responsible Professor: Dr. Zeki Erkin, z.erkin@tudelft.nl , Supervisor: Devris Isler

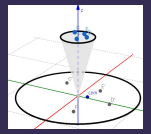
TU Delft

4. Watermarking Algorithm



The face normals of the mesh are calculated and put into bins if they lie within the radius of the bin to create an orientation histogram of the normals.

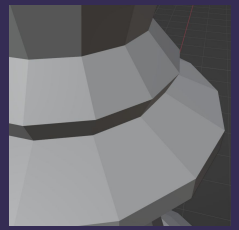




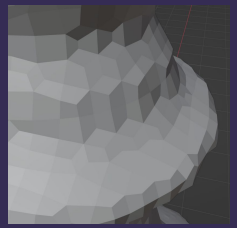
The center of mass of the normals in each bin is calculated. To encode a "0" bit move the center of mass in the positive x direction and opposite to encode a "1".

5. Mesh Regularization

Before regularizing



After regularizing



6. Results

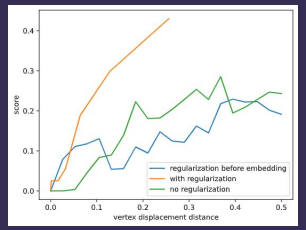


Figure 1: Error scores of the watermarking technique plotted against the vertex displacement distances of the randomization of points attacks. Lower error scores indicate fewer incorrect bits. The green graph represents runs with no regularization steps. The blue graph represents the runs where the mesh was regularized solely before watermark embedding and the orange graph included regularization before embedding and extraction.

7. Conclusion

The result show no increase in robustness with the addition of the regularization steps. In fact, including any regularization steps with O. Benedens algorithm always results in a higher error score.

Possible causes:

- The regularization step itself partially destroys the watermark.
- randomization attacks could be more effective against meshes with smaller faces.

Limitations:

- Regularization was only tested with O. Benedens algorithm.
- It could provide positive results in combination with other watermarking algorithms.

References

[1] Wang, K., Lavoué, G., Denis, F., & Baskurt, A. (2008). A comprehensive survey on three-dimensional mesh watermarking. IEEE Transactions on Multimedia, 10(8), 1513-1527.

[2] Benedens, O. (1999). Geometry-based watermarking of 3D models. FRAUNHOFER INST FOR COMPUTER GRAPHICS DARMSTADT (GERMANY) VIRTUAL REALITY DEMONSTRATION CENTRE.