A High-Capacity Data Hiding Method for Polygonal Meshes*

Hao-tian Wu and Yiu-ming Cheung

Department of Computer Science,
Hong Kong Baptist University, Hong Kong, China

Abstract. This paper presents a high-capacity data hiding method for 3D polygonal meshes. By slightly modifying the distance from a vertex to its traversed neighbors based on quantization, a watermark (i.e., a string of binary numbers) can be embedded into a polygonal mesh during a mesh traversal process. The impact of embedding can be tuned by appropriately choosing the quantization step. The embedded data is robust against those content-preserving manipulations, such as rotation, uniformly scaling and translation, as well as mantissa truncation of vertex coordinate to a certain degree, but sensitive to malicious manipulations. Therefore, it can be used for authentication and content annotation of polygonal meshes. Compared with the previous work, the capacity of the proposed method is relatively high, tending to 1 bit/vertex. Besides to define the embedding primitive over a neighborhood so as to achieve resistance to substitution attacks, the security is also improved by making it hard to estimate the quantization step from the modified distances. A secret key is used to order the process of mesh traversal so that it is even harder to construct a counterfeit mesh with the same watermark. The numerical results show the efficacy of the proposed method.

1 Introduction

With the development of digital modeling and visualization techniques for 3D objects, 3D models have been widely created and used for geometry representation, such as the cultural heritage recording like Digital Michelangelo Project [1], CAD models, and structural data of biological macromolecules [2]. As more and more 3D models appear, polygonal meshes in particular, how to hide information within them [3] has received much attention for a variety of purposes, ranging from copyright enforcement (e.g. [9,10]) to authentication (e.g. [4,6]). In this paper, we only discuss fragile watermarking of polygonal meshes, which is contrast to robust watermarking for the fragility of the embedded watermark. Compared with digital images, video and audio streams, there exists no grid for meshes, i.e., each vertex in a mesh is connected with variable neighboring vertices at different distances. This flexibility of mesh data makes it an attractive cover object for data hiding.

* This work was supported by a Faculty Research Grant of Hong Kong Baptist University with the Project Code: FRG/06-07/II-07.

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 188–200, 2007.

In the literature, quite a few watermarking methods (e.g.[4]-[18]) have been proposed to embed data into meshes. Depending on the applications, the requirements are different. For instance, one purpose of robust watermarking is to protect the copyright of digital works so that the embedded watermark is designed robust against outer processing while the original work can be used in the retrieval process [10]. In contrast, in fragile watermarking for authentication and integrity verification, the embedded data should be blindly retrieved and sensitive to illegal modifications [4], and high information rate is preferred. Nevertheless, there are some common requirements, such as security and fidelity. In [19], T. Kalker defined the security of robust watermarking as the inability of unauthorized users to remove, detect or change the watermark. A data hiding scheme is considered secure if there is little information leakage from the public domain. It should be assumed that the algorithms are publicly known and the attacker has sufficient computational capability so that some valuable information may be leaked from the observation of watermarked objects. Fidelity means that the embedded data is invisible (except the case that it is intentionally visible), i.e., the embedding process should not introduce noticeable distortion to the cover object. And it is often required that the introduced error can be numerically analyzed and bounded.

Only a few fragile watermarking algorithms (e.g.[4]-[8]) have been proposed for authentication of polygonal meshes. The first fragile watermarking of 3D objects is addressed by Yeo and Yeung in [4] for authentication and integrity protection by using a set of lookup tables (LUTs). If two values generated from the positions of a vertex and its traversed neighboring vertices are identical to each other, the vertex is considered as valid. Otherwise, its position will be perturbed until the two values match. Since the data embedded in [4] is sensitive to *R*otation, uniformly *S*caling and *T*ranslation transformations (denoted as RST hereinafter), its applications may be limited. By adapting the work in [4], Lin et al. proposed a fragile watermarking method in [5] to detect malicious attacks. They improve the mapping from vertex positions to location indices so that the embedded watermark is resistant to incidental data processing, such as vertex reordering, but RST transformations are still not allowed. Moreover, Benedens and Busch proposed the algorithm called Vertex Flood Algorithm (VFA) in [6] for mesh authentication. Basically, their algorithm modifies the vertices so that their distances to the centroid of a designated triangle encode the watermark bits. In this way, a certain amount of vertex coordinate truncation caused by format conversions, as well as RST transformations, can be allowed. As for a triangle mesh, the security of VFA relies on the selection of the start triangle since the vertex position can be modified without changing the distance from it to the centroid of the start triangle. Later, Cayre and Macq presented a steganographic scheme [7] for triangle meshes by treating a triangle as a two-state geometrical object. By choosing an appropriate Macro Embedding Procedure (MEP) order, a watermark can be imperceptibly embedded with robustness against RST transformations. The upper bound of capacity has been given in [7], but the optimal mesh traversal to reach it has not been addressed yet. Alternatively, in