Part I

General Introduction and Notions of Digital Shape Processing

Chapter 1

General Introduction

1.1 Context of the work

The context of this thesis relates to the protection of the intellectual property rights (IPR) associated with three-dimensional (3D) models. This relatively new kind of multimedia has recently met an increasing success since its applications have been worldwidely broadcasted over the Internet. Such applications are varied and range from the entertainment industry (animation movies, video games, cultural heritage exposition in mixed or virtual reality,...) to the technical or scientifical world (medical imaging, Computer Aided Design (CAD), physical simulations, ...). Indeed, 3D models are digital representations of a shape in the 3D space and are particularly well suited for the visualization of complex scientific data (e.g. dynamic flows, etc.) as well as for real-time or photo-realistic visual effects for respectively, video games and animation movies.

3D data approximate continuous surfaces and are commonly represented by 3D meshes. A 3D mesh is composed of two parts: the *geometry* and the *connectivity*. The geometry is the set of samples of the surface i.e. the points of the surface and their position in space (x, y, z coordinates). The connectivity is the set of triangles connecting these points. The connectivity enables to represent a piecewise linear approximation of the continuous surface.

The production or acquisition of 3D models usually involves large costs that content owners would like to compensate through licensed distribution. Digital Rights Management (DRM) now enables to provide different

kinds of licenses, from e.g. the full licensed distribution with all functionalities to the free largely distributed version but with limited functionalities. However, likewise for digital image, audio or video files, DRM systems still fail to protect copyrighted material against theft and misuse (i.e. piracy). This fact is mostly due to the evolution from the analog to the digital world and the subsequent ease of copying, distributing and consuming audiovisual content.

One particular example among applications making use of 3D models and depending on the efficiency of DRM systems, is the case of the Stanford Michelangelo Project. This project has developed a high-resolution digital archive of ten of Michelangelo's large statues which represent the artistic patrimony of Italy's cultural institutions. Italian authorities permit distribution of the 3D models only to established scholars for noncommercial use. The digital 3D model of the David would quickly be pirated if it were distributed without protection; simulated marble replicas would then be manufactured outside the provisions of the parties authorizing creation of the model.

The solutions provided by DRM systems generally rely on *cryptography* and *digital watermarking*. Digital watermarking refers to the process of *hiding imperceptible and robust data into the content to protect*. The hidden data is called *watermark* and consists in e.g. serial numbers of the licensee or the owner of the content. Usually a *secret key* is necessary to insert the watermark as well as to retrieve it. Imperceptibility is a strong requirement because the watermark should not damage the appearance, use and function of the content. The robustness requirement refers to the fact that common or malign manipulations (a.k.a. *attacks*) of the content should not threaten the detection or retrieval of the watermark. The idea (somewhat simplified for the sake of pedagogy) is that a content owner can prove his/her ownership by retrieving his/her hidden serial number in a pirated model and then sue the responsible of this infraction.

The detection of a watermark is referred to as *non-blind* when the availability of the original version of the content is needed to be able to retrieve the watermark. The algorithms based on this kind of detection are usually much more robust because they can synchronize the modified and original versions of the same model knowing exactly where the watermark should be hidden. However, non-blind detection is not practical since a content

owner should use all his/her database of copyrighted material, synchronize this database with the database of the suspected pirat and compare pairs of corresponding models. This involves a high computational cost as well as a high risk related to the fact that the detection needs the availability of a nearly unprotected database. On the opposite, *blind* watermarking schemes do not need to rely on the availability of the original data. The watermark is directly detected on the suspect models. This gain in computational cost and time is usually made at the expense of the robustness of the watermark.

Compared to other audiovisual multimedia such as image, audio and video, 3D watermarking is relatively new and is not yet a mature technology. This thesis focuses on two main issues: 3D watermark or attack imperceptibility and blind robust 3D watermarking.

Imperceptibility is a requirement for watermarks as well as for watermarking attacks. Content manipulations or hidden data should not modify the use, appearance or function of the content. For 3D models, it is difficult to assess whether modifications of the surface are perceptible or not for the human eye. Some metrics are currently used to assess the quality of watermarked or compressed models but usually fail at predicting human perception. A first contribution of this thesis relates to a new metric which better captures human perception by comparing 2D views of the 3D model with a Mutual Information criterion. A psychovisual experiment has validated this metric for the case of watermarking attacks.

The other issue addressed by this thesis is the blind and robust watermarking of 3D shapes. As aforementioned, blind detection is more difficult than non-blind detection because the original data are not available. Blind watermarking algorithms are thus currently less robust and reliable. This solution should however be required in practice because of the risks related to the handling of unprotected original data when trying to detect a pirated model. Robustness is often measured in terms of the number of watermarking attacks categories the watermark is able to withstand. Most common categories of attacks are *similarity attacks* (rotation, translation, scaling, sample re-ordering), *geometrical attacks* (noise addition, surface smoothing), *resampling attacks* (connectivity modifications such as simplification, subdivision, remeshing) and *cropping* (i.e. cutting part of the 3D model by a plane). Current non-blind watermarking schemes are able to

resist against all these attacks at some extent. Blind watermarking schemes usually all resist to similarity attacks and at most one other category. For example, some schemes resist against cropping but not against geometrical and resampling attacks. Others are robust to geometrical and/or resampling attacks but not to cropping. However, a reliable watermark should be able to be retrieved after any of these attacks and their combinations provided they are imperceptible.

The second contribution of the thesis is a scheme based on the spectral decomposition of 3D meshes which resists well against geometrical and similarity attacks but fails to withstand resampling and cropping. We present the mathematical background of the spectral decomposition as well as the good properties of this transform for watermarking purposes.

The third contribution relates to the detection of robust feature points that enable to preserve the good properties of spectral decomposition while resisting now to some resampling attacks. These feature points are based on the curvature tensor field analysis which we have deeply explored and commented. We also explain why this scheme cannot resist to cropping.

The last contribution is another blind watermarking scheme which is able to resist all the aforementioned categories of attacks (however, in very limited bounds of parameters so far). This scheme is based on other robust feature points wich are called *prongs*. These points are very robust and we use them as seeds to watermark their surrounding parts of the surface.

1.2 Organization of the thesis

This thesis is organized in three main parts. Part I contains the General Introduction as well as Chapter 2 dedicated to basic definitions and processing tools related to 3D models.

Part II focuses on 3D model perception. Chapter 3 presents the technologies used to render 3D models on screens and the current available metrics used to assess the quality of these 3D models. Chapter 4 presents our first contribution which is a perceptive metric based on 2D views of the model as well as a Mutual Information criterion.

Finally, Part III is dedicated to digital watermarking. Chapter 5 gives an introduction to digital watermarking applications and vocabulary. Chapter 6 provides a detailed survey of existing 3D watermarking schemes, focusing on their characteristics, performances and limitations. Chapter 7 presents a blind watermarking scheme based on spectral decomposition. Finally, Chapters 8 and 9 expose the two last contributions of this thesis.