A digital watermarking scheme for Bezier surfaces

J Chadwick[1] S Bangay[2] P Wentworth[3]

[1] (All communications should be addressed to this author)

Department of Computer Science, University of Fort Hare, ALICE
email: j.chadwick@ru.ac.za, TEL AND FAX (+27) (40) 6022030

[2] Department of Computer Science, Rhodes University, PO Box 94, GRAHAMSTOWN
email: s.bangay@ru.ac.za TEL (+27) (46) 6038628 FAX (+27) (46) 6361915

[3] Department of Computer Science, Rhodes University, PO Box 94, GRAHAMSTOWN
email: p.wentworth@ru.ac.za TEL (+27) (46) 6038291 FAX (+27) (46) 6361915

Index terms-- Broadband communication, Security

Abstract-- **Owners and vendors are increasingly publishing their materials in digital form. Because such materials can be exactly copied, a mechanism is required that will protect the legitimate owners of these works, by providing proof of original ownership. Digital watermarking has now become one accepted method of establishing ownership of digital materials. The owner of a work embeds a pattern, called a digital watermark, in the content. This embedded watermark is normally undetectable, but its presence can be demonstrated by the owner of the work or his agent, thereby proving ownership. Digital watermarking has been used for many types of multimedia content, primarily audio, video and flat images. Recently, interest has been shown in applying digital watermarking schemes to 3D surfaces, in various formats. In this paper, we examine a method whereby a digital watermark can be embedded in a Bezier surface. A prototype watermarking method for such surfaces is presented, with some experimental results, and a discussion of directions for future research.**

1. INTRODUCTION

In view of the explosive growth in the use of the World Wide Web, it has become natural for vendors and other owners to place materials on web sites where they can be easily accessed. Vendors can make their content available for a fee, but run the risk that purchased materials may be illicitly resold by the recipients. It is therefore necessary to devise strategies that will protect the owners of copyrighted material who choose to make their property available in electronic form.

During the past ten years, digital watermarking has emerged as a method for protecting the owners of electronically stored materials. The owner embeds a digital pattern (the watermark) in the digital work, in such a manner that it does not perceptibly degrade the work, but is readily detectable by the owner or his agent. The presence of the digital watermark serves as proof of ownership.

An extensive amount of research has now been done in the general area of digital watermarking. An excellent overall discussion of the field can be found in [3]. For many years, researchers focused mainly on the watermarking of (two dimensional) images and on audio. In recent years, a number of publications have appeared that investigate digital watermarking of three dimensional surfaces stored in a variety of formats (see e.g. [1], [2], [5], [6]).

One method of storing a 3D surface is to have a set of control points which determine a Bezier surface (or, alternatively, a set of Bezier patches.) There are fast algorithms that allow the Bezier surface to be rendered if the control points are known. This paper explores a method for watermarking Bezier

surfaces by making small changes to the control points that introduce an imperceptible adjustment to the geometry of the surface. This adjustment does not impair the visual quality of the surface, but is detectable by the owner of the work. It is reasonable to use the surface geometry for the watermark insertion, as this is what is actually perceived by the end user that views the surface.

2. GENERAL CONSIDERATIONS

Given a set of $(n + 1)(m + 1)$ control points $\mathbf{P_{ij}} = (x_{ij}, y_{ij}, z_{ij})$, $0 \le i \le n$, $0 \le j \le m$, the corresponding Bezier surface is the set of points $\mathbf{P(u, v)}$, $0 \le u \le 1$, $0 \le v \le 1$, where $\mathbf{P(u, v)} = \sum^{n}_{i=0} \sum^{m}_{j=0} B_{ni}(u) B_{mj}(v)\, \mathbf{P_{ij}}$. Here $B_{ni}(u) = C(n, i)\, u^{i}\, (1- u)^{n-i}$ with $C(n, i) = n!/(i!(n-i)!)$.

There are fast routines available for calculating a point on the Bezier surface, as well as for calculating tangent vectors and normals to the surface.

We take the view here that the process of embedding a watermark should make a small change to the geometry of the Bezier surface. The change should not be large enough to be easily visible, yet must be sufficiently large so that the watermark is easily detectable by the proper authority, even in the presence of noise. A small change can be effected in the surface by suitably moving the control points. The strategy therefore is to (a) decide what change the watermark should effect in the surface and (b) make as small as possible a change to the control points which will result in the required adjustment to the surface.

It should be possible to extract the watermark even if the watermarked surface has undergone standard transformations such as rotation, translation, scaling, clipping etc. We concentrate in this work on a watermark embedding process that will survive any three dimensional transformation that preserves the scalar product of two vectors. Such transformations include rotation and translation.

3. WATERMARK EMBEDDING

We assume that the watermark to be embedded consists of st bits w_{kr} $(1 \le k \le s, 1 \le r \le t)$ where w_{kr} $\{1, -1\}$. We use a parameter for the embedding strength. A high value of means that the watermark is strongly embedded and therefore easily detectable. On the other hand, using a high may cause an unacceptably high level of distortion to the surface. Finding a suitable value of may require some trial and error.

The surface is divided into a total of $(s + 2)(t + 2)$ regions R_{kr}, corresponding to values of the surface parameters u, v in the ranges $u_k \le u \le u_{k+1}$, $v_r \le v \le v_{r+1}$ where $u_k = k / (s + 2)$ and $v_r = r / (t + 2)$ $(0 \le k \le s + 2, 0 \le r \le t + 2)$. One bit of the watermark will be embedded in each of the regions R_{kr} $(1 \le k \le s, 1 \le r \le t)$. We do not use the regions next to the boundary of the surface for embedding purposes, to avoid distortions at the surface edges.

We choose a reference vector **rv** based on the geometry of the surface. In the work done here, we take **rv** to be the vector joining opposite corners of the surface i.e. $\mathbf{rv = P(1, 1) - P(0, 0)}$. Other choices are possible. For example, one might take **rv** to be the average normal to the surface.

To embed the watermark bit w_{kr} in the surface region R_{kr}, we move the control points so that the scalar product $s_{kr} = \mathbf{rv.\ (P(u_{k+1}, v_{r+1}) - P(u_k, v_r))}$ is changed to $s_{kr} +$ $|s_{kr}|$.

We would like the change to the control points to be as small as possible, subject to the adjustments to the surface being carried out as described above.

Let $\Delta\mathbf{P_{ij}} = (\Delta x_{ij}, \Delta y_{ij}, \Delta z_{ij})$ denote the changes to the control points. There is no need to move all the control points and we choose to take $\Delta\mathbf{P}_{ij} = \mathbf{0}$ when $i = 0$, $j = 0$, $i = n$ or $j = m$. We have the following optimization problem. We need to minimize $[(\Delta x_{ij})^2 + (\Delta y_{ij})^2 + (\Delta z_{ij})^2]$ subject to the constraints that $\mathbf{rv.\ (P`(u_{k+1}, v_{r+1}) - P`(u_k, v_r))} = s_{kr} +$ $|s_{kr}|$, where $\mathbf{P`(u, v)} = \sum^{n}_{i=0} \sum^{m}_{j=0} B_{ni}(u) B_{mj}(v)\ (\mathbf{P_{ij} + \Delta P_{ij}})$ and $s_{kr} = \mathbf{rv.\ (P(u_{k+1}, v_{r+1}) - P(u_k, v_r))}$, as defined above. This involves a total of st constraints on the 3 $(n - 1)(m - 1)$ independent variables $\Delta x_{ij}, \Delta y_{ij}, \Delta z_{ij}$ $(1 \le i \le n - 1, 1 \le j \le m - 1)$.

This minimization problem can be solved exactly. Introducing st Lagrange multipliers $_{kr}$, the usual theory leads to the following set of equations

$$2\Delta x_{ij} = \partial/\partial(\Delta x_{ij}) \left[\sum_{k,r} {}_{kr}\, s`_{kr} \right]$$

$$s`_{kr} = \mathbf{rv.\ (P`(u_{k+1}, v_{r+1}) - P`(u_k, v_r))}$$

After some calculation, this leads to

$$2\Delta x_{ij} = (\mathbf{rv})_x \sum_{k, r} {}_{kr}\, D(i, j, k, r)$$

$$D(i, j, k, r) =$$

$$B_{ni}(u_{k+1}) B_{mj}(v_{r+1}) - B_{ni}(u_k) B_{mj}(v_r)$$

Similar equations are obtained for Δy_{ij} and Δz_{ij}.

We can substitute these formulas for Δx_{ij}, Δy_{ij} and Δz_{ij} in the constraints, leading in turn to the following system of equations for the Lagrange multipliers.

$$\tfrac{1}{2} \sum_{k,r} |\mathbf{rv}|^2 \, \lambda_{kr} E(c, d, k, r) = w_{cd} |s_{cd}|$$

$$E(c, d, k, r) = \sum_{i,j} D(i, j, k, r) \, D(i, j, c, d)$$

This is a linear system of st equations for the multipliers, which is readily solved. The values of Δx_{ij}, Δy_{ij} and Δz_{ij} can then be found from the earlier equations.

4. IMPROVEMENTS AND ENHANCEMENTS

The general embedding strategy described above was kept simple in the interests of clarity. In practice, some straightforward modifications are needed in order to obtain a system that can be used in practice.

The process of solving for the multipliers using e.g. Gauss reduction, can give problems if the number of equations is large. The embedding scheme described was found to fail if more than about 20 bits were embedded. This problem can be overcome by dividing the surface into sections and embedding 20 bits in each section. The whole process is linear so that the individual sections can be handled one at a time. This ensures that the number of equations to be solved never becomes too large.

In the scheme described, we made use of all of the regions R_{kr} when embedding the watermark bits. This results in excessive distortion to the surface, preventing the use of a higher embedding strength. In practice, one would make use of a very large number of regions, not all of which would be used to embed a bit. Instead, one can use a random number generator to select st of the regions for the actual embedding. The key for the generator can be made available at the detector. Apart from allowing greater embedding strengths, this procedure provides added security, as an attacker will not know which regions contain the embedded bits. Indeed, if the regions used are known to an attacker, the watermark can be removed by simply undoing the embedding steps.

The use of a single reference vector **rv** to embed all the bits might allow for statistical attacks that determine the direction in which the control points have been moved. This can be dealt with by using several reference vectors. In the extreme case, we could use a different reference vector to embed each bit, with the directions of these vectors again obtained using a random number generator.

Implementation of these enhancements involves only a straightforward modification to the theory described above.

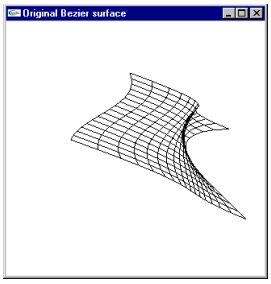
5. WATERMARK DETECTION

There are two main types of watermark detection described in the literature. *Informed* detection occurs when the detector has access to the original image (i.e. the original control points in our case). *Blind* detection occurs when there is no such access. Blind detection uses statistical correlation to determine whether the watermark is present. The number of bits embedded by the system described above is too small to allow the use of statistical methods, so we implemented an informed detector. This successfully detected the watermark, even at the low embedding strengths used in the tests. The detector simply compares the original set of control points with the watermarked set, and extracts the watermark in a straightforward manner.

If the scheme is enhanced to allow a larger number of bits to be embedded, then the use of a blind detector becomes feasible.

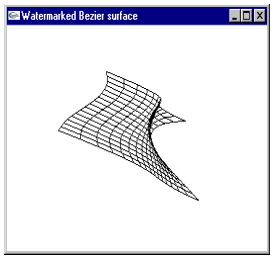
6. EXPERIMENTAL RESULTS

In order to test out the basic system described in Section 3, we made use of a simple Bezier surface taken from [4]. This surface has 16 control points, laid out in a 4 by 4 grid (i.e. n = m = 3.)

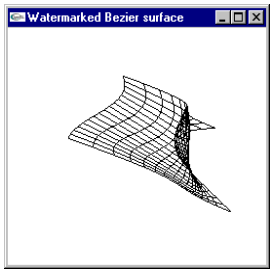


Original Bezier surface

This surface was watermarked by embedding 16 bits, using various values of the embedding strength .



Watermarked Bezier surface with = 0.01



Watermarked Bezier surface with = 0.1

It can be seen that when = 0.01 the visual appearance of the surface is not degraded, but that using the higher value 0.1 for the embedding strength causes a clearly visible distortion in the image. Watermark detection is successful in all cases, using an informed detector.

7. AN ALTERNATIVE APPROACH

There are many ways in which we can modify the geometry of the surface in order to embed a watermark. The scheme proposed above has the advantage that the changes to the control points can be determined exactly, and without excessive computation.

We have also investigated an embedding method that makes use of the normal directions to the surface. As a reference vector for this method, we let **rv** be the average normal to the surface. For each region R_{kr}, let $\mathbf{n}_{kr}$ be the average normal to the surface taken over that region. This scheme now moves the control points (minimally) so that $\mathbf{rv}.\mathbf{n}_{kr}$ changes to $\mathbf{rv}.\mathbf{n}_{kr} + w_{kr} |\mathbf{rv}.\mathbf{n}_{kr}|$. As is readily observed, this system is very similar in theory to that already described. However, this approach leads to a nonlinear system of equations that cannot be solved exactly. An attempt to solve the optimization problem using simulated annealing was only partly successful, in that it worked for some surfaces but not others. Furthermore, this approach proved to be computationally very expensive. It was found, however, that in those cases where it worked, higher embedding strengths were achieved without excessive distortion to the surface. Further investigation is needed.

8. CONCLUSION

Results obtained so far indicate that the basic watermarking scheme proposed for Bezier surfaces does at least satisfy the basic requirements of a watermarking scheme. A detectable watermark can be embedded in a manner that does not significantly degrade the visual appearance of the surface. Furthermore, the watermark remains detectable in the presence of many geometric transformations of the surface, including rotation and translation. Further testing and refinement is in progress. In particular, the variations and enhancements described in Section 4 need to be implemented, so that a larger payload can be embedded allowing the implementation of a blind detector. Other systems that modify the geometry of the surface, such as that proposed in Section 7, are also receiving attention.

REFERENCES

[1] O Benedens, Geometry-Based Watermarking of 3D models, *IEEE Computer Graphics, Special Issue on Image Security, pp46-55*, January/February 1999.

[2] O Benedens, Watermarking of 3D polygon based models with robustness against mesh simplification, *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, pp 329-340, 1999.

[3] Ingemar J Cox, Matthew L Miller, Jeffrey A Bloom, Digital Watermarking, *Academic Press* 2002.

[4] Jackie Neider, Tom Davis and Mason Woo, OpenGL Programming Guide ("The Red Book"), *Addison Wesley*, 1993.

[5] R Ohbuchi, H Masuda and M Aono, Watermarking Three-Dimensional Polygonal Models, *ACM Multimedia 97*, pp261-272, 1997.

[6] E Praun, H Hoppe and A Finkelstein, Robust Mesh Watermarking, *SIGGRAPH 99, Proceedings*, pp 69-76, 1999.

Biographical Note-- The primary author has lectured extensively in both mathematics and computer science and is currently associate professor of computer science at the University of Fort Hare