WATERMARKING OF 3D MODELS USING PRINCIPAL COMPONENT ANALYSIS

A. Kalivas, A. Tefas and I. Pitas

Department of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 540 06, GREECE, pitas@zeus.csd.auth.gr

ABSTRACT

A novel method for 3D model watermarking robust to geometric distortions such as rotation, translation and scaling is proposed. A ternary watermark is embedded in the vertex topology of a 3D model. A transformation of the model to an invariant space is proposed prior to watermark embedding. Simulation results indicate the ability of the proposed method to deal with the aforementioned attacks giving very good results.

1. INTRODUCTION

In the last decades, many new technologies for representation, storage and distribution of digital media information became available. Furthermore, the amount of digital data distributed through international networks like Internet, has increased rapidly. The danger of copying, tampering and transmitting copyrighted data through these networks, generated an increased demand for robust methods of copyright protection and ownership security.

A new important element in security research aimed at protecting intellectual property rights and data ownership is information hiding [1]. A large amount of systems has been proposed for the watermarking of 2D image data and sound, addressing with a varying success the existing difficulties, but few methods have been proposed for watermarking of 3D models. Watermarking of 3D models gains a lot of popularity due to the increased processing power of today's computers and the demand for a better representation of virtual worlds and scientific data.

A first algorithm for embedding affine invariant watermarks is proposed in [2]. It is named *Tetrahedral Volume Ratio Embedding* and uses the ratio of volume of tetrahedrons generated from three neighbor triangles along the range of triangles in a model.

Praun et al. [3] presented a technique for embedding secret watermarks, using a spread spectrum technique. The algorithm is robust against many attacks but requires significant assistance from the user, by supplying not only the original model but also by manual compensation for all affine transforms.

Benedens et al. presented a technique for embedding secret watermarks robust against remeshing and more specifically triangle reduction attacks, named *Normal Bin Encoding* [4]. The method needs a model reorientation to provide successful detection. A second proposed method, *Affine Invariant Embedding*, withstands geometrical transforms but needs extra information, for the detection, appended to the secret key.

In this paper, a novel technique for 3D model watermarking robust against geometric transforms is proposed. It is based on an still image watermarking technique [5]. The algorithm uses the center of mass and the principal component of the model in order to transform the data to a space, which is not affected by geometric transformations, such as translation, rotation and scaling.

2. 3D SURFACE WATERMARKING

2.1. Transform of the 3D surface

A 3D model is comprised of a set of vertices $\mathbf{V}$ and a set of connections between these vertices. Each vertex $\mathbf{v}_i$ has three coordinates in the cartesian space, $\mathbf{v}_i = \{x_i, y_i, z_i\}$. The purpose of the transform is to convert the 3D data to a 1D signal so that the embedding of the watermark can be then applied. The resulting space is invariant to rotation, translation and scaling of the 3D model and thus robustness against these attacks is achieved. A description of each step of the transform follows.

- **Center of Mass Calculation**. To find the center of mass the following equation is used

$$\mathbf{K} = \frac{1}{N} \sum_i \mathbf{v}_i \tag{1}$$

  where $\mathbf{v}_i$ is vertex i

- **Model Translation**. The model is translated so that the center of mass falls on the center of the axes.

$$x_i^{'} = x_i - k_x$$

This work has been supported by the European Project IST-1999-10987 CERTIMARK

$$y_i^{'} = y_i - k_y \qquad (2)$$
$$z_i^{'} = z_i - k_z$$

where k_x, k_y and k_z are the coordinates of the center of mass, x_i, y_i and z_i are the original coordinates of vertex $\mathbf{v}_i$ and $x_i^{'}$, $y_i^{'}$ and $z_i^{'}$ are the coordinates of the translated vertex $\mathbf{v}_i^{'}$. That way the watermarking method is robust against translation of the model under investigation.

- **Principal Component Calculation**. The principal component $\mathbf{u}$ of the vertices is the eigenvector that corresponds to the greatest eigenvalue of the covariance matrix C of the vertices coordinates. The covariance matrix C is calculated in the following way:

$$C = \begin{bmatrix} \sum_{i=0}^{N} x_i^2 & \sum_{i=0}^{N} x_i y_i & \sum_{i=0}^{N} x_i z_i \\ \sum_{i=0}^{N} x_i y_i & \sum_{i=0}^{N} y_i^2 & \sum_{i=0}^{N} y_i z_i \\ \sum_{i=0}^{N} x_i z_i & \sum_{i=0}^{N} z_i y_i & \sum_{i=0}^{N} z_i^2 \end{bmatrix} \qquad (3)$$

where x_i, y_i and z_i are the coordinates of the vertex $\mathbf{v}_i$.

- **Model Rotation**. The model is rotated so that $\mathbf{u}$ coincides with the z axis. Thus robustness against rotation of the watermarked model is achieved.

- **Conversion to Spherical Coordinates**. The model is converted to Spherical Coordinates. Each vertex is represented as (r, θ, ϕ). This is done in order to achieve robustness against scaling by embedding the watermark in the r component of each vertex.

Robustness to translation, rotation and scaling is achieved by applying the described transformation prior to watermark detection. The signal $r(\theta)$ is formed and is used in the embedding procedure. All the extra information in the original signal is discarded.

2.2. Watermark Generation and Embedding

The watermark generation procedure aims at generating a three-valued watermark $w(\theta) \in \{-1, 0, 1\}$, from the transformed signal of the vertices $r(\theta)$, given a digital key K. The algorithm uses the digital key as a seed for a gaussian random number generator. The mean and variance of the θ angles of the model vertices are the parameters of the generator that produces the watermark.

Watermark embedding is performed by altering the transformed signal according to the following formula:

$$r_w(\theta) = \begin{cases} r(\theta) & \text{if } w(\theta) = 0 \\ g_1(r(\theta), N(\theta)) & \text{if } w(\theta) = 1 \\ g_2(r(\theta), N(\theta)) & \text{if } w(\theta) = -1 \end{cases} \qquad (4)$$

where g_1, g_2 are suitably designed functions based on θ and $N(\theta)$ denotes a function that depends on the neighborhood of θ. The functions g_1, g_2 are called *embedding functions* and they are selected so as to define an inverse detection function $G(r_w(\theta), N(\theta))$. The detection function, when applied to the watermarked model $r_w(\theta)$, gives the watermark $w(\theta)$:

$$G(r_w(\theta), N(\theta)) = w(\theta) \qquad (5)$$

Obviously several embedding functions and the appropriate detection function can be designed giving different watermarking schemes. The function that is used in our method is based on the values of the neighboring surface vertices of the vertex to be modified.

$$g_1(r(\theta), N(\theta)) = N(\theta) + a_1 r(\theta) \qquad (6)$$
$$g_2(r(\theta), N(\theta)) = N(\theta) + a_2 r(\theta) \qquad (7)$$

where a_1, a_2 are suitably chosen constants and $N(\theta)$ is a local neighborhood operation of the vertices around $r(\theta)$. The sign of a_1, a_2 is used for the detection function and its value determines the watermark power.

2.3. Watermark Detection

In the watermark detection procedure we generate first the watermark $w(\theta)$ according to the watermark key K. Afterwards the model under investigation is transformed according to the transformation presented in Section 2 and the signal under investigation $r_w(\theta)$ is formed. The detection function resulting from (6),(7) is defined by:

$$G(r_w(\theta), N(\theta)) = \begin{cases} 1 & \text{if } r_w(\theta) - N(\theta) > 0 \\ -1 & \text{if } r_w(\theta) - N(\theta) < 0 \end{cases} \qquad (8)$$

The detection function is valid if $a_1 > 0$ and $a_2 < 0$. This fact should be accounted for, in the design of the embedding functions. By employing the detection function in the transformed watermarked signal $r_w(\theta)$, a bi-valued detection signal $d(\theta)$ is produced:

$$d(\theta) = G(r_w(\theta), N(\theta)) \qquad (9)$$

Based on the watermark $w(\theta)$ and the detection signal $d(\theta)$, we can decide whether the watermark under investigation is embedded in the model or not. The detection is based on the value by value comparison for the nonzero samples in $w(\theta)$. By comparing the watermark $w(\theta)$ and the detection signal $d(\theta)$ we form the false detection signal:

$$e_w(\theta) = \begin{cases} 1 & \text{if } w(\theta) \neq 0 \text{ and } w(\theta) \neq d(\theta) \\ 0 & \text{otherwise} \end{cases} \qquad (10)$$

The false detection signal has value 1 if a watermarked vertex is falsely detected and 0 otherwise. The detection ratio is given by the ratio of the correctly detected vertices to the sum of the watermarked vertices in the 3D model.

$$D_w = 1 - \frac{\text{card}\{e_w(\theta)\}}{\text{card}\{w(\theta)\}} \qquad (11)$$

The embedding functions are designed in such way, so as the probability p of a pixel to be detected as signed with g_1 or g_2, for an unwatermarked model, to be 0.5. Thus, the detection ratio in an unwatermarked model forms a binomial distribution. The cumulative distribution function (*cdf*) of the watermark detection ratio is given by:

$$P_n = p^k \sum_{i=0}^{n} \frac{k!}{i!(k-i)!} \tag{12}$$

where k is the total number of the watermarked vertices and n is the number of correctly detected watermarked vertices.

The decision about the image ownership is taken by comparing the watermark detection ratio of the model to a predefined threshold T. The value of the threshold determines the minimum acceptable level of watermark detection.

3. WATERMARKING ALGORITHM PERFORMANCE

To evaluate the performance of the algorithm we use two measures. For the visual quality of the model we use the SNR, and for its robustness the ROC curves are evaluated. A more detailed description follows.

3.1. SNR measure

To measure the SNR of a 3D model the following formula is used:

$$SNR = \frac{\sum_{i=0}^{N-1} x_i^2 + y_i^2 + z_i^2}{\sum_{i=0}^{N-1} (x_i^{'} - x_i)^2 + (y_i^{'} - y_i)^2 + (z_i^{'} - z_i)^2} \tag{13}$$

where x_i, y_i and z_i are the coordinates of vertex $\mathbf{v}_i$ before the embedding of the watermark and $x_i^{'}$, $y_i^{'}$ and $z_i^{'}$ are the coordinates of the same vertex after the embedding of the watermark.

3.2. ROC Curves

The decision on whether there is a watermark in the model, is taken by comparing the detection ratio D_w to the threshold T. For a given threshold, the performance of the system can be expressed as a function of the false alarm probability $P_{fa}(T)$ (i.e. the probability of detecting a watermark on a non watermarked model or a watermarked model with another key) and the false rejection probability $P_{fr}(T)$ (i.e. the probability of not detecting a watermark in a watermarked model using the correct key):

$$P_{fa}(T) = Prob(D_w > T|H_1) \tag{14}$$

$$P_{fr}(T) = Prob(D_w < T|H_0) \tag{15}$$

where H_0 is the hypothesis that the watermark exists in the model and H_1 is the hypothesis that the watermark under investigation doesn't exist in the model.

In an ideal case, there should be a threshold T so that P_{fa} and P_{fr} are both zero. The values of P_{fa} and P_{fr} can be calculated using the following formulas:

$$P_{fa}(T) = \int_{T}^{\infty} f_{D_w|H_1}(t)dt \tag{16}$$

$$P_{fr}(T) = \int_{-\infty}^{T} f_{D_w|H_0}(t)dt \tag{17}$$

These two equations can be solved for the independent variable T and as a result P_{fa} can be expressed as a function of P_{fr}. This function forms the receiver operating characteristic (ROC) curve of the watermarking system. The operating stage where $P_{fa} = P_{fr}$ is called equal error rate (EER) and is used as a quantitative estimation of the algorithm robustness.

We assume a Gaussian distribution for both $f_{D_w|H_0}$ and $f_{D_w|H_1}$ and we calculate their means $\mu_{D_w|H_0}$, $\mu_{D_w|H_1}$ and variances $\sigma^2_{D_w|H_0}$, $\sigma^2_{D_w|H_1}$

We can then use the following formula for evaluating the ROC curve.

$$P_{fa} = \frac{1}{2}[1 - erf(M)] \tag{18}$$

where M is given by:

$$M = \frac{\sqrt{2}\sigma_{D_w|H_0} erf^{-1}(2P_{fr} - 1) + \mu_{D_w|H_0} - \mu_{D_w|H_1}}{\sqrt{2}\sigma_{D_w|H_1}} \tag{19}$$

4. EXPERIMENTAL RESULTS

The proposed approach was evaluated using a series of tests based on geometrical transformations. The models used for the testing were Startrek, Turtle and Klingon. The tests were realized on a Celeron 433 machine and both the embedding and detection procedures were found to take approximately 3 seconds. This is sufficiently fast for commercial applications and the speed of the application can be improved if it is further optimized. The original model Startrek and the watermarked model with embedding parameter equal to 0.005 for 100 watermarked vertices are shown in Figures 1 and 2, respectively.

The geometrical attacks that were tested are translation, rotation and uniform scaling. Due to the invariance properties of the transform that is applied to the model prior to watermark embedding and detection, the results for these attacks were identical to the ones produced when no attack is performed. The watermark embedding strength is related to the constants a_1 and a_2 and for the tests we used

Fig. 1. Startrek original model

Fig. 2. Startrek model with 100 watermarked vertices. Embedding strength was 0.5%

$a_1 = -a_2$. Several tests were conducted using various values for the embedding parameters. The values $a_1 = 0.005$ and $a_2 = -0.005$ proved to be a good compromise between visual quality and performance. As shown in [5] the minimum detection threshold T that can be used for the algorithm depends on the length of the watermark $w(\theta)$. The value of T increases as the amount of non zero watermark samples decreases. We have tested the algorithm for many watermark lengths and found that a size of at least 100 samples gives good results even for small models. Of course the performance is improved if we increase the size of the watermark.

The ROC curves of the model Startrek are illustrated in Figure 3. The ROCs were evaluated using 1000 different watermark keys for estimating the corresponding P_{fa} and P_{fr}. The value of the embedding parameters a_1, a_2 and the number of watermarked vertices was 100 and 200. It is obvious that the proposed algorithm attains very good performance in both cases and the EER is smaller than 10^{-10}, even for 100 watermarked vertices. The measured SNR was 120dB for the first case and 126dB for the second.

5. CONCLUSIONS

A novel 3D model watermarking method has been presented. A transform that makes the proposed method completely immune to geometrical attacks like rotation, translation and scaling has been proposed. The algorithm also

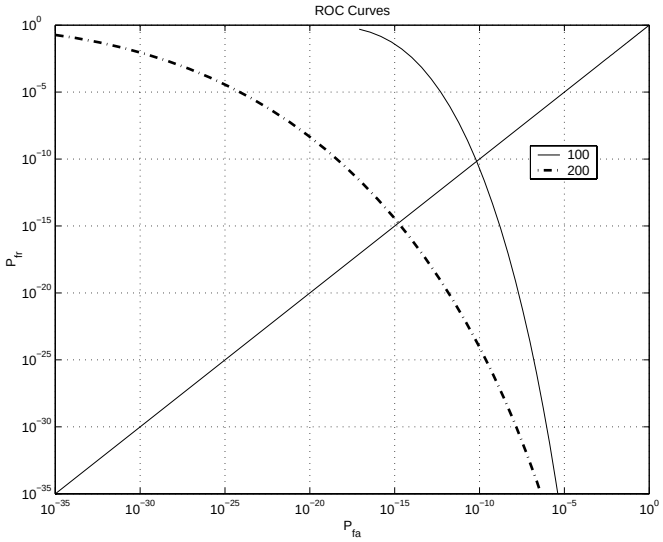

Fig. 3. ROC curves for Startrek model with 100 and 200 watermarked vertices

proved to give good results even for small embedding strengths and short watermark lengths. The major advantage of the proposed method is its robustness against the aforementioned geometric distortions.

6. REFERENCES

[1] F.A.P. Petitcolas, R.J Anderson, and M.G. Kuhn, "Information hiding - a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, July 1999.

[2] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygonal models through geometric and topological modifications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, May 1998.

[3] E. Praun, H. Hoppe, and A. Finkelstein, "Robust mesh watermarking," in *SIGGRAPH 99 Proceedings*, 1999, pp. 69–76.

[4] O. Benedens and C. Busch, "Towards blind detection of robust watermarks in polygonal models," in *Eurographics 2000 Conference Procceedings*, August 2000, pp. 199–209.

[5] A. Tefas and I. Pitas, "Robust spatial image watermarking using progressive detection," in *Proc. of 2001 IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP 2001)*, Salt Lake City, Utah, USA, 7-11 May 2001.