Robust Zero-Watermarking Algorithm for CAD Models

Nan Liu, Sanyuan Zhang, Yin Zhang
College of Computer Science and Technology
Zhejiang University
Hangzhou 310027
P.R. China
saviorlan@yahoo.com.cn, syzhang@cs.zju.edu.cn, yinzh@zju.edu.cn

Journal of Digital Information Management

ABSTRACT: *Copyright protection and authentication of digital contents have become a significant issue in the current digital epoch with efficient communication mediums such as Internet. Digital watermarking technique is now one of the hot research fields of copyright protection for CAD graphic data under the network environment. But there are very limited techniques available for that because of its high shape-preserving demand. Zero-watermarking is such a good means to deal with it and it has lots of advantages such as high capacity, good robustness and various functions. In this paper, we will discuss zero-watermarking algorithm for CAD models and eventually propose a watermarking-based digital rights management system that would test our techniques.*

Categories and Subject Descriptors:
C.3 [SPECIAL-PURPOSE AND APPLICATION-BASED SYSTEMS]: Real-time and Embedded Systems; D.2.9 **[Management]**: Copyrights

General Terms:
Watermarking, Computer-aided Design, Copyright

Keywords: Zero-watermarking, NURBS, Chaos, CAD, Copyright, Embedded Design

Received: 4 February 2013, Revised 28 March 2013, Accepted 2 April 2013

1. Introduction

With the development of digital technology and the Internet, various kinds of multimedia digital products have been distributed on the network, but the convenience and insecurity of digital products co-exist. How to protect the digital copyright and guarantee the information security have now become the significant issues, while digital watermarking technology became a primary means of selection.

2. Related Work

Since Ohbuchi et al. [1, 2] introduced the watermarking algorithms for mesh models in 1997, 3D digital watermarking technology has been rapidly developing. Harte et al. [3] suggested the watermarking embedding algorithm by adjusting the relative positions of vertices in the ring neighborhood; Kanai et al. [4] described an algorithm that employs multiresolution wavelet decomposition of 3D polygonal mesh models for data embedding; Qi et al. [5] proposed algorithm by embedding watermarks into the bottom nodes of octree.

Till now there has not been much discussion on the watermarking of 3D NURBS models. For example, Ohbuchi et al. proposed two algorithms. One [6] embeds information into the knot equations by knot reparameterization. This algorithm has merits that the resulting NURBS model has exactly the same shape as the original one, and that the number of knots and control points are unchanged. But the embedded information can be detected only when one has the original model because it is embedded into the coefficients of the function that reparameterizes the original knot vector. Moreover, the maximum number of embedded data is only three, which is the degree of freedom of bilinear function, and a slight

modification of the knots and control points makes it impossible to detect the information. The other algorithm [7] embeds the information into the absolute position of newly inserted knot. But it also needs the original model to detect the watermark, and this makes it hardly be widely spread. Aiming at these drawbacks, Jae Jun Lee et al. [8] proposed two 3D NURBS watermarking algorithms. In these algorithms, a virtual NURBS model is first generated from the original one. Instead of embedding information into the parameters of NURBS data as in the existing algorithm, they extract several 2D images from the 3D virtual model and apply the 2D watermarking methods. This new idea makes the watermarking more capacity and more robust against lots of attacks. But the slight modification of shape seems intolerable in those CAD applications that need high precision.

CAD models are easier to copy, reproduce and tamper. They require specialized copyright protection and authentication solutions. Traditional watermarking algorithms modify the contents of the digital medium to be protected by embedding a watermark. This traditional watermarking approach is not applicable for CAD models. A specialized watermarking approach such as zero-watermarking would do the needful for CAD models. In this paper, we propose a novel zero-watermarking algorithm which utilizes the NURBS data of CAD models. This algorithm does not change the geometry data of original CAD models, but utilize the characters of original data to construct original watermark information. I'll show you how this algorithm works in the next section.

3. Our Zero-Watermarking Algorithm

CAD models are usually organized in Breps of NURBS primitives such as NURBS curves or surfaces. In our algorithm we first select some specific NURBS primitives as the watermark carriers. Then watermark is generated through the chaotic map to the knot vector of these primitives and register it to DRM (Digital Rights Management) with time stamped. The specific procedure shown in Figure 1 will be explained in the subsections.

3.1 Selecting NURBS Primitives

There are lots of ways to select NURBS primitives. First we should order the NURBS primitives, and such ordering can be achieved by using the topology of objects in CAD models for example, by creating a spanning tree of surface patches and traversing the tree in a depth-first order. And select the "*important*" nodes of tree to watermark, here "*important*" nodes mean the importance in the topology. So the watermarks can't be easily deleted by the removal of these primitive. Moreover, In order to increase the watermarking security and the resistance against cut attacks, we could employ the scrambling transform to decide the watermarked position.

3.2 Time Stamp Authentication Technique

The time stamp plays the role as the postmark, which provides exact time evidence for any digital file, in order to prove that it exists from that moment. Assuming that the author asked for the DRM (Digital Rights Management) to get his works time-stamped before publishing it, so the CAD model, the copyright watermark and the time stamp were bound together to prove that the author owns his works. When the attackers wants to watermark the works and declare the copyright, the time stamp must be later than the author's one. Therefore we could determine the copyright when multiple watermarks found according to the time stamp in the watermarks.

3.3 Generating Watermarks

The NURBS data is consist of the knot vector, the control points and its weights. We choose the knot vector to generate watermarks since it does not change when the model is affine transformed. Figure 1 shows the concrete process of our algorithm.

1. We select the primitives to watermark as the way mentioned before.

2. Given the knot vector, we transform it to a binary sequence A_i with chaotic map [9].

3. We compute the bitwise exclusive-OR of the copyright watermark W_i with A_i and we get the zero-watermark W_a:

$$W_a = W \oplus A$$

4. This zero-watermark is then encrypted using a secret key Ks and delivered to TSA (Time Stamp Authority) to ask for time stamp. If it succeeds for time stamp, a time stamped watermark W_a' is finally generated and registered to DRM.

3.4 Detecting Watermarks

The procedure of detecting watermarks is the reverse procedure of generating watermarks.

1. We select the primitives to watermark as the same way mentioned before.

2. Given the knot vector, we transform it to a binary sequence A_i'.

3. We use the secret key to decrypt the time stamped watermark and get the zero-watermark W_a and the time stamp.

4. We compute the bitwise exclusive-OR of the zero-watermark W_a with A_i' and we get the detected copyright watermark W':

$$W' = W_a \oplus A$$

5. We finally compare the W' with W by computing the correlation coefficient. And we conclude that it is watermarked if NC is larger than some threshold T.

$$NC(W, W') = \frac{\sum w_j w_j'}{\sum w_j^2}$$

4. System Design and Implementation

The system is designed and implemented in our multiple

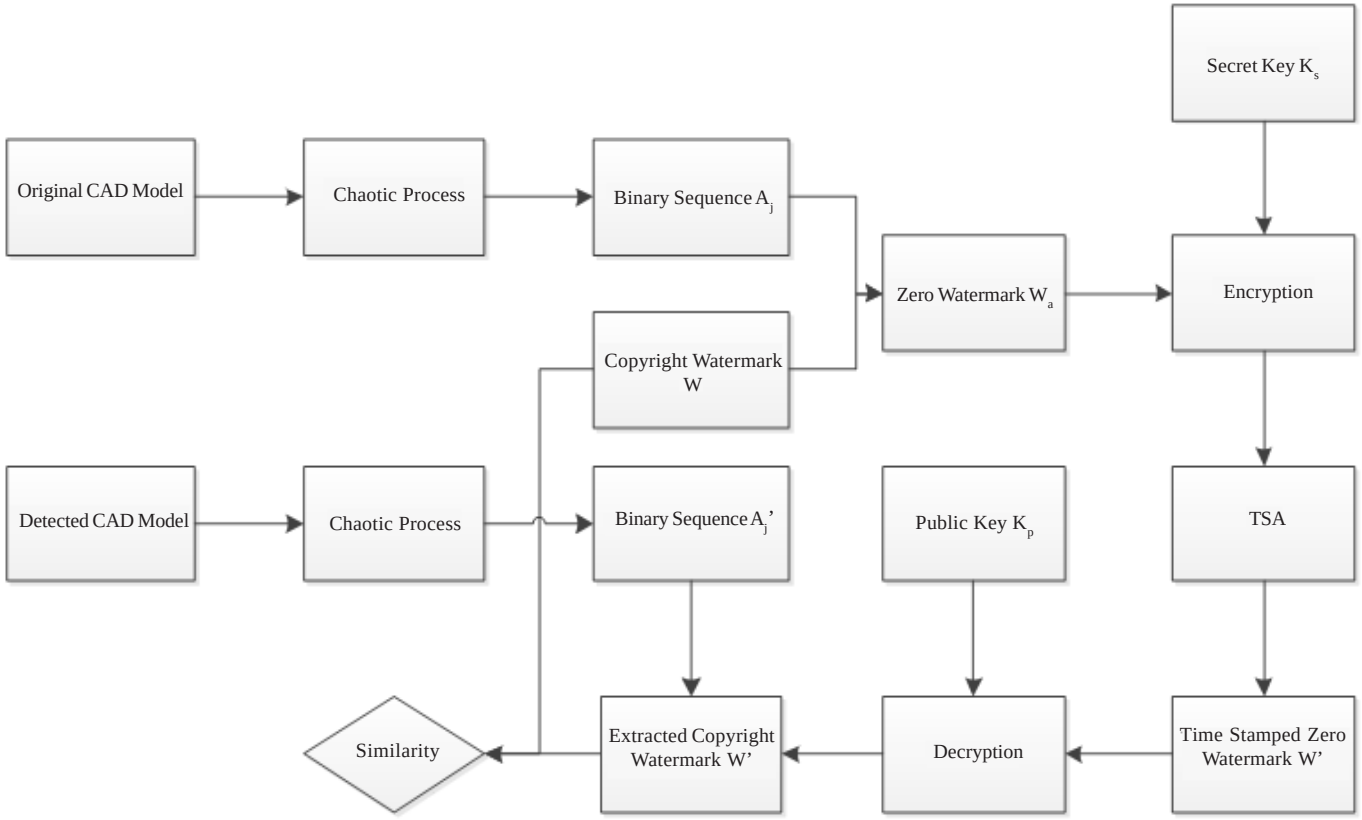

Figure 1. Zero Watermarking Generating and Detecting Algorithm Diagram

watermarking-based digital rights management model [10]. Figure 2 shows how this model works in details.

When A decides to authorize the publisher B to sell his copy of the works, he need apply to R for authorization registration. R verifies the copyright ownership of A and uses the private key K_r and the identifier M_b which is the unique identifier indicating B to generate a second robust watermark W_b. R provides B the dual watermarked X_{ab} as the master copy to publish and sends B a signed digital certificate as the authorization proof. B could also use the public key K_p and the watermark detecting software to test the works X_{ab}. The publisher could protect his own rights and interests through W_b while W_a proves the authorization legality of A.

If it is a non-exclusive license, A can also apply different watermarks to authorize other publishers B_i. Similarly, publishers can also authorize sub-publishers as long as they apply to R for the corresponding watermarks. Any sub-publishers can use the public key K_p and the watermark detecting software to test it.

When the publisher B sells the copy to the user C, he needs apply to R for a trade registration. R uses the private key K_r and the identifier M_c to generate a third robust watermark W_c. B sends C the triple watermarked works X_{abc} and gives A a royalty income. C could use the public key K_p and the watermark detecting software testing the works X_{abc} to confirm his own user authority. The user C can also directly visit the database to purchase and download the works which R embeds a user watermark into. R should also give A a royalty income.

The system features that: the copyright holders (including the above authors, authorized publishers and authorized users, etc.) have a strict division of the right level, and different levels of rights holders can apply to the digital rights management for the corresponding digital watermarks using the registration rights according to their rights.

5. Conclusion

In this paper, we have discussed a zero-watermarking algorithm for CAD models. This algorithm exactly preserves the shape of CAD models since it does not change the geometry data at all. Also it is robust against affine transform since that does not modify the knot vector. We then explained how it works in the designed system in detail. This system provides many security services including copyright protection, copy tracking, profit distribution and so on. It guarantees the rights and interests of copyright owners, publishers and also the users. But this multiple watermarking-based system can only deal with the copyright issues technically to some degree; the support by law is also necessary and need to get more attentions as quick as possible.

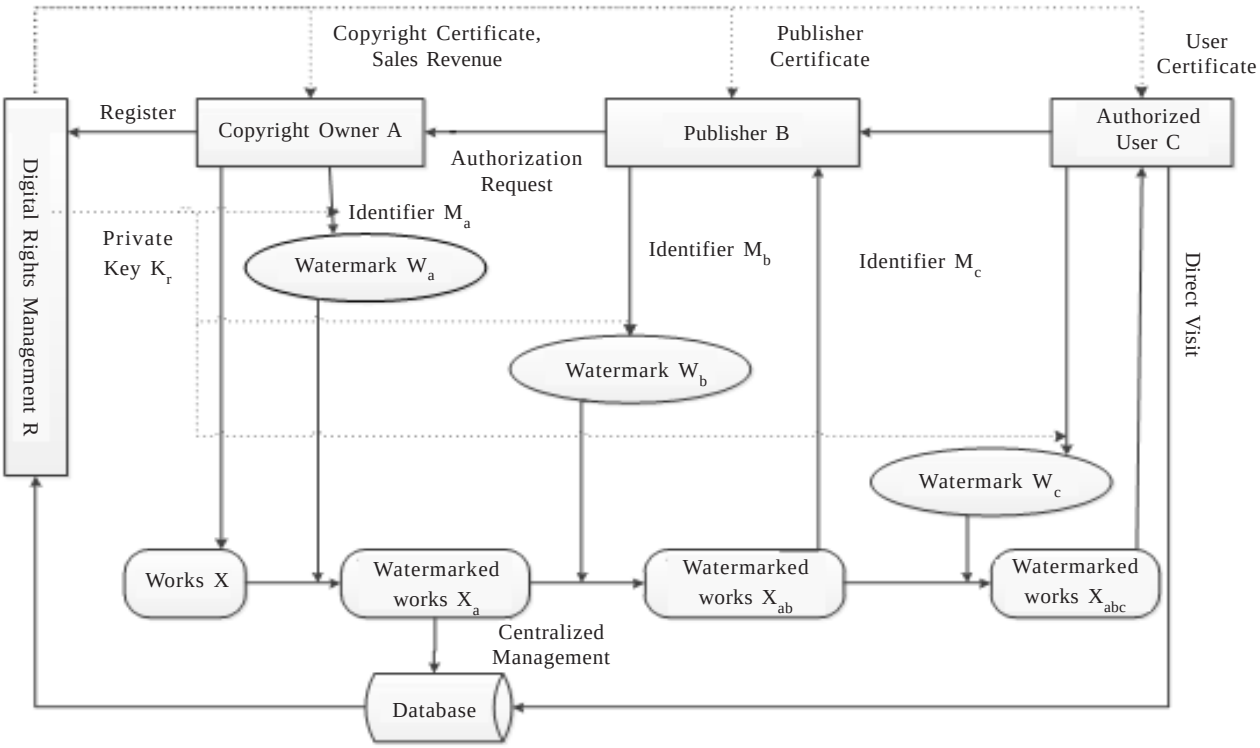

Figure 2. A Multiple Watermarking-Based Digital Rights Management Model

6. Acknowledgment

This work is supported in part by NSFC (No. 61272304), Zhejiang Provincial Natural Science Foundation of China (No. Y1090597) and Program for production-university-academe of Guangdong province joint with ministry of education (No.2011B090400546).

References

[1] Ohbuchi, R., Masuda, H., Aono, M. (1997). Embedding data in 3D models. *In*: Proceedings of the 4th International Workshop on Interactive Distributed Multimedia Systems and Telecommunication Services, Darmstadt, p.1-10.

[2] Ohbuchi, R., Masuda, H., Aono, M. (1997). Watermarking three-dimensional polygonal models. *In*: Proceedings of the ACM International Conference on Multimedia, Seattle, p. 261-272.

[3] Harte, T., Bors, A. G. (2002). Watermarking 3D models. *In*: Proceedings of International Conference on Image Processing, Rochester, p. 661-664.

[4] Kanai, S., Date, H., Kishinami, T. (1998). Digital Watermarking for 3D Polygons using Multiresolution Wavelet Decomposition. *In*: Proceedings of the Sixth IFIP WG, Tokyo, 5, p. 296-307.

[5] Qi Yue, Shu Jun, Shen Xukun, et al. (2008). Octree-based blind watermarking on 3D meshes. *Journal of Beijing University of Aeronautics and Astronautics*, p. 331-335.

[6] Ohbuchi, R., Masuda, H., Aono, M. (1999). A shape-preserving data embedding algorithm for NURBS curves and surfaces. *In*: Proceedings of COMPUTER GRAPHIC INTERNATIONAL, Canmore, p. 180-187.

[7] Ohbuchi, R., Masuda, H. (2000). Managing CAD data as a multimedia data type using digital watermarking, *In*: IFIP WG 5.2 Fourth Workshop on Knowledge Intensive CAD, p. 103-106, .

[8] Jae Jun Lee, Nam Ik Cho, Jong Weon Kim. (2002). Watermarking for 3D NURBS graphic data. Multimedia Signal Processing, *IEEE Workshop*, p. 304-307, .

[9] Liu Nan, Zhang Yin, Chen Zhiyang, Zhang Sanyuan. (2009). Chaos-Based Semi-Blind Watermarking for CAD Models. WRI Global Congress on Intelligent Systems, 3, 411-414.

[10] Liu Nan, Zhang Sanyuan, Zhang Yin. (2011). Multiple Digital Watermarking Techniques for CAD Models. Applied Mechanics and Materials, 88 – 89, 703-708.