

基于 B-Rep 的三维 CAD 模型盲水印算法^①

陈志杨, 贾筱菲

(浙江工业大学 计算机科学与技术学院, 杭州 310023)

摘要: 随着信息时代的到来, 数字水印不仅在版权保护、来源认证、私有探测领域受到了前所未有的重视, 而且在信息安全领域也引起了广泛的关注。提出了一种基于 B-rep 的 CAD 模型盲水印算法, 该算法主要针对 NURBS 曲线或曲面来嵌入水印, 能精确地保持模型的形状。首先遍历模型找到所有的 NURBS 曲线, 并将其依据曲线的长度进行排序, 然后利用相邻节点插入法将生成的水印嵌入到排好序的 NURBS 曲线中, 对半盲水印算法进行改进得到了盲水印算法, 从而在提取水印时不需要原始模型和原始的水印消息, 直接从相对应的 NURBS 曲线中进行水印提取, 最后通过比较提取出来的水印和原始水印的相似度来验证水印是否被篡改。实验表明该算法能够在模型中嵌入大容量的水印消息, 并减少了提取水印的时间。

关键词: 数字水印; 盲水印; 三维 CAD 模型; NURBS 基元; 版权保护

A Blind Watermarking Algorithm Based on B-rep for CAD Models

CHEN Zhi-Yang, JIA Xiao-Fei

(College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: With the appearance of informatization period, digital watermarking is attached importance to a great extent in these facts such as copyright protecting, source authentication, private detection and on, and becomes one hot research field of information security. This paper proposes a blind watermarking algorithm based on B-rep for CAD models, the algorithm embeds watermarking aiming at NURBS surfaces or curves, and its merit is preserving the model's shape exactly. Firstly, we go through the model for obtaining all NURBS primitives, and order these primitives by its length, then use interfacing knot insertion method to embed generated watermarking into ordered primitives. Semi-Blind watermarking is improved and becomes All-Blind watermarking, so we can directly extract watermarking from corresponding ordered NURBS curves, and don't need provide origin model and origin watermarking messages. At last, through comparing the similarity both the extracted watermarking and origin messages to test if this watermarking is distorted or not. Results show blind algorithm can embed high-capacity watermarking into models, and reduce the time of extracting watermarking.

Keywords: digital watermarking; blind watermarking; CAD models; NURBS primitives; copyright protecting

1 引言

数字水印技术——作为版权保护和认证来源的一种有效手段, 其实是一种信息隐藏技术, 主要是指将一段表明版权所有者的信息在不被感知的情况下嵌入到模型中, 以此达到保护产品版权和验证拥有者身份的目的。

随着越来越多的基于 CAD 的三维数据在互联网

上广泛传播, 那些通过网络来交付三维数据产品的版权人也急切需要版权保护, 因此数字水印技术在三维模型中的应用也与日俱增。但是由于 CAD 模型中能嵌入水印的载体较少, 并且嵌入的水印要抵抗住各种各样的几何或拓扑方面的攻击, 因此三维 CAD 模型的水印研究成为当前的一个难点和重点^[1]。

早期的数字水印研究集中在二维图像或影像的数

① 基金项目: 国家高技术研究发展计划(863)(2007AA04Z1A5)

收稿时间: 2010-07-14; 收到修改稿时间: 2010-08-13

字水印研究。1993 年 Caronni 第一次提出了数字水印技术的概念, 早期水印主要侧重于静止图像(如照片或计算机图形)的版权保护; 随后, Ohbuchi 提出了一些具有代表性的网格水印算法^[2]: TSQ 算法(三角形相似四元组)主要利用相似三角形的概念, 将相邻的 4 个三角形作为一个嵌入单元; TSPS 算法(剥离的三角形条带符号序列)的嵌入单元是一个三角形条带中的一对三角形的位置邻接关系^[3]; 文献[4]主要针对 NURBS 模型嵌入水印, 先抽取出对应的 2D 图像, 然后使用 2D 的水印算法进行嵌入和提取^[5]。

本文针对目前 CAD 模型数字水印需要提供原始水印信息等问题, 提出了无需原始水印信息的盲水印算法。在嵌入水印时先按体、面的层次来遍历 CAD 模型, 根据曲面类型来得到模型中所有的 NURBS 面, 此时得到的 NURBS 序列可能不是按重要特征顺序排列的, 若往其中添加水印时, 水印可能会更容易受到攻击和干扰, 为了抵抗这种攻击, 本文通过排序将杂乱的 NURBS 序列按从小到大的规模排序, 然后根据字符在原始消息中的位置来判断它应该嵌入在哪条 NURBS 曲线中, 此算法和现有的 CAD 模型水印算法的主要不同之处在于提取水印时不需要给出原始的 CAD 模型, 也不需要重新输入原始的水印信息, 而是先根据字符在消息中的位置, 去嵌入过程中按排序好的 NURBS 曲线序列中找到要进行水印提取的 NURBS 曲线, 然后得到相应曲线的属性并利用其节点向量来进行具体的水印提取, 最后将提取到的水印和原始消息进行对比来验证其是否经过篡改。文献[6]中的半盲算法在提取水印的过程中需要再次输入原始的水印消息, 也就需要再次遍历模型得到能容纳水印的 NURBS 面, 而本文的盲算法通过对文献[6]的算法进行改进, 提取水印时不再需要原始消息, 也就不需要再次遍历模型, 不需要再对杂乱的 NURBS 面进行排序, 这就大大加快了进程的执行, 提高了整个算法的效率; 本文算法对文献[6]算法的另一个改进是远远扩大了水印的容量, 文献[6]的算法是将水印嵌在一个 NURBS 曲线中, 而且水印的长度不能超过 7, 本文算法是将水印信息分段嵌入到好多个 NURBS 曲线中, 增加了水印容量, 足以满足日常应用中对水印容量的需求。本文第 2 节主要介绍各种水印的嵌入与检测过程。第 3 节详细说明了水印的生成、嵌入和提取以及整个算法的流程, 第 4 节进行了实验结果分析, 并对全文进行

了总结。

2 数字水印的嵌入与检测

三维模型数字水印按照水印检测过程所需的信息可以分为盲水印、半盲水印和非盲水印。在各种类型的水印中, 水印的嵌入与检测是一对逆过程。

2.1 非盲水印

非盲水印在检测过程中不仅需要知道原始水印信息, 还需要嵌入水印之前的原始模型, 这就大大限制了数字水印的应用。嵌入流程如图 1(a)所示, 在模型中嵌入水印后, 同时选中嵌入水印的面(绿色的面), 检测流程则见图 1(b)^[7]。

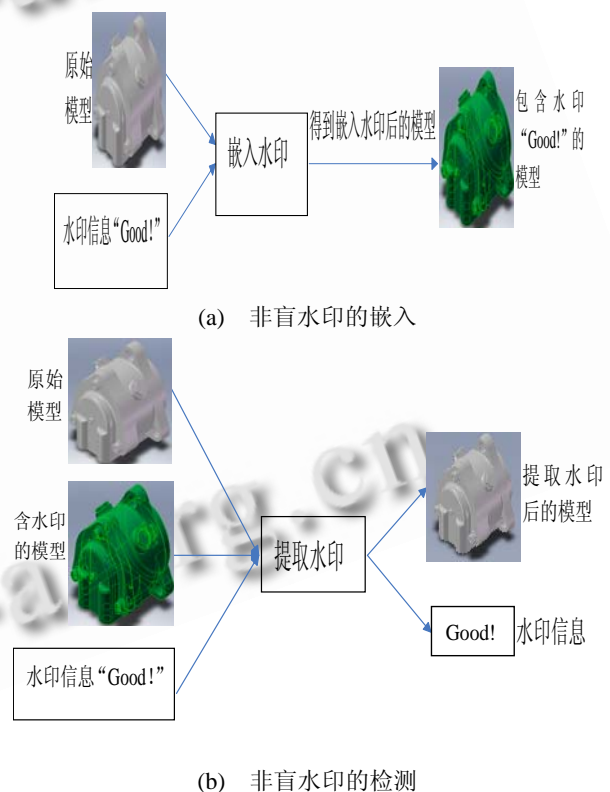


图 1 非盲水印的整个流程

2.1 半盲水印

半盲水印与非盲水印的区别在于, 检测时它不需要提供没嵌入水印的原始模型, 而只需要原始的水印消息, 且其抵抗攻击与干扰的能力较强, 这就为 CAD 模型的发布和传播创造了更加有利得条件。半盲水印的嵌入过程与非盲水印的嵌入相似, 这里不再给出, 图 2 是半盲水印提取的过程, 嵌入的水印是“Hello”。

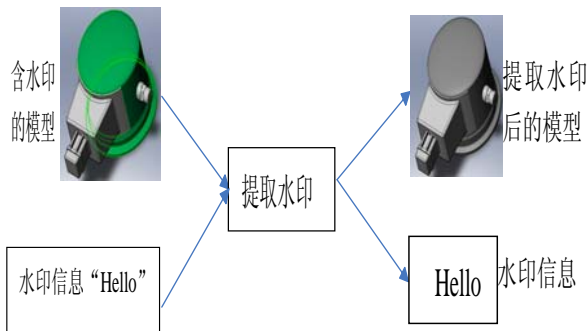


图2 半盲水印的提取

2.3 盲水印

盲水印指的是在检测时不需要原始模型的相关信息，仅仅根据待检测的含有水印的模型便可提取出水印信息，这个检测是先抽取后验证的过程，即先从嵌入水印的模型中提取出水印消息，再与已知的原始水印信息进行比较，若两者相等，则模型中存在该原始水印，且提取水印成功。这就可以进行版权保护，以免水印被篡改，该类型的水印易于传播，携带方便，且与半盲水印相比，在提取时不需要原始的水印消息，因此能提高水印提取的效率。同样盲水印的嵌入和非盲水印嵌入过程是相似的，图3表示的是盲水印的提取与检测过程，嵌入的水印是“World”。

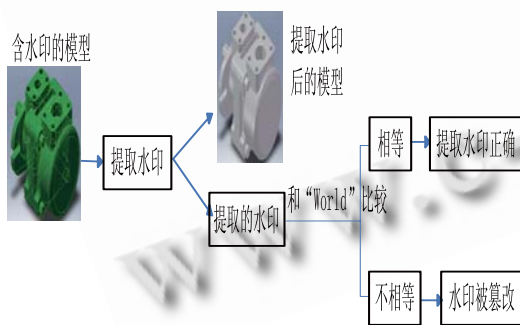


图3 盲水印的提取与检测

3 三维CAD模型数字水印

三维模型数字水印技术是数字水印技术的一个分支，其原理是在三维模型中嵌入不可见的水印来保护模型的所有权，或用于检验模型的真实性和真实性，或嵌入可见信息来申明模型所有权。通常的水印技术包含三方面：水印生成、水印嵌入和水印提取。

3.1 水印的产生

水印实质是一系列的二进制信息，对于任意的字符串 D ，如产品序列号、公司标志等这些基本信息^[8]，要转化成嵌入到模型中的二进制水印的一般步骤是：首先利用混沌映射来产生一个随机数序列 K ，然后利用产生的随机数序列 K 和已知的那些基本信息 D 相互运算，最后得到要嵌入的水印 W 如下：

$$W = \{w_i / w_i = (2d_i - 1) * k_i, i = 1, 2, 3, \dots, l\} \quad (1)$$

其中 w_i 指的是生成的每一位水印， d_i 表示的是与基本信息字符串ANSII码相对应的二进制位。 k_i 表示的是随机数序列中的单个元素。

混沌映射有多种表达式，最常用的一种是Logistic映射： $x_{n+1} = \lambda \cdot x_n \cdot (1 - x_n)$ ，其中 $0 < \lambda \leq 4, x_n \in [0, 1]$ ， λ 称为分支参数。将Logistic映射离散化，便得到改进型Logistic映射。本文采用的是改进的Logistic映射来生成水印，用如下方程式来描述改进型Logistic映射：

$$\begin{cases} x_{i+1} = 1 - 2(x_i)^2, x_i \in (-1, 1) \\ k_i = \begin{cases} 1, & x_i > 0 \\ 0, & x_i = 0 \\ -1, & x_i < 0 \end{cases} \quad i = 1, 2, 3, \dots, l \end{cases} \quad (2)$$

在生成水印 W 前需要先算出原始消息字符串 D 中各个字符的ANSII码，根据其ANSII码将 D 中每个字符转化为相对应的二进制形式 d_i ，然后利用公式(2)生成随机数序列 K ，最后通过公式(1)将 d_i 和 k_i 相互运算得到 w_i ，从而得到要嵌入的水印 W 。

Logistic映射最关键的一步是确定初始值 x_0 ，文献[6]是将整个字符串作为一个整体来计算 x_0 ，而本文提出的算法是针对每个字符算出一个 x_0 ，然后去计算相应的 $k_i (i=1, 2, \dots, 7)$ ，并将所有的 k_i 压入到一个向量中得到整体的随机数序列 K 。这样分开计算的好处是 K 的计算不受各个字符的影响，前面字符的篡改不会影响到后面字符的正确提取，从很大程度上保证了利用相似度来验证提取字符的正确性，而文献[6]中若对前面字符篡改，后面所有的字符可能都会受到影响。

3.2 水印的嵌入

水印信息一般嵌入在模型的几何特征或拓扑结构中，CAD模型的几何特征主要是NURBS曲线或曲面，在嵌入水印前，要先找出一部分可以承载水印的目标载体。

3.2.1 目标载体的选择

目标载体一般指的是水印要嵌入其中的 NURBS 基元, CAD 模型中可以有多个嵌入水印的载体,通过对目标载体进行排序和选择可以保证嵌入、提取过程中的有序性和明确性,这比盲目地选取一些 NURBS 曲线要有针对性,而且更加节省时间,提高整个算法的效率,而不是把时间浪费在查询上。

选择载体时可以将 NURBS 曲面按照面积从大到小的顺序排列,水印嵌入在几个大面积的 NURBS 曲面中,但是选取大规模的曲面时,侵权者往往会替换关键曲线或曲面来破坏水印,为了抵抗这种替换攻击,本文采用小规模曲线来作为目标载体嵌入水印,即将 NURBS 曲线按长度从小到大排列,这就将水印隐藏在复杂的拓扑结构中,更好地抵抗非法用户的攻击^[9]。

3.2.2 相邻节点插入法

NURBS 曲线或曲面被广泛应用在 CAD 模型中,本文采用相邻节点插入法向已知的 CAD 模型中嵌入生成的水印信息,其优点在于可以精确地保持 CAD 模型的形状。

NURBS 曲线的主要属性有阶数、控制点和节点,其曲线的形状主要由控制点来决定,且满足节点个数=阶数+控制点个数-1,所以在曲线中插入一个节点会同时增加一个控制点,移除一个节点也会减少一个控制点。

相邻节点插入法完整的描述如下(本文算法假设每条 NURBS 曲线最多可以嵌入 9 个字符,即可以嵌入 $9*7=63$ 位二进制水印信息):对每条要嵌入水印的 NURBS 曲线来说,首先得到其原始的主要属性,如阶数、控制点数组和节点向量;其次根据每位水印信息 w_i 和 w_j 属于此曲线允许嵌入的 63 位二进制信息中的位数来得到新增节点的向量,从而得到新的节点向量 U' ,这样就把水印 w_i 嵌入到了曲线中,此时节点数加 1,同样控制点数要加 1,根据相应新增控制点的规则来得到新的控制点数组;最后利用新的节点向量和新的控制点数组来构建新的 NURBS 曲线,水印嵌入后,控制点数的增加并不会改变曲线的形状,只是控制点所组成的曲线形状更加逼近节点曲线,这就精确地保持了模型的形状。

3.2.3 嵌入水印

本文实验中假设要嵌入的信息串长度为 len ,每个

嵌入基元中允许嵌入的水印位数为 $num=9$,然后利用相邻节点插入法对模型嵌入水印,具体如下:

1) 遍历整个模型找到所有的 NURBS 曲线。

2) 对所有的 NURBS 曲线进行冒泡排序,则得到按长度从小到大排序的 NURBS 序列。

3) 对每个要嵌入的字符,根据其在整个字符串的位置,判断此字符应该嵌在模型中第 j 条曲线的第 d 个位置(每个字符根据其 ANSI 码的二进制形式在曲线中占 7 位)。

4) 假设 NURBS 曲线的节点向量是 U ,其中每个节点的 $u_i \in [0,1]$,则新插入节点的 u' 也应该 $\in [0,1]$,将 $\in [0,1]$ 分为 $num*7$ 份(ANSI 一般用 7 位表示),新节点向量 u' 表示如下:

$$u' = \frac{d*7+i+1}{num*7+1} + W[charnum*7+i] * \frac{1}{4*(num*7+1)} \quad (3)$$

$charnum$ 指的是要嵌入的字符串的第 $charnum$ 个字符, $d = charnum \% 9, i=0,1,2,\dots,6$ 。

5) 曲线的节点向量 U 是按从小到大顺序排列的,对每个新增 u' 根据其大小插入在 U 中合适的位置,得到新曲线的节点向量 U' ,同时计算新增控制点坐标,并将其插入控制点数组得到新的控制数组,这就把水印嵌入到了模型的 NURBS 曲线中。

6) 水印嵌入后,把模型中相应的嵌入水印的 NURBS 面特征都选中。

3.3 水印的提取

从嵌入水印的模型中提取水印的过程叫水印提取。本文采用的是盲水印算法,即提取水印时不需要给出原始的 CAD 模型,也不需要重新输入原始的水印信息,而是先根据字符位置去排好序的 NURBS 曲线序列中找到要进行水印提取的 NURBS 曲线,然后得到相应曲线的属性并利用其节点向量来进行具体的水印提取,最后将提取到的水印和原始消息进行相似度对比来验证其是否经过篡改。具体的提取与检测过程如下:

1) 嵌入过程中已经得到了排好序的曲线序列,由于是盲水印提取,所以不需要再有具体的生成随机序列 K 和对 NURBS 进行排序的过程,而在文献[6]的半盲水印中,提取时重新输入了原始的消息串,重新生成了 K 和重新去遍历模型来得到排序的基元序列,所以本文算法大大减少了整个提取过程的时间。

2) 对每个字符而言,要先根据它在原始消息字符串中的位置来找到其在目标载体的初始位置,依次来计算它对应的 u' (每个字符的 ANSII 码有 7 位,就能得到 7 个对应的 u' , 即得到对应的 7 位 w'), 并利用如下公式来计算提取的水印 w_i' :

$$w_i' = \begin{cases} -1 & u' \in U \text{ 且 } u' = \frac{d*7+i+1}{num*7+1} \frac{1}{4*(num*7+1)} \\ 1 & \text{else} \end{cases} \quad (4)$$

其中 $d = charnum \% 9$, $i=0,1,2,\dots,6$

3) 利用水印产生进程中混沌映射所生成的随机数序列 K 和上式的 w_i' 来得到提取水印相对应的二进制消息串 D' :

$$D' = \left\{ d_i' / d_i = \frac{w_i' * k_i + 1}{2}, i = 0, 1, 2, \dots, charnum * 7 - 1 \right\} \quad (5)$$

其中 $charnum$ 表示水印字符串的个数, 7 是指单个字符 ANSII 码位数。

4) 将二进制消息串 D' 依次按 7 位计算出一个 ANSII 码值, 并转化为相对应的实际水印字符串值 $Mess'$ 。

5) 假设原始消息字符串是 $Mess$, 当 $Mess$ 与 $Mess'$ 完全相等时, 可以断定待检测的 CAD 模型中包含版权信息 $Mess$; 反之不一定成立, 通过比较 $Mess'$ 与 $Mess$ 的相似度, 来判断待检测的 CAD 模型在一定的置信区间内是否含有版权信息 $Mess$ 。

4 系统实现与结果分析

4.1 系统的具体实现

本算法是借助插件以菜单方式在 SolidWorks 平台上运行的, 以下是具体的流程:

图 4 表示的是启动 SolidWorks 并加载插件后平台的状态: 有三个下拉菜单, 算法总共分三步, 即生成水印(Generate WM)、嵌入水印(Embed WM)、提取水印(Extract WM)。

图 5 是打开模型“a.SLDPRT”后点击“WaterMark”的下拉菜单“Generate WM”, 出现对话框“GenerateWatermark”, 在文本框中输入消息“Hello, world!”并采用改进的 Logistic 映射对“Hello, World!”所生成的二进制水印消息(每个字符对应 7 为二进制水印)。



图 4 加载插件后平台的状态

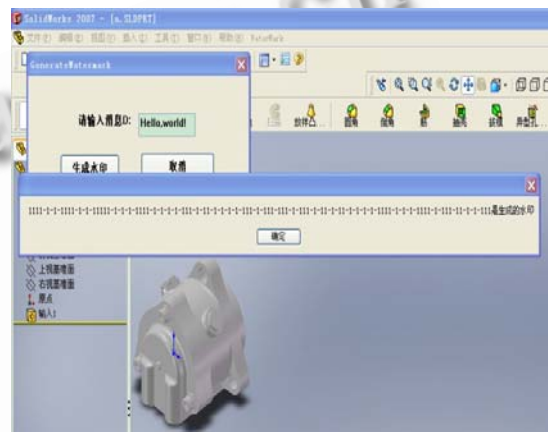


图 5 消息“Hello,world!”所生成的二进制水印信息

4.2 实验结果分析

本文采用了盲水印算法, 盲水印提取水印时不需要原始模型和原始水印消息, 所以与文献[6]中半盲水印相比在提取时速度会加快, 能提高算法的效率。具体比较结果见下表 1(时间的基本单位用的是 ms):

表 1 实验结果对比

	原始模型	原始水印消息	嵌入水印时间	提取过程时间	累计时间
本文方法	不需要	不需要	11165ms	55ms	12220ms
文献[6]	不需要	需要	16335ms	880ms	17215ms

上表是用本文算法和文献[6]算法作用在同一个模型(“a.SLDPRT”)、相同的原始水印消息“good”得到的结果: 本文算法嵌入水印所用时间是 11165ms, 而文献[6]算法嵌入水印的时间是 16335ms; 本文算法提取水印使用的时间是 55ms, 而文献[6]算法提取水印的时间则是 880ms; 本文算法嵌入和提取水印并检测所使用的总时间是 12220ms, 而文献[6]算法使用的总

时间是 17215ms。按效率来讲,本文算法在提取水印时明显效率更高,整个时间比文献[6]中的算法的时间更少,明显加快了算法的执行效率。

与文献[6]相比,本文算法的另一个优点是可以嵌入比较多的水印信息,文献[6]的算法将水印信息只嵌入在一条 NURBS 曲线上,且嵌入水印信息的长度不能超过 7,而实际应用中的水印容量会远远超过 7 个字符,鉴于此缺点,本文算法将水印信息分组嵌入到几个 NURBS 面中,假设每条曲线嵌入的水印信息不能超过 18 个字符,对上表 1 中的模型来讲,最多可以嵌入 $18 \times 13 = 234$ 个字符,而文献[6]提出的算法使用相同模型时最多只能嵌入 7 个字符,所以本文算法极大地提高了嵌入水印的信息容量。

5 结束语

本文主要采用的是改进的 Logistic 映射来生成一系列的要嵌在模型中的二进制水印串,并采用相邻节点插入法重新构造新的 NURBS 曲线来进行水印的嵌入,这样做并不会改变模型的形状,所以适宜用在 CAD 这种要求精确保持模型形状的平台,最后通过提取嵌在模型中的水印来与原始水印相比,检测此水印是否被篡改过。

在选择目标载体时,本文选取的是小规模曲线,但在实际生活中,侵权者往往会将模型次要部分舍弃,同时水印就会随着嵌入面的删除而丢失,所以水印无法抵抗删除面的攻击;另一方面,本文算法针对的只是 NURBS 曲线或曲面,对于不包含 NURBS 面的模型,就无法嵌入水印。以后的研究中,打算从以上方面着手,在删除嵌入水印面前先将水印转移到其它面中,这样就可以抵抗删除面的攻击;对于二次曲面来说,

可以考虑先将其转化为 NURBS 曲面,然后利用本文算法嵌入水印,这样并不会改变模型的形状,仍然满足保形性的要求。

参考文献

- 1 李军. 三维模型数字水印研究. 湖北民族学院学报, 2009, 1(27): 44-46.
- 2 Ohbuchi R, Masuda H, Aono M. Watermarking Three Dimensional Polygonal Models Through Geometric and Topological Modifications. IEEE Journal on Selected Areas in Communication, 1998, 16(4): 551-560.
- 3 张新宇, 彭维, 张三元, 等. 3D 网格数字水印研究进展. 计算机辅助设计与图形学学报, 2003, 15(8): 915-916.
- 4 Lee JJ, Cho NI, Lee SU. Watermarking Algorithms for 3D NURBS Graphic Data. EURASIP Journal on Applied Signal Processing, 2004, 14: 21-44.
- 5 Sun SS, Pan ZG. Blind Watermarking of Non-uniform BSpline Surfaces. International Journal of Image and Graphics, 2008, 8(3): 442.
- 6 Liu N, Zhang Y, Chen ZY. Chaos based Semi-Blind Watermarking for CAD Models. Intelligent Systems, 2009. GCIS' 09. WRI Global Congress on. 2009, 3: 411-414.
- 7 Ohbuchi R., Masuda H, Aono M. A shape preserving data embedding algorithm for NURBS curves and surfaces. Computer Graphics International Proceedings, 1999: 180-185.
- 8 van Schyndel RG, Tirkel AZ, Osborne CF. A digital watermarking. IEEE Proceedings of International Conference on Image Processing. 1994: 86-90.
- 9 高路. 基于鲁棒性数字水印的三维 CAD 模型版权保护[硕士学位论文]. 杭州: 浙江大学, 2004.