Computers & Graphics 37 (2013) 269–279

Contents lists available at SciVerse ScienceDirect

Computers & Graphics

journal homepage: www.elsevier.com/locate/cag

Technical Section

Topology authentication for CAPD models based on Laplacian coordinates

Zhiyong Su [a,*], Lang Zhou [b], Weiqing Li [c], Yuewei Dai [a], Weiqing Tang [d,e]

[a] School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China
[b] School of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210046, China
[c] School of Computer Science, Nanjing University of Science and Technology, Nanjing 210094, China
[d] Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
[e] Beijing Zhongke Fulong Computer Technology Co., Ltd., Beijing 100085, China

ARTICLE INFO

Article history:
Received 24 September 2012
Received in revised form
23 February 2013
Accepted 23 February 2013
Available online 4 March 2013

Keywords:
Semi-fragile watermarking
Watermarking
Laplacian coordinates
Topology authentication
Topological integrity
Process plant

ABSTRACT

Topology authentication for computer-aided plant design (CAPD) models features intrinsically complex topological relations. This study investigates a semi-fragile watermarking scheme for CAPD models represented by parametric solids, which offers a solution to the problem of topology authentication. We first analyze the geometrical and topological structures of CAPD models. Then, we propose an effective semi-fragile watermarking method for topology authentication, which is based on Laplacian coordinates and quantization index modulation (QIM), against several attacks. We compute the custom Laplacian coordinate vector for each marked connection point according to the topological relation among joint plant components. The topology-based watermark for each marked connection point is generated from selected attributes of its joint plant component. Watermarks are inserted into the coordinates of marked connection points by adjusting the lengths of their Laplacian coordinate vectors. Both experimental results and theoretical analysis demonstrate that our approach can not only detect and locate malicious topology attacks, such as component modification and joint ends modification, but is also robust against various non-malicious attacks, such as similarity transformations and level-of-detail (LOD).

1. Introduction

With the rapid development of 3D acquisition and geometric modeling technologies, 3D models have been used increasingly in many applications, such as scientific simulation, medical imaging, cultural heritage and computer-aided design (CAD). As 3D models are used in a wide variety of fields, the ease of duplication and modification of 3D models calls for the development of techniques for copyright protection and integrity authentication [1–5].

3D computer-aided plant design (CAPD) models, which are one type of 3D models, are widely used in the process plant industry. Process plants are complex facilities that primarily consist of various plant components, such as equipment and pipelines, which include pipes and piping components. With increasing product complexity and intensive global competition in the process plant industry, companies are increasingly relying on collaborative design techniques to shorten the design cycle and to sustain the optimum productivity. CAPD is an essential technology that helps to increase productivity, accuracy and collaboration, to meet the challenges of complex plant design projects. Collaborative design is the process by which multidisciplinary designers and engineers participate in design decision-making and share product information. Thus, CAPD models can be easily modified when they are shared with collaborators and customers. And this will have a great influence on various construction documents which generated automatically from CAPD models according to their topological and geometrical information. Therefore, integrity authentication and verification are critical to companies when sharing CAPD models with their collaborators and customers.

One of the most important items to authenticate a CAPD model is its intrinsically complex topological information. Generally, the CAPD model can be completely represented by three types of information: geometrical information, engineering information and topological information [6]. Geometrical information describes the shape and 3D positions of all of the plant components. Engineering information refers to design constraints, engineering disciplines, etc. Topological information provides complex topological relations among different plant components [7]. Unlike the traditional mechanical CAD industry, which mainly concentrates on geometric modeling, CAPD systems mainly focus on optimizing the plant layout [8]. The goal of plant layout design is to find the most economical spatial arrangement of process vessels,

* Corresponding author. Tel.: +86 25 84315467; fax: +86 25 84317332.
E-mail addresses: suzhiyong@gmail.com, suzhiyong@njust.edu.cn (Z. Su).

0097-8493/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cag.2013.02.009

equipment and the interconnecting pipes that satisfies the construction, operation, maintenance and safety requirements [9,10].

Topological information can easily be edited through various operations that are provided by CAPD systems during collaboration. We classify these operations into two groups: non-malicious operations and malicious operations. Non-malicious operations always include similarity transformations (e.g., translation, rotation and uniform scaling) and simplification. Malicious operations often involve attacks against plant components and joint ends. Component attacks include adding, deleting and replacing plant components. Joint-end attacks refer to the logical modification of the topological relation between two joint ends. Therefore, establishing a trustworthy mechanism to authenticate the topological information is vital to CAPD models. The problem of topology authentication for CAPD models comprises two aspects, joint plant components authentication and joint ends authentication. The goal of joint plant components authentication is to ensure that the joint plant components of each plant component are the same. Joint ends authentication further verifies that the exact joint ends between the two joint plant components have not been modified.

Digital watermarking techniques provide a simple and reasonable solution for the authentication of 3D models [11,12]. However, in the literature, existing watermarking schemes for 3D models, including CAD models, mainly target geometrical information protection or authentication. Topology authentication for CAPD models is still in its infancy and offers interesting potential for improvement because of the models' intrinsically complex topology. In this study, we propose a semi-fragile watermarking scheme to address the issue of authenticating the integrity of the topological information of CAPD models. We select a subset of the model's connection points to be watermark carriers, also called marked points. The topological information among different plant components is exploited to generate watermark strings. The topology-based watermarks are embedded into the coordinates of marked points by adjusting the lengths of their Laplacian coordinate vectors.

The remainder of this paper is organized as follows. We review some related works in Section 2. Section 3 provides a brief introduction to CAPD models. Section 4 describes the proposed scheme. Experimental results that demonstrate the performance of our watermarking scheme are presented in Section 5. Conclusions and future work follow in Section 6.

2. Related works

In this study, we tackle the problem of topology authentication through digital watermarking techniques. In the literature, few related works have referenced this problem. There are, however, some related works on watermarking 3D CAD models for geometrical information protection or authentication.

Digital watermarking techniques for 3D models have been widely studied since Ohbuchi first proposed a watermarking scheme for 3D models [3,12–15]. However, relatively few watermarking algorithms have been proposed for 3D CAD models; even fewer have been proposed for CAPD models. Watermarking schemes for 3D CAD models mainly target CAD drawings, NURBS curves, subdivision surfaces, constructive solid geometry (CSG) models, etc.

A robust digital watermarking scheme for 3D CAD drawings was proposed by Park et al. [16]. The scheme uses LINEs and 3D FACEs to prevent copyright infringement from unlawful reproduction and distribution. Kwon et al. presented two watermarking schemes for 3D CAD drawings [17,18]. Their schemes arbitrarily select the LINE, FACE and ARC components and embed the watermark into the difference in the length between the reference line and the connected lines in the case of line components, the circular radius in the case of the arc components and the length ratio of two sides in the case of face components. Lee et al. proposed a robust watermarking scheme based on geometric features with k-means++ clustering for 3D CAD drawings [19]. The watermark is embedded into the geometric distribution of POLYLINE, 3DFACE and ARC objects in the main layers. A watermarking scheme for 3D NURBS curves using re-parameterization was proposed by Ohbuchi et al. [20]. Their method is invariant to affine transformations, but it is sensitive to Möbius re-parameterization. Lee et al. also presented a method for watermarking NURBS data using 2D virtual images [21]. Fornaro and Sanna proposed a fragile watermarking scheme for authenticating CSG models [22]. The watermark is generated from selected attributes of the model and is stored in one or more places in the model itself. A watermarking algorithm for T-spline curves and surfaces using knot insertion was proposed by Weng et al. [23]. Cheung et al. presented a robust non-blind watermarking scheme for subdivision surfaces using modulating spectral coefficients of the subdivision control mesh [24].

3. CAPD models

This section provides a brief introduction to the geometrical and topological modeling of CAPD models.

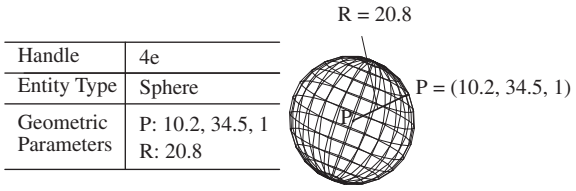
3.1. Geometrical modeling

Plant components are created using the CSG representation by combining basic solid entities that have simple shapes, such as spheres, cylinders, cones, etc. Compared with the complex topological relations among plant components, their individual geometrical shapes are not as important.

The geometrical information of plant components is defined through geometrical parameters. These parameters are then employed to support the automatic generation of construction documents, such as isometrics, orthographies, etc. Currently, the top software applications in the field of plant design, such as AutoCAD Plant 3D, AutoPLANT and SmartPlant3D, are characterized by this vital and popular function. In general, the main sections of a solid entity consist of its handle value, entity type and geometric parameters. An example of a sphere entity is shown in Fig. 1.

3.2. Topological modeling

The topological representation of the interconnections among plant components plays a significant role in the plant design. The layout poses significant limitations on the type, size and location of plant components. Not only should the layout represent the interconnection between two plant components, but also it should describe their ends. Only the two ends of different plant components that satisfy the specific requirements, such as the pipe diameter, end type, pressure rating and flow direction, can be connected.



Handle	4e
Entity Type	Sphere
Geometric Parameters	P: 10.2, 34.5, 1 R: 20.8

Fig. 1. An example of a sphere entity.

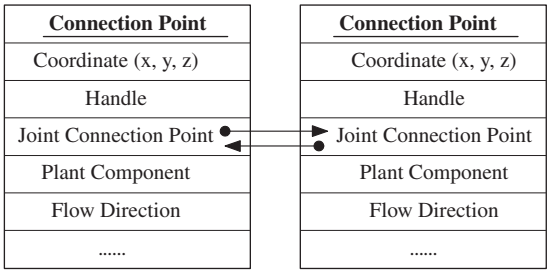


Fig. 2. The structure of connection points.

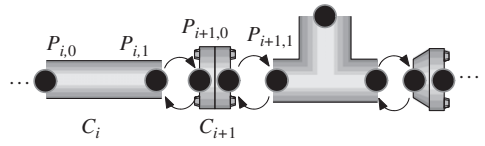


Fig. 3. Examples of connection points of a simple pipeline.

There are two formats for representing the end connection: connection points [25] and the order of plant components stored in the CAPD file. We use the CAPD model that describes the end connection by connection points because this format is one of the most widely used and most effective representations for topological modeling.

Each connection point has the same attributes, which include geometrical information, topological constraint, handle value and various engineering properties. Geometrical information includes the position of the point, which also exists as an entity. In general, the connection point is defined on its corresponding plant component. For example, a pipe, which is represented by a cylinder, has two connection points, which are also the center points of its two end faces. A topological constraint is used to describe a singular joint connection point, if one exists. The handle value is an abstract reference to an entity. In the CAPD file, this value (i.e., an identification number) is unique and is not changed, even if the entity is modified [26]. Connection points are added, deleted and transformed, along with their corresponding plant components, by various operations that are provided by CAPD systems. The maintenance of connection points is performed automatically by CAPD systems without the need for human intervention. Fig. 2 shows the structure of a connection point. Fig. 3 shows the connection points of a simple pipeline. The interconnection between two joint plant components, C_i and C_{i+1}, is represented through their connection points, $P_{i,1}$ and $P_{i+1,0}$.

4. The watermarking scheme for topology authentication

This section describes our topology authentication method, which is inspired by traditional Laplacian operators.

4.1. Overview of the method

The proposed watermarking scheme consists of two separate procedures, the *embedding procedure* and the *extraction procedure*, which are shown in Fig. 4. An overview of the proposed watermarking scheme is described as follows.

In the watermark embedding stage, we first compute a component-radius mapping table (CRMT), which should be maintained and registered for the watermark extraction and verification. We traverse the plant components of each pipeline according to its flow direction and select marked plant components. Then, for each selected marked plant component, we generate a singular topology-based watermark string for each of its connection points. After that, we calculate the Laplacian coordinate vector for each marked connection point. Finally, the topology-based watermark is embedded into each marked connection point by modifying the length of its Laplacian coordinate vector.

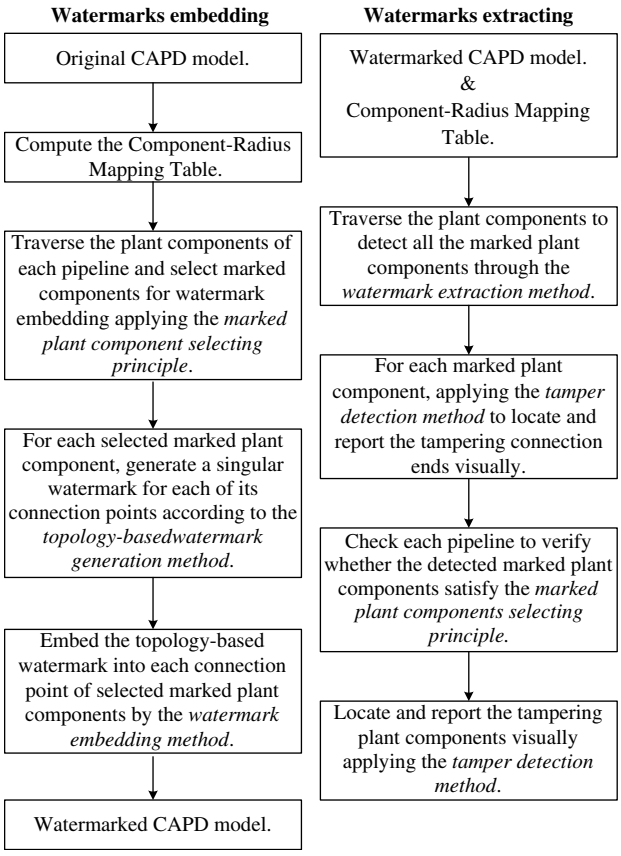


Fig. 4. Overview of the proposed semi-fragile watermarking scheme.

In the watermark extraction stage, the scheme detects and labels all of the marked plant components of the watermarked model with its registered CRMT. For each marked plant component, we first extract the embedded watermark for each of its connection points. Second, we calculate the topology-based watermark for each of its connection points. Third, we verify the topology integrity of each joint end of the marked plant components by comparing the extracted watermark with the calculated topology-based watermark. Last, we report the tampered joint ends of the marked plant component visually. For each pipeline, we verify that the detected marked plant components satisfy the *marked component selecting principle*. For those components that do not satisfy the *marked component selecting principle*, we locate and report them visually as suspicious tampered components.

4.2. Watermark targets

We authenticate and verify the topological information by embedding specific watermark bits into the CAPD model. In theory, there are two types of eligible candidates for the watermark embedding: geometrical parameters of the plant components and coordinates of the connection points. As described in Section 3.1, the geometrical parameters of the plant components are used to automatically generate various construction documents, which means that the modification of geometrical parameters will inevitably lead to incorrect construction documents.

To avoid this problem, and for the following reasons, the connection points are the logical candidates for data embedding. First, the topological relation among different plant components is described by their connection points. Second, connection points are, by definition, the least likely to be removed among the types of data objects that exist in CAPD models. Moreover, the deletion of connection points will inevitably result in topology modification and will further impact the automatic generation of construction documents. Third, the slight altering of the coordinates of connection points will have no influence on the generation of construction documents.

4.3. Component-radius mapping table computation

To achieve robustness against uniform scaling, we construct a component-radius mapping table (CRMT) for the target model before embedding the watermark. This table is also used as a private key for both the embedding and extraction of the watermark to enhance the security of the scheme. The table should be kept in reserve and should be registered for both watermark embedding and extraction.

The CRMT consists of two parts: (1) the handle value of each plant component in the original model and (2) the radius of the bounding sphere of each plant component and its joint plant components. Both the geometrical and topological information are used to construct the CRMT as follows.

For each component C_m, we first obtain its handle value, $cHandle_m$. Then, we find its 1-ring neighboring components, $N(C_m)$. After that, we compute the radius of the bounding sphere of C_m and $N(C_m)$, R_m. Finally, the unique handle value, $cHandle_m$, and the radius, R_m, are used to construct the CRMT. For the handle values of those plant components that are not in the original model, we label them as 'Undefined handle values'. A default value, such as 0, is employed to represent the corresponding radius R_m and to indicate that these plant components are newly added. Fig. 5 gives an example of the CRMT of a CAPD model with n plant components. From this table, we can retrieve the radius for each component according to its handle value. The computed radius, R_m, is then utilized to calculate the adaptive quantization step for both watermark embedding and extraction. For those handle values that are not included in the table, a default value will be returned. This situation will occur during the watermark extraction stage when new plant components are added into the original model.

4.4. Marked plant components selecting principle

The principle of marked plant components selection will be described in this section. Initially, we set all of the plant components as *non-marked* components and traverse each pipeline of the model to find eligible plant components for watermark embedding, according to the flow direction, following the procedure described below:

- One of the two joint plant components should be selected as a marked plant component.
- The plant component chosen as a marked plant component must have no marked components among its 1-ring neighboring components. Once a plant component has been chosen as a marked component, its 1-ring neighboring components are no longer eligible.

This principle is quite simple, and Fig. 6 shows two different selection results for the same abstracted CAPD model. The union of the marked plant components and their 1-ring neighborhood cover all of the plant components in the model. All of the connection points of the selected marked plant components are set as marked connection points and are then used for watermark embedding. Thus, it can be guaranteed that the marked plant components and their marked connection points are uniformly distributed in the model. Experimental data in Table 1 show that our principle selects approximately 50% of plant components and connection points as marked components and marked connection points. This selection process results in a high locating accuracy, which will be discussed in Section 5.2.

Handle Value	Radius
$cHandle_1$	R_1
$cHandle_2$	R_2
...	...
$cHandle_n$	R_n
Undefined handle values	Default Value

Fig. 5. An example of a component-radius mapping table.

4.5. Topology-based watermark generation

We generate a topology-based watermark for each marked connection point taking some singular properties of its joint connection point and joint plant component into consideration using a deterministic chaotic map.

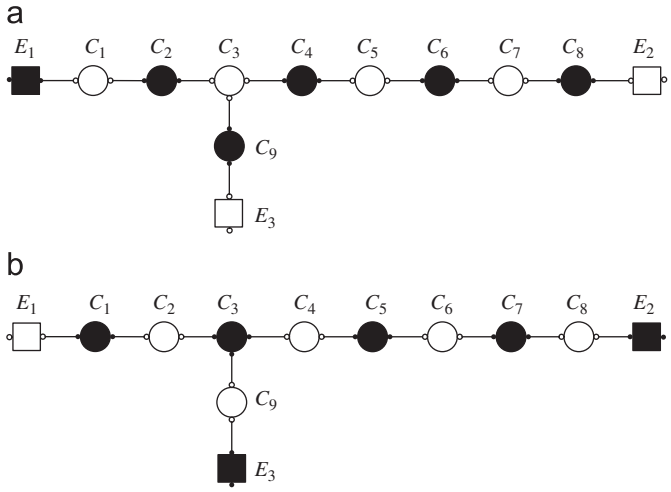


Fig. 6. Two different selection results of marked plant components for the same simple abstracted CAPD model. Circular nodes represent pipe components, whereas rectangular nodes represent equipment. Black nodes are selected marked plant components, whereas white nodes are non-marked plant components.

Table 1
Lists of three CAPD models used in our experiments and their detailed information, including plant components (PCs), connection points (CPs), marked plant components (MPCs), marked connection points (MCPs) and model precision.

Model	PCs	CPs	MPCs	MCPs	Model precision
Carton board	6810	13,964	3365	7002	10^{-3}
Hydrogenation	15,570	32,624	8145	16,556	10^{-3}
Styrene	18,912	38,198	9652	19,484	10^{-3}

Let C_m be a selected marked plant component with n connection points. Plant component C_{m+1} is one of the joint plant components of C_m. $P_{m,i}$ is a marked connection point of C_m ($i \in [0,n-1]$). $P_{m+1,j}$ is a connection point of C_{m+1}. Assume that the joint connection point of $P_{m,i}$ is $P_{m+1,j}$. We denote the handle value of $P_{m+1,j}$ as $pHandle_{m+1,j}$. The handle value is involved in the construction of the watermark because each object in CAPD models has a unique handle value and it is not changed even if the object is modified [26]. Let the total number of joint plant components of C_{m+1} be d_{m+1}. These components are also involved in the watermark generation. The chaotic map used in this study for the watermark generation is a well-known logistic function as follows:

$$f(x_n) = x_{n+1} = ax_n(1-x_n), \tag{1}$$

where a is a positive number that acts as a function seed and x_n is a number between 0 and 1, which represents the current value of the mapping in time with an initial value x_0 [27]. When $a > 3.5699456$, the sequence iterated with an initial value is chaotic. Different sequences will be generated with different initial values because the logistic function is extremely sensitive to the initial conditions. The complicated but deterministic properties of the map make it ideally suited for watermark generation [28–30].

To generate the watermark $w_{m,i}$ for $P_{m,i}$, we first convert the handle value $pHandle_{m+1,j}$ into a positive float number $h_{m,i}(0 < h_{m,i} < 1)$ as follows:

$$h_{m,i} = hash(pHandle_{m+1,j}), \tag{2}$$

where $hash()$ is a hash function. Then, the logistic function, shown in Eq. (1), is seeded with an initial starting value of $x_0 = h_{m,i}$, and iterated, and a final float value $f_{m,i}$ is calculated. After that, we generate the watermark $w_{m,i}(0 < w_{m,i} < 1)$ as follows:

$$w_{m,i} = d_{m+1} \times f_{m,i}. \tag{3}$$

There may be some marked connection points that have no joint connection points. In general, the selected marked plant components at the beginning or end position of a pipeline may have one or more marked connection points with no joint connection points. The marked plant component E_1 in Fig. 6(a), for example, has two marked connection points, but only one of them has a joint connection point. We assume that $P_{m,i}$ has no joint connection point. The handle of $P_{m,i}$ is $pHandle_{m,i}$. Let the total number of joint plant components of C_m be d_m. To generate a watermark $w_{m,i}$ for $P_{m,i}$, the positive number $h_{m,i}(0 < h_{m,i} < 1)$ for $P_{m,i}$ is calculated as follows:

$$h_{m,i} = hash(pHandle_{m,i}). \tag{4}$$

And the watermark $w_{m,i}(0 < w_{m,i} < 1)$ is generated as follows:

$$w_{m,i} = d_m \times f_{m,i}. \tag{5}$$

4.6. The watermark embedding

To embed the watermark, we first calculate the Laplacian coordinate vector, δ, for each marked connection point. Then, we compute a new length $\hat{l}$ by modifying the Laplacian length l for carrying the watermark. Finally, the new Laplacian vector, $\hat{\delta}$, with length $\hat{l}$ is realized through a minimization process, and eventually the corresponding Cartesian coordinate is computed.

4.6.1. The computation of Laplacian coordinates

For each marked connection point $P_{m,i}$ of C_m, we first define its neighboring connection points using the following definition: the neighboring connection points $N(P_{m,i})$ are the set of all of the connection points of the joint plant components of $P_{m,i}$. $P_{m,i}$ is conventionally represented using absolute Cartesian coordinates, denoted by $P_{m,i} = (x_{m,i}, y_{m,i}, z_{m,i})$. Fig. 7 shows an example of the neighboring connection points of a marked connection point. The marked component C_1 is a flange, whereas its joint component C_2 is a valve. $P_{1,1}$ is a marked connection point of C_1. The neighboring connection points $N(P_{1,1}) = \{P_{2,0}, P_{2,1}, P_{2,2}\}$, where $P_{2,0}$, $P_{2,1}$ and $P_{2,2}$ are the connection points of C_2.

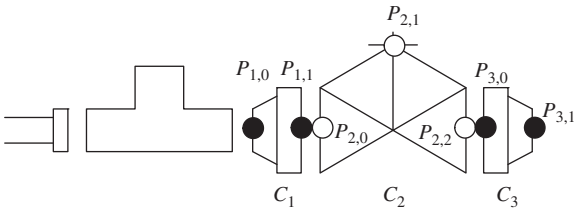


Fig. 7. Illustration of the neighboring connection points of a marked connection point. C_1 is a flange, and it is a marked plant component, whereas its joint component C_2 is a valve. The black point $P_{1,1}$ is a marked connection point of C_1, and its neighboring connection points are the white connection points $P_{2,0}$, $P_{2,1}$ and $P_{2,2}$ of C_2.

Then, we define the *differential* or *δ-coordinates* of $P_{m,i}$ to be the difference between the absolute coordinates of $P_{m,i}$ and the center of mass of $N(P_{m,i})$ as follows:

$$\delta_{m,i} = (x'_{m,i}, y'_{m,i}, z'_{m,i}) = P_{m,i} - \frac{1}{d_{m,i}} \sum_{P_{m,j} \in N(P_{m,i})} P_{m,j} \tag{6}$$

where $d_{m,i} = |N(P_{m,i})|$ is the number of neighboring connection points of $P_{m,i}$. $\delta_{m,i}$ is also called the Laplacian coordinate of $P_{m,i}$. The length of the Laplacian coordinate vector is then selected as the watermark carrier for the topology authentication as follows:

$$l_{m,i} = \|\delta_{m,i}\| = \sqrt{(x'_{m,i})^2 + (y'_{m,i})^2 + (z'_{m,i})^2}. \tag{7}$$

As mentioned in Section 4.5, there may be some marked connection points with no joint plant components. For these marked connection points, we define the connection points of the plant component that they are subject to as their neighboring connection points. For example, $P_{3,1}$ is a marked connection point of C_3 that has no joint plant components, as in Fig. 7. Its neighboring connection points $N(P_{3,1}) = \{P_{3,0}, P_{3,1}\}$, where $P_{3,0}$ and $P_{3,1}$ are all subject to C_3.

4.6.2. Quantization-based modulation

After calculating the Laplacian length, the QIM-based watermark embedding method is applied, as described in this section.

We notice that the lengths of the Laplacian coordinates, unlike the Laplacian coordinates themselves, are invariant under both translation and rotation but are sensitive to uniform scaling. To achieve robustness against uniform scaling, an adaptive quantization step computing method for watermark embedding and extraction is proposed. The adaptive quantization step, $\Delta_{m,i}$, is denoted as follows:

$$\Delta_{m,i} = \frac{R_m}{S_m} \times f. \tag{8}$$

In Eq. (8), the variable R_m is the radius of the bounding sphere of C_m and its 1-ring neighboring components. The value of S_m is retrieved from the registered CRMT using the handle value of C_m. The factor f is predefined as a key for adjusting the quantization step. Its value depends on the model precision.

It is obvious that the quantization step $\Delta_{m,i}$ has a ratio to the radius of the bounding sphere of the marked component and its 1-ring neighboring components. In other words, a model with a larger or smaller size will have a larger or smaller quantization step. Thus, we can achieve uniform scaling invariance.

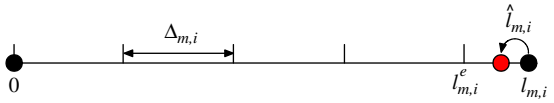


Fig. 8. With the quantization step $\Delta_{m,i}$, a watermark $w_{m,i}$ can be embedded by modifying the length $l_{m,i}$ to $\hat{l}_{m,i}$.

Fig. 8 illustrates how the watermark $w_{m,i}$ is embedded in the length $l_{m,i}$. We first initialize the integer quotient $q_{m,i}$ by $q_{m,i}=\lfloor l_{m,i}/\Delta_{m,i}\rfloor$ with the quantization step size $\Delta_{m,i}$, where $\lfloor\cdot\rfloor$ represents the floor function. The remainder $r_{m,i}$ is defined by $r_{m,i}=l_{m,i}-q_{m,i}\times\Delta_{m,i}$. In general, $l_{m,i}$ cannot be completely divided by $\Delta_{m,i}$. In that case, the remainder $r_{m,i}$ is discarded by adjusting the length $l_{m,i}$ such that $l^e_{m,i}$ can be divided by $\Delta_{m,i}$ as follows:

$$l^e_{m,i}=l_{m,i}-r_{m,i}. \tag{9}$$

Then, we embed $w_{m,i}$ into $l_{m,i}$ as follows:

$$\hat{l}_{m,i}=l^e_{m,i}+w_{m,i}\times\Delta_{m,i} \tag{10}$$

where $\hat{l}_{m,i}$ is the length after embedding, $0<w_{m,i}<1$.

4.6.3. Distortion minimization

The calculation of the new Laplacian coordinate, $\hat{\delta}_{m,i}$, after the computation of the embedded length, $\hat{l}_{m,i}$, is discussed in this section. We solve this undetermined problem by minimizing the distance between the Laplacian coordinates before and after watermarking [31]. We minimize the distance for each connection point as follows:

$$(x'_{m,i}-\hat{x}'_{m,i})^2+(y'_{m,i}-\hat{y}'_{m,i})^2+(z'_{m,i}-\hat{z}'_{m,i})^2=\|\delta_{m,i}-\hat{\delta}_{m,i}\|^2 \tag{11}$$

subject to the following:

$$(\hat{x}'_{m,i})^2+(\hat{y}'_{m,i})^2+(\hat{z}'_{m,i})^2=(\hat{l}_{m,i})^2 \tag{12}$$

This minimization problem is equivalent to finding a point $(\hat{x}'_{m,i},\hat{y}'_{m,i},\hat{z}'_{m,i})$ that is closest to the given point $(x'_{m,i},y'_{m,i},z'_{m,i})$ on a sphere of radius $\hat{l}_{m,i}$, which is centered at the origin. We can assume that the point $(\hat{x}'_{m,i},\hat{y}'_{m,i},\hat{z}'_{m,i})$ is the projection of $(x'_{m,i},y'_{m,i},z'_{m,i})$ on the sphere. As the sphere is centered at the origin, the projection of $(x'_{m,i},y'_{m,i},z'_{m,i})$ on it is given as follows:

$$\begin{cases}\hat{x}'_{m,i}=\dfrac{x'_{m,i}\hat{l}_{m,i}}{\sqrt{(x'_{m,i})^2+(y'_{m,i})^2+(z'_{m,i})^2}}\\ \hat{y}'_{m,i}=\dfrac{y'_{m,i}\hat{l}_{m,i}}{\sqrt{(x'_{m,i})^2+(y'_{m,i})^2+(z'_{m,i})^2}}\\ \hat{z}'_{m,i}=\dfrac{z'_{m,i}\hat{l}_{m,i}}{\sqrt{(x'_{m,i})^2+(y'_{m,i})^2+(z'_{m,i})^2}}\end{cases} \tag{13}$$

Finally, we compute the Cartesian coordinates of the watermarked connection point from its Laplacian coordinates, $(\hat{x}'_{m,i},\hat{y}'_{m,i},\hat{z}'_{m,i})$, according to Eq. (6).

In our scheme, the distortion induced by watermark embedding depends on the quantization step, $\Delta_{m,i}$. From Eq. (8), we can see that the larger the key value, f, the larger the induced distortion. Therefore, the maximum distortion from each marked connection point can be controlled by setting the key value, f, according to the precision requirement.

4.7. The watermark extraction and tamper detection

In the watermark extraction stage, we initially set all of the plant components and connection points as marked plant components and marked connection points. The registered CRMT and the key, f, are employed to calculate the quantization step with Eq. (8). We first check to determine all of the marked plant components of the model. Then, we apply the *marked plant components selecting principle* to detect and locate the tampered regions.

For each plant component C_m with n connection points, we check each of its connection points $P_{m,i}$ to see whether it is a marked connection point.

The corresponding radius, S_m, is first retrieved from the registered CRMT according to the handle value of C_m for the computation of the quantization step, $\Delta_{m,i}$. We compute the length, $l_{m,i}$, of the Laplacian coordinate vector of $P_{m,i}$ with Eqs. (6) and (7). Then, we extract the embedded watermark with the quantization step, $\Delta_{m,i}$, as follows:

$$w'_{m,i}=\frac{\left(l_{m,i}-\left\lfloor\frac{l_{m,i}}{\Delta_{m,i}}\right\rfloor\times\Delta_{m,i}\right)}{\Delta_{m,i}} \tag{14}$$

To see whether $P_{m,i}$ is a marked connection point, the topology-based watermark $w_{m,i}$ for $P_{m,i}$ is generated according to the *topology-based watermark generation method*, described in Section 4.5. Thus, $w_{m,i}$ and $w'_{m,i}$ should satisfy $w_{m,i}==w'_{m,i}$ if $P_{m,i}$ is a marked connection point. We label C_m as a marked plant component if it has at least one marked connection point. Otherwise, C_m is set as a non-marked plant component.

After the labeling of marked connection points and marked plant components, we detect and locate the tampered plant components and connection points by applying the *marked plant components selecting principle*. For each marked plant component, we set it as an unmodified plant component only if all of its connection points are marked connection points. Otherwise, we label its non-marked connection points and their joint plant components as suspicious regions. For each pipeline, we traverse its plant components according to its flow direction and check that the labeled marked plant components satisfy the *marked plant components selecting principle*. We set those plant components that do not meet the *marked plant components selecting principle* as tampered plant components.

5. Experimental results and discussion

Because no relevant work that targets the topology authentication of CAPD models has been published in the literature, it is difficult to directly perform comparisons with existing approaches. To validate the feasibility of our topology authentication algorithm, we first give some experimental results and then discuss the performance later in the section.

5.1. Experimental results

We evaluated the proposed semi-fragile watermarking scheme on a set of CAPD models with various unauthorized attacks. Three of these models are shown in Fig. 9. Table 1 provides detailed information about the three models. The following parameter settings are used in our experiments. The logistic function used for the watermark generation is seeded with the value $a=4$ for 5000 iterations. The key value, f, is set to 10^{-3}, according to the model precision, which is also provided in Table 1. The registered CRMT of each tested model is also required.

The results in Table 1 show that our approach selects approximately 50% of the plant components as marked plant components. Furthermore, the watermark bits are embedded into nearly 50% of the connection points.

5.1.1. Tamper detection and localization evaluation

Fig. 10(a) and (c) shows a close view of part of the original hydrogenation plant model rendered in solid and wireframe modes, respectively. The hydrogenation plant model has 15,570 plant components, and 52.3% of these components are selected as marked components. Fig. 10(b) and (d) is the same view of part of the watermarked model rendered in solid and wireframe modes, respectively, which are visually identical to the original model.

Fig. 11 shows that our scheme accurately detects and locates several types of attacks simultaneously in the hydrogenation plant model. Fig. 11(a), (c) and (e) shows a close view of the regions of the watermarked model before being attacked illegally by joint components modification and joint ends modification. The regions labeled 'A', 'B' and 'C' denote the regions of joint components addition, joint components deletion and changes in the topology relations between two joint ends logically. Our scheme locates these changed regions by setting all of the detected suspicious plant components as suspicious regions. Fig. 11(b), (d) and (f) shows the located suspicious plant components in red. Fig. 11(b), (d) and (f) shows (by the regions in red) exactly where the tampering operations occur. The experimental results verify the accuracy of our locating procedure.

5.1.2. Robustness evaluation

We evaluated the robustness of the method against various operations provided by CAPD systems that are non-malicious attacks on the design model. The non-malicious attacks include rotating, uniform scaling, transformation and LOD. Robustness is evaluated in terms of the *BER* (bit error rate) of the extracted watermark bit sequence, as well as the correlation coefficient *Corr* between the extracted binary sequence, w_i^e, and the originally embedded sequence, w_i^o, as given by the following equation [5]:

$$Corr = \frac{\sum_{i=0}^{n-1}(w_i^e - \overline{w^s})(w_i^o - \overline{w^o})}{\sqrt{\sum_{i=0}^{n-1}(w_i^e - \overline{w^s})^2} \times \sqrt{\sum_{i=0}^{n-1}(w_i^o - \overline{w^o})^2}}, \tag{15}$$

where $\overline{w^e}$ and $\overline{w^o}$ are the averages of the watermark bit sequences w_i^e and w_i^o, respectively.

For each plant component, we set the plant component to untampered if the values of *BER* and *Corr* are 0 and 1, respectively. Otherwise, the plant component is tampered. Let n_c be the total number of plant components in a model and let n_m be the number of plant components that are detected as tampered. Table 2 presents the n_m/n_c of the three models after various non-malicious attacks. The results show that our scheme is robust against the non-malicious operations.

5.1.3. Imperceptibility evaluation

We perform both a subjective assessment and an objective assessment of the imperceptibility of our scheme in this section.

To evaluate the imperceptibility, we compare the original hydrogenation plant model with the watermarked hydrogenation plant model rendered in solid and wireframe mode. Fig. 10 shows a close view of a section of the original hydrogenation plant model

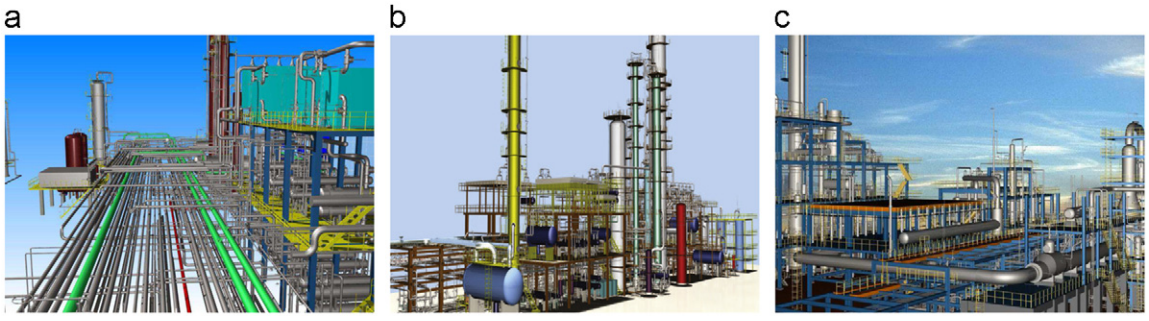


Fig. 9. Three CAPD models used for experiments. (a) Carton board plant; (b) hydrogenation plant; and (c) styrene plant.

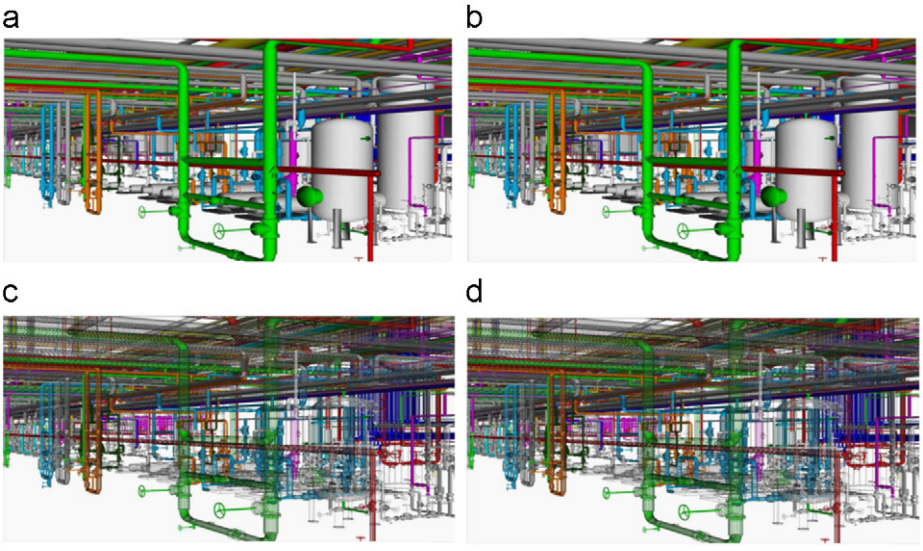


Fig. 10. An example of semi-fragile watermarking. (a) and (c) A close view of part of the original model rendered in solid and wireframe modes. (b) and (d) A close view of part of the watermarked model rendered in solid and wireframe modes.

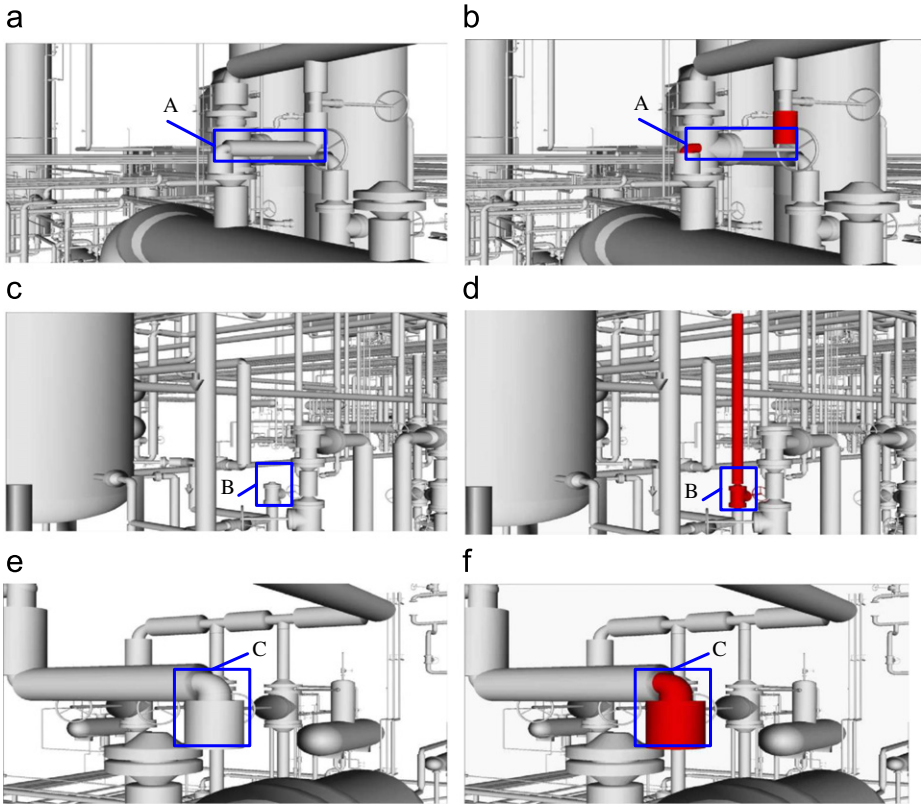


Fig. 11. The proposed scheme works on a hydrogenation plant model. (a), (c), (e) The regions before being attacked. Label A denotes regions of joint components deletion. Label B denotes regions of joint components addition. Label C denotes the region of changing the topology relation between two joint ends logically. (b), (d), (f) Our scheme accurately locates these attacks visually. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 2
n_m/n_c of the three CAPD models after various non-malicious attacks.

Attacks	Carton board	Hydrogenation	Styrene
RST	0	0	0
LOD			
80% Triangles	0	0	0
60% Triangles	0	0	0
40% Triangles	0	0	0

Table 3
PSNR values of connection points between the original and watermarked models.

Model	PSNR (dB)
Carton board	68.56
Hydrogenation	81.03
Styrene	79.64

and the same section of the watermarked hydrogenation plant model. The watermarked connection points are imperceptible.

The objective distortion of plant components is not taken into consideration because our scheme prefers the connection points, which are integral parts of CAPD models, instead of the geometric parameters of plant components themselves as watermark carriers. In other words, our scheme has no influence on the geometrical shape of the CAPD models. Although the connection points, compared with the large scale plant components, are not observed by viewers because of their small size and small contribution to the final scene, we still measure their objective distortion that is induced by watermarking in terms of the peak signal-to-noise ratio (PSNR) method [19] as follows:

$$PSNR = 10 \lg \frac{MAX^2}{MSE}, \tag{16}$$

where

$$MAX = \max \|P_i - o\|, \quad i \in [0, n-1],$$

$$MSE = \frac{1}{n} \sum_{i=0}^{n-1} \|P_i - P_i'\|,$$

P_i and P_i' are the corresponding connection points in the original model and the watermarked model, respectively, o is the geometric center of the model, n is the number of connection points, and $\|P_i - P_i'\|$ is the Euclidean distance between the two connection points. Table 3 lists the PSNR values of the connection points.

The impact of watermark embedding on connection points can be tuned by the quantization step size. According to our *watermark embedding method* described in Section 4.6, our scheme just slightly adjusts the positions of marked connection points. The topology relation is not modified either. As a consequence, our scheme will have no influence on the design and automatic generation of various construction documents. Thus, our scheme is functionally imperceptible.

5.2. Discussion on tamper detection and localization

We analyze the performance of our scheme with respect to detecting and locating tampered regions in the model from the following two aspects: attacks against plant components and attacks against joint ends, both of which are common operations that are provided by CAPD systems in a practical design process.

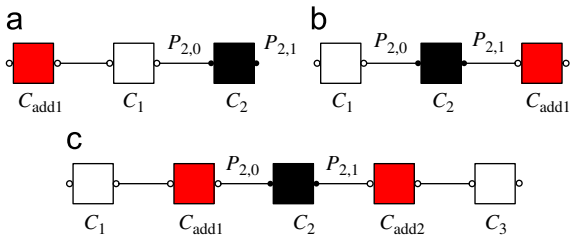


Fig. 12. Illustration of detecting and localizing components addition. Black nodes are marked plant components. White nodes are non-marked plant components. Red nodes represent the added plant components. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

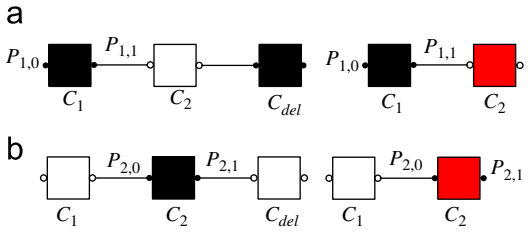


Fig. 13. Illustration of detecting and localizing component deletion. Black nodes are marked plant components. White nodes are non-marked plant components. The suspicious plant components are represented by red nodes. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

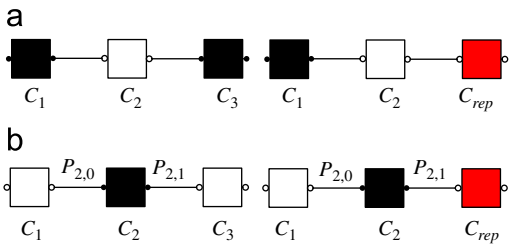


Fig. 14. Illustration of detecting and localizing component replacement. Black nodes are marked plant components. White nodes are non-marked plant components. Red nodes represent the plant components after replacement. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Component attacks mainly cover adding, deleting and replacing plant components. Joint ends attacks refer to the logical disconnection of two joint ends.

5.2.1. Components modification

- *Component addition*. Without loss of generality, there are three situations that cover the possible addition of plant components into the model. These situations are shown in Fig. 12.
  Fig. 12(a) shows that a new component C_{add1} is added, and it is connected with a non-marked component C_1. This type of attack modifies the topological relation of C_1, changing the total number of joint plant components of C_1 from one to two. As a result, the watermark for $P_{2,0}$, which is generated according to the *topology-based watermark generation method*, is different from the extracted watermark. Thus, the topological modification of C_1, as well as that for $P_{2,0}$, is detected.
  Fig. 12(b) illustrates the addition of a new component, C_{add1}, which is connected with a marked component C_2. This type of attack changes the radius of the bounding sphere of C_2 and its joint plant components. C_{add1} now becomes the joint plant component of $P_{2,1}$, which had no joint plant component previously. Either of the above two modifications can lead to a different watermark for $P_{2,1}$, generated according to the *topology-based watermark generation method* from the extracted watermark. Therefore, the topological modification of C_2, as well as $P_{2,1}$, is detected.
  Fig. 12(c) shows that C_{add1} is inserted between C_1 and C_2, and C_{add2} is inserted between C_3 and C_2. C_1 and C_3 are non-marked components, whereas C_2 is a marked component. These attacks modify the topological relation of C_1, C_2 and C_3. In addition, the radius of the bounding sphere of C_2 and its joint plant components may be changed. During the watermark extraction stage, all of the connection points are labeled as non-marked connection points according to the *watermark extraction and tamper detection method* because of the above modifications. Then, all of the components are set as non-marked components. As a result, we label all the components as tampered components because they do not satisfy the *marked plant components selecting principle*. Subsequently, the topological modification of C_1, C_2 and C_3 are detected and located accurately.
- *Components deletion*. These attacks modify the topological relation of the model. There are two situations when deleting plant components from the model shown in Fig. 13, which are marked component deletion and non-marked components deletion.
  In Fig. 13(a), a marked component, C_{del}, is deleted. Thus, the total number of joint plant components of C_2 changes from two to one. This modification then leads to the difference between the generated watermark for $P_{1,1}$ and the extracted watermark. As a result, the topological modification of C_2 is detected and located accurately.
  In Fig. 13(b), a non-marked component C_{del} is deleted. Therefore, no joint plant component is assigned to the marked connection point, $P_{2,1}$. The radius of the bounding sphere of C_2 and its joint plant components is also changed. Consequently, during the watermark verification stage, the generated watermark for $P_{2,1}$ is different from the extracted watermark according to the *topology-based watermark generation method*. As a result, the topological modification of C_2, as well as that for $P_{2,1}$, which is induced by the component deletion, is detected and located accurately.
- *Components replacement*. Two main situations arise when replacing plant components from the model: replacing marked plant components and replacing non-marked plant components.
  In Fig. 14(a), a marked component, C_3, is replaced by a plant component, C_{rep}. During the watermarking extraction stage, the connection points of C_{rep} are labeled as non-marked connection points because no watermarks have been embedded into them. Furthermore, C_{rep} is labeled as a non-marked component. As a result, C_{rep} and C_2 are set as suspicious components by applying the *marked plant components selecting principle* because both of them are non-marked components.
  In Fig. 14(a), a non-marked component, C_3, is replaced by a plant component, C_{rep}. This type of attack changes the joint plant component of $P_{2,1}$. In addition, the radius of the bounding sphere of C_2 and its joint plant components could also be changed. Either of the above two modifications can result in a difference between the generated watermark for $P_{2,1}$ and the extracted watermark. Hence, the modification of

the topological relation between C_2 and C_3, which is induced by replacing components, is detected and located accurately.

5.2.2. Joint ends modification

Attacks on the two joint connection ends are discussed in this section. The two attacked connection ends are subject to two different joint plant components. One is a marked connection point, and the other is a non-marked connection point according to the *marked plant components selecting principle*.

This type of attack changes the topological relation logically between the two joint ends. Therefore, the joint connection point of the marked connection point is modified. This modification leads to the difference between the embedded watermark and the calculated watermark during the watermark extraction stage. Consequently, both attacked joint ends are detected.

Notice that, for the tow joint connection ends, they should connect with each other logically and geometrically in practice. However, we can separate one connection end from the other connection end geometrically while keep their topology relation logically. This type of operation should also be regarded as attacks. And our scheme can detect the two attacked connection ends due to the modification of their Laplacian coordinate vectors and the radius of the bounding sphere.

5.3. Discussion on robustness against non-malicious attacks

A good semi-fragile watermarking scheme should be invariant to translation, rotation, uniform scaling and LOD operations. These operations do not change the integrity of the original model and should not be regarded as malicious attacks.

5.3.1. Robustness against similarity transformation

Similarity transforming operations modify the coordinates of the model. Our scheme prefers the lengths of the Laplacian coordinates to the Laplacian coordinates themselves of the marked connection points as watermark carriers. Thus, the scheme is invariant to both translation and rotation. To resist the uniform scaling operation, a registered CRMT is involved in the *quantization-based modulation* stage for watermark embedding and extraction. That is, a model with a larger or smaller size will have larger or smaller quantization steps. Thus, we can also achieve uniform scaling invariance.

5.3.2. Robustness against level-of-detail

For the past several years, the widespread use of collaborative CAPD systems and the reuse of existing CAPD data in new designs have created a data explosion in many application areas. This explosion has resulted in large databases of complex CAPD models. As the complexity of CAPD models increases, the enormous size of these CAD data sets poses a number of challenges in terms of interactive display and manipulation. Thus, CAPD systems must employ methods for filtering out the data that is not contributing to a particular image, and doing it as efficiently as possible. LOD is a key technology for reducing the model complexity and improving the rendering performance for large scale complex CAPD models. An LOD model is a compact description of multiple representations of a single shape and is the key element for providing the necessary degrees of freedom to achieve runtime adaptability. However, connection points and topological relations among plant components will not be influenced by LOD because it can only change the details of entity surfaces. Therefore, the 1-ring neighboring points set of each marked connection point will not be affected. Consequently, this approach will not change the centroid of the neighborhood of the marked points. As a result, our scheme is robust against LOD.

6. Conclusions and future work

This paper presents digital watermarking as a possible topology authentication tool for providing security to 3D CAPD models. Both the topological relations and the singular attributes of plant components are taken into consideration in the watermark generation and embedding. The watermarks are embedded into the coordinates of marked connection points by adjusting the lengths of their Laplacian coordinate vectors. Theoretical analysis and experimental results show that our semi-fragile scheme has a strong ability to detect and locate malicious attacks that are common operations in practical design processes. Meanwhile, our scheme can exactly preserve the geometric shape of plant components and, hence, has no effect on the automatic generation of construction documents.

Although the proposed semi-fragile watermarking technique in this paper is designed for 3D CAPD models, it is believed that our approach is also helpful to watermark other 3D models, except for CAPD models. The proposed technique demonstrates that it is a feasible and effective way to employ the topological information to watermark 3D models. And there have been some watermarking schemes that take the topological information of 3D models into consideration [32].

In its current form, our approach has several limitations. First, our scheme requires a pre-computed mapping table for watermark extraction and tamper detection. In other words, we should reserve a mapping table for each distributed CAPD model, which introduces a level of inconvenience to the practical application of our algorithm. In addition, our scheme can only authenticate and verify the topology integrity of CAPD models. To date, the authentication of geometrical parameters of plant components has not been taken into consideration in our scheme. However, these geometrical parameters are crucial for the automatic generation of construction documents, such as isometrics, orthographies, etc. Hence, in our future work, we intend to improve the performance of our scheme to obtain better practicability. Furthermore, we hope to take both geometrical and topological information into consideration for integrity authentication and verification.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61170250, No. 61103201). The models used in this paper are courtesy of the Beijing Zhongke Fulong Computer Technology Co., Ltd. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] Li L, Zhang D, Pan ZG, Shi JY, Zhou K, Ye K. Watermarking 3d mesh by spherical parameterization. Comput Graph 2004;28(6):981–9.
[2] Lavoué G, Denis F, Dupont F. Subdivision surface watermarking. Comput Graph 2007;31(3):480–92.
[3] Wang YP, Hu SM. A new watermarking method for 3d model based on integral invariant. IEEE Trans Vis Comput Graph 2009;15(2):285–95.
[4] Chou CM, Tseng DC. Affine-transformation-invariant public fragile watermarking for 3d model authentication. IEEE Comput Graph Appl 2009;29(2):72–9.
[5] Wang K, Lavoue G, Denis F, Baskurt A. Robust and blind mesh watermarking based on volume moments. Comput Graph 2011;35(1):1–19.
[6] Liu YJ, Lai KL, Dai G, Yuen MF. A semantic feature model in concurrent engineering. IEEE Trans Autom Sci Eng 2010;7(3):659–65.
[7] Zeng L, Liu YJ, Lee SH, Yuen MF. Q-complex: efficient non-manifold boundary representation with inclusion topology. Comput-Aided Des 2012;44(11):1115–26.
[8] Burdorf A, Kampczyk B, Lederhose M, Schmidt-Traub H. CAPD—computer-aided plant design. Comput Chem Eng 2004;28(1–2):73–81.

[9] Georgiadisa M, Macchietto S. Layout of process plants: a novel approach. Comput Chem Eng 1997;21(Suppl. 1):S337–42.
[10] Guirardello R, Swaney R. Optimization of process plant layout with pipe routing. Comput Chem Eng 2005;30(1):99–114.
[11] Wang K, Lavoué G, Denis F, Baskurt A. A comprehensive survey on three-dimensional mesh watermarking. IEEE Trans Multimedia 2008;10(8): 1513–27.
[12] Wang JR, Feng JQ, Miao YW. A robust confirmable watermarking algorithm for 3d mesh based on manifold harmonics analysis. Vis Comput 2012;28(11):1049–62.
[13] Ohbuchi R, Masuda H, Aono M. Watermarking three-dimensional polygonal models. In: Proceedings of the ACM multimedia, Seattle, USA; 1997. p. 261–72.
[14] Wang YP, Hu SM. Optimization approach for 3d model watermarking by linear binary programming. Comput Aided Geometric Des 2010;27(5): 395–404.
[15] Gao XF, Zhang CM, Huang Y, Deng ZG. A robust high-capacity affine-transformation-invariant scheme for watermarking 3d geometric models. ACM Trans Multimedia Comput Commun Appl 2012;8(S2):34:1–21.
[16] Park HK, Lee SH, Kwon KR. Blind watermarking for copyright protection of 3d CAD drawing. In: Proceedings of the eighth international conference on advanced communication technology, Gangwon-Do, Korea; 2006. p. 253–6.
[17] Kwon K, Lee S, Lee E, Kwon S. Watermarking for 3d CAD drawings based on three components. Lect Notes Comput Sci 2006;4109:217–25.
[18] Kwon K, Chang H, Jung GS, Moon K, Lee S. 3d CAD drawing watermarking based on three components. In: Proceedings of the IEEE international conference on image processing, Atlanta, GA, USA; 2006. p. 1385–8.
[19] Lee SH, Kwon KR. Cad drawing watermarking scheme. Digit Signal Process 2010;20(5):1379–99.
[20] Ohbuchi R, Masuda H, Aono M. A shape-preserving data embedding algorithm for NURBS curves and surfaces. In: Proceedings of the computer graphics international, Alberta, Canada; 1999. p. 180–7.
[21] Lee JJ, Cho NI, Lee SU. Watermarking algorithms for 3d NURBS graphic data. EURASIP J Appl Signal Process 2004;2004(14):2142–52.
[22] Fornaro C, Sanna A. Public key watermarking for authentication of CSG models. Comput-Aided Des 2000;32(12):727–35.
[23] Weng B, Ri JP, Yao ZQ, Yang SC, Feng XQ, Pan ZG. Watermarking t-spline surfaces. In: Proceedings of the 11th IEEE international conference on communication technology proceedings, HangZhou, China; 2008. p. 773–6.
[24] Cheung YM, Wu HT. A sequential quantization strategy for data embedding and integrity verification. IEEE Trans Circuits Syst Video Technol 2007;17(8): 1007–16.
[25] Dow M. Integration of calculation models and CAD systems in building services design. Comput-Aided Des 1987;19(5):226–32.
[26] Peng F, Guo RS, Li CT, Long M. A semi-fragile watermarking algorithm for authenticating 2d CAD engineering graphics based on log-polar transformation. Comput-Aided Des 2010;42(12):1207–16.
[27] Marek M, Schreiber I. Chaotic behaviour of deterministic dissipative. Cambridge University Press; 1991.
[28] Zhang L, Liao X, Wang X. An image encryption approach based on chaotic maps. Chaos Solitons Fractals 2005;24(3):759–65.
[29] Mooney A, Keating J, Heffernan D. A detailed study of the generation of optically detectable watermarks using the logistic map. Chaos Solitons Fractals 2006;30(5):1088–97.
[30] Mooney A, Keating J, Heffernan D. Performance analysis of chaotic and white watermarks in the presence of common watermark attacks. Chaos Solitons Fractals 2009;42(1):560–70.
[31] Yang Y, Ivrissimtzis I. Polygonal mesh watermarking using Laplacian coordinates. Comput Graph Forum 2010;29(5):1585–93.
[32] Beddiaf A, Puech W, Babahenini MC. Topological synchronization mechanism for robust watermarking on 3d semi-regular meshes. In: Proceedings of the 2011 IEEE international conference on multimedia and expo, Barcelona, Spain; 2011. p. 1–6.