Customized Encryption of CAD Models for Cloud-Enabled Collaborative Product Development

X.T. Cai, S. Wang, X. Lu and W.D. Li

Abstract Collaborative product development via cloud has changed the information distribution, organization and management means of traditional product design. Under this new paradigm, product information needs to be shared flexibly to meet collaborators' requirements. Feature-based Computer Aided Design (CAD) models contain abundant intellectual property information. It is paramount to maintain the security of the sensitive information in CAD models while sharing other information of the models in cloud for effective collaboration. The developed security research works for CAD models are still far away from meeting collaboration requirements. In this chapter, an innovative customized encryption approach to support product development collaboration is presented. The approach is composed of a customized encryption algorithm for feature-based CAD models, a key based authorization algorithm for users to decrypt shared features in the models, and a customized geometric transformation algorithm for effective protection mode-based visualization of the models during collaboration. By using this approach, CAD models can be flexibly encrypted to realize the customized sharing of features used for collaboration and protection of other features of the models according to collaboration requirements. A complex case study has been used to verify and illustrate the effectiveness of the approach to industrial applications.

Keywords Customized encryption · CAD model · Product collaboration

X.T. Cai
School of Computer Science and Technology, Wuhan University, Wuhan, China
e-mail: caixiantao@whu.edu.cn

S. Wang · X. Lu · W.D. Li (✉)
Faculty of Engineering and Computing, Coventry University, Coventry, UK
e-mail: weidong.li@coventry.ac.uk

S. Wang
e-mail: sheng.wang@coventry.ac.uk

X. Lu
e-mail: xin.lu@coventry.ac.uk

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_2

1 Introduction

Collaborative product development via cloud is an inevitable trend in the Industry 4.0 era. To optimize design resources, product development companies have been increasingly designing their products in a cloud-enabled collaborative environment. Design features contained in a Computer Aided Design (CAD) model reflect design goal and functions. It is a challenging issue how to effectively protect the sensitive feature information of a model when the model is shared in cloud (Cai et al. 2012; Li and Mehnen 2013). The related research either cannot protect the sensitive information in the sharing process of CAD models effectively or cannot support the sharing of CAD models in the feature level flexibly.

In this chapter, an innovative approach for customized encryption on feature-based CAD models to support collaboration via cloud is presented. The approach supports a typical collaborative scenario illustrated in Fig. 1. In Fig. 1, there are two types of people, i.e., a model owner and collaborators. The model owner uploads an encrypted CAD model into cloud, and collaborators download and decrypt the model from cloud. To effectively share as well as protecting information, features in a CAD model are classified into the following three categories:

- Protected features (e.g., the blades in Fig. 1): The features contain sensitive and private information of the model. These features are only owned by the model owner and not shared with the collaborators. From the collaborators' perspective, the protected features will be only visualized in transformed (deformed) geometry and critical parameters of the features are hidden;

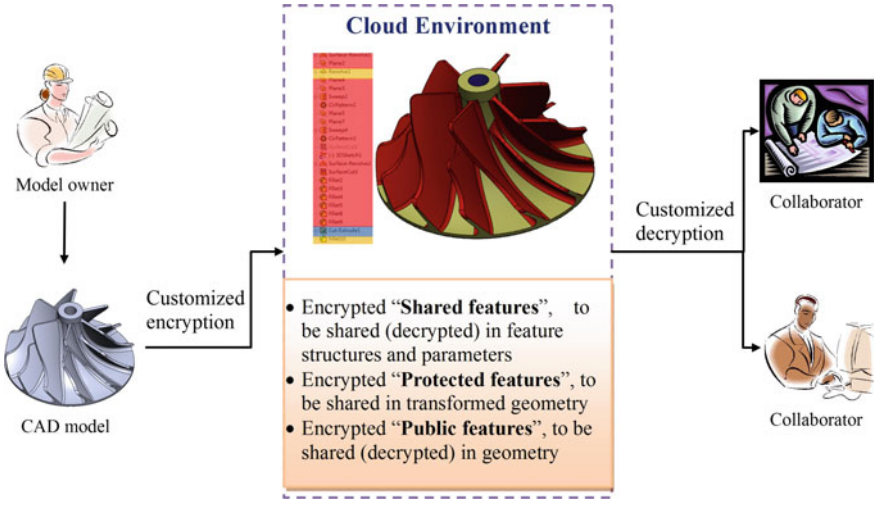


Fig. 1 A typical collaborative scenario for a CAD model

- Shared features (e.g., the central hole in Fig. 1): The shared features are shared to interface with collaborators. The features are encrypted by the model owner, decrypted in the cloud for the collaborators;
- Public features (e.g., the base in Fig. 1): The features do not contain sensitive information. They are shared with collaborators in the form of geometry without deformation.

To process features, this approach is composed by the following algorithms:

- A customized encryption algorithm. In the algorithm, the protected and shared features of a CAD model are encrypted through sketch transformation and random invertible matrices of the features. In addition, the generation of an encryption matrix is controlled in a parametric means to provide flexibility to the model owner to adjust and ensure the security of the model;
- A key based authorization algorithm. When the model owner selects the features to be encrypted, the keys of the shared features are recorded in an authorization file, which is used to decrypt the shared features;
- A customized geometric transformation algorithm. In order to hide the design procedure and feature parameters, the protected features and public features in the CAD model are transformed to a geometric model. The geometric model is combined with the decrypted shared features to collaborators.

The innovations and characteristics of this approach include: (1) Protected, shared and public features can be selected by the model owner flexibly; (2) The CAD model is always manifold and valid in geometry no matter which feature is encrypted or decrypted; (3) The parameters of the model are effectively protected through the encryption and geometric transformation mechanisms; (4) The model owner can authorize any shared feature by issuing the keys of the features to meet the customized requirements of various collaborators; (5) The shared features in the model are still parameterized after decryption to be inter-operated by collaborators flexibly; (6) This approach is content-based and customized and applicable to CAD model-based collaboration in cloud.

In the following sections, the previously developed security approaches for CAD models in networked environments are first reviewed. The approach of customized encryption of feature-based CAD models is then detailed. Finally, case studies and validation of the approach are described.

2 Related Research

The Internet provides convenience for information sharing, but simultaneously, brings security risks during sharing. Security risks have been becoming barriers to implement product development collaboration via the Internet. According to the theory of the information security, there are two main requirements to ensure security during information sharing: (1) Information hiding: an unauthorized user

Table 1 Related security research for collaborative product development

	A	B	C	D	Purpose	Problems
Watermark	√			√	Protect the intellectual property by embedding the watermark into CAD models	Design information (design knowledge, parameters) cannot be hidden by watermark in a safe way
Access control		√	√		Control the access of the design data by users' authorization according to a group of access control rules	Unable to support information protection of a CAD model
Multi-resolution approach		√		√	Multi-resolution is to simplify a CAD model during data sharing in a network with limited bandwidth	It can realize the secure sharing of a CAD model to some degrees, but not flexibly
Encryption of CAD models		√		√	Hide the design information by encryption	No research applied to CAD models

Notes: A—Information authentication; B—Information hiding; C—Architecture-level security; D—Data-level security

cannot access the confidential information; (2) Information authentication: information has a verification capacity which can ensure the information has not been changed (Rutledge and Hoffman 1986). Various research works about the secure sharing of CAD models have been developed according to the above two requirements. The developed approaches can be classified in Table 1. More technical details are expanded below.

2.1 Watermark of CAD Models

The watermark concept was first proposed (Tirkel et al. 1993). The digital watermarking technology is used for the intellectual property protection and the integrity authentication of electronic files. The creation information and logo of a creator are embedded in an electronic file. Watermark embedded into a product model cannot be removed during sharing, and the information can be detected by a special software package (Tao et al. 2012). Various watermarking approaches for 2D/3D CAD models were developed for intellectual property protection (Cayre et al. 2003; Chou and Tseng 2006; Wang et al. 2008; Ai et al. 2009; Peng et al. 2011; Lee and Kwon 2012; Su et al. 2013). However, the design information can still be retrieved so that the model is not safe.

2.2 Access Control of CAD Models in a Network Environment

Access control is an important security method for a network environment. Access to special resources is controlled by users' authorization. The related works can be classified in the following categories.

The general access control approaches. The access control appeared in the 1970s. Lampson initiated the concept of access matrix. The access control became an important approach for information protection in networked environments (Lampson 1974). Conway used the concept of secure matrix for access control, and standardized the secure matrix and finally presented the theory of discretionary access control (Conway et al. 1972). Later, more access control approaches were developed. A role based access control approach was developed (Sandhu et al. 1996). Task role-based Access Control was proposed (Oh and Park 2003), and Usage Control called the next generation of access control model was presented (Park and Sandhu 2004).

The access control approaches of files. To support product development collaboration, many special access control approaches were developed. van der Hoeven proposed an access control based CAD architecture (van der Hoeven et al. 1994). However, access control is still file based. Stevens developed an ADOSX system to support product development collaboration between two enterprises, while the system just focuses on the access control of files (Stevens and Wulf 2002). Cera et al. developed a secure access control mechanism for 3D models (Cera et al. 2006). The approach, however, supports the collaborative view of product models not the full-scale collaborative design. Leong et al. devised a security approach for a distributed product data management system. The approach combines the Lampson's access matrix and it is still file based (Leong et al. 2003).

The sharing space based access control approaches. Considering the frequent sharing of design data, sharing space based access control methods were proposed, in which a secure sharing space was designed. A dynamic data sharing and security approach for product development collaboration was developed (Rouibah and Ould-Ali 2007). Chang et al. developed the security system for sharing engineering drawings in the sharing space (Chang et al. 2008).

The multi-method based access control methods. In order to improve the security during product development collaboration, multi-method based access control methods were proposed. Some other security methods are combined with access control to ensure better security. Yao devised a security model of data for collaborative design and management system, which combines multi security methods with access control (Yao et al. 2007). A security system for sharing CAD drawings which used a multi-method approach was developed (Chang et al. 2008). Speiera et al. also used a multi-method approach to mitigate product safety and security risks (Speiera et al. 2011). A network security mechanism for the

collaborative combined Virtual Private Network and access control was proposed (Xiang and Li 2012).

The access control method constructs a secure environment based on the architecture level. On the other hand, all the existed general and special access control approaches are file based. They cannot handle the case that a CAD model contains both confidential information and sharing information.

2.3 *Multi-level Design Data Sharing Based on the Multi-resolution Models*

Multi-resolution modeling can be used for the secure sharing of CAD models. The approaches can be classified further into the following categories.

Multi-resolution mesh model. In the past, a solid model is changed to a mesh model, and then the mesh model is transformed to a multi-resolution mesh model for model simplification (Hoppe 1996). Han proposed a multi-resolution modeling approach of CAD models to support collaborative design (Han et al. 2003), Qiu et al. designed a T-Curve based simplification method for CAD models (Qiu et al. 2004). Li et al. present a 3D simplification algorithm for distributed visualization (Li et al. 2007). All the methods are mesh model based. However, a mesh model lacks design information (history, features, parameters and so on) to support product collaboration effectively.

Multi-resolution B-rep, solid and feature modeling. Belaziz et al. provided an analysis tool of a B-rep model, which can delete some features without any complex Boolean operations (Belaziz et al. 2000). A B-rep based multi-resolution modeling method based on the Wrap-Around was developed (Seo et al. 2005); Wrap-around, smooth-out and thinning were integrated to develop a new B-rep based multi-resolution modeling method (Kim et al. 2005). Lee et al. designed the Progressive Solid Model (PSM) to support the multi-resolution solid model (Lee et al. 2004). A feature based multi-resolution modeling method was developed (Lee 2005), which is based on the calculation of the valid volume.

Combination of the multi-resolution feature model and the access control. Cera et al. combined the multi-resolution modeling and access control to realize the access control of multi-level CAD models (Cera et al. 2006). Chu et al. focused on multi-level data sharing based on multi-LOD (Level of Detail) models (Chu et al. 2009). A matrix-based modularization approach for supporting collaboration in parametric design was developed (Li and Mirhosseini 2012).

Multi-level design data sharing based on the multi-resolution models can realize the customized secure sharing of a CAD model in some degrees. However, this method is not flexibly enough due to the following limitations: (1) The hidden information cannot be selected by the model owner; (2) The approaches cannot support collaboration freely because the sharing model is not complete.

2.4 Encryption of CAD Models

Data encryption is an important approach for information hidden in network. It can ensure that the hidden information cannot be obtained by unauthorized users. In recent years, the encryption methods have been widely used for multi-media data, such as the image encryption. Due to the complexity, there are a few research works about 3D models. Huang et al. proposed a method of encrypting 3D data information with virtual holography (Huang et al. 2009). Esam and Ben proposed secured sharing approaches for 3D mesh model encryption (Esam and Ben 2011). An approach for encryption based multi-level data access control to share the images in a collaborative environment was developed (Naveen and Thomas 2011) On the other hand, until now, there are few research works about the encryption of CAD models.

2.5 Summary of the Related Works

The requirements for customized sharing of CAD models are complex. Based on the above discussions, the existing research for the secure sharing of design data has the following shortages: (1) Lack of flexible and feature based protection mechanism; (2) Lack of different levels of security; (3) Lack of flexible authorization mechanism for accessing CAD models;.

To support complex collaboration requirements, it is imperative to develop a more flexible encryption approach with the following characteristics: (1) The approach needs to support a model owner to flexibly realize customized protection of a CAD model for different users; (2) The approach should provide user friendliness and flexible control to ensure less deformation and geometric validity of CAD model during customized encryption; (3) The approach is feature based.

3 Customized Encryption of Feature-Based CAD Models

Data encryption is an important approach for information protection in a network environment. Effective approaches can prevent the sensitive information to be obtained by unauthorized users. In the early time, any files represented in binary formats are regarded as encrypted. Later, content based encrypted approaches based on the encryption of the basic content elements appeared. Based on that approaches, the encrypted file could be open. However, the content cannot be distinguished correctly by unauthorized users (such as the image encryption). As thus, content-based encryption can be used to protect the information of a CAD model when it is being shared. The approach presented in this chapter is content-based, and a new research work for customized encryption of CAD models.

3.1 Encryption of a CAD Model

A group of design or manufacturing features and their related position constraints are the building blocks of a CAD model. As thus, a CAD model can be defined as the following Representation (1).

$$M = \bigcup_{i=1}^{n} (C_i \otimes f_i) \tag{1}$$

where M denotes a CAD model, and f_i means a feature of M, C_i is a set of containing all the constrains between f_i and its father features, $\otimes$ means a geometric operation on the model applied by the constraints on the features.

A definition of the constraint between two features is given as following.

Definition 1 $\forall f \in M$ *and* $\forall f' \in M$, $f \rightarrow f'$ *means* f *has* constraints propagated to f'.

Where M is a CAD model, the f and f' are both the features of M.

Definition 2 If $a \propto b$, means the shape of a is decided by b.

According to Definition 2 and Representation (1), Representation (2) is given below, which means the shape of a CAD model is decided by all its features.

$$M \propto \bigcup_{i=1}^{n} f_i \tag{2}$$

According to the constitution of a feature, the features can be classified as two types: Sketch Based Feature (SBF) and Non Sketch Based Feature (NSBF).

Definition 3 Sketch Based Feature (SBF). SBF means the feature's creation is based on its sketch(es), and the primary shape of a SBF is decided by its sketch(es)

Definition 4 Non Sketch Based Feature (NSBF). NSBF means the feature's creation is dependent on its nesting feature(s), and the primary shape of a NSBF is decided by its nesting feature(s)

The above can be represented in Representation (3):

$$\forall f_i \in M, \quad f_i \propto \begin{cases} \bigcup_{j=1}^{p_i} s_j, & (f_i \, is \, SBF) \\ \bigcup_{j=k_1}^{q_i} f_j, & (f_i \, is \, NSBF) \end{cases} \tag{3}$$

where $\cup_{j=1}^{m_i} s_j$ is the sketch set of f_i if it is a SBF, p_i means the number of the sketches; and $\cup_{j=k_1}^{m_i} f_j$ is the nesting feature set of f_i if it is a NSBF, q_i means the number of the nesting features and k_1 means the id of the basic feature f_{k_1}. Obviously, the first feature of any CAD model is SBF.

Based on Representation (2) and Representation (3), Theorem 1 is given.

Table 2 Proof of Theorem 1

Step 1: To prove the shape of any feature is finally decided by a group of sketches.

(1) For the features in Level 0

$\because$ f_0 *is the first feature of model M*

$\therefore$ f_0 *is a BSF*

$\therefore$ *According to Representation (3):* $f_0 \propto \bigcup_{j=1}^{p_0} s_j$

(2) For the features in Level 1

Based on the DLG, for any feature on Level 1: $\forall f_{1i}.level = 1$

$\because$ f_0 *is the only feature in Level 0, according to Representation (3):*

$$f_{1i} \propto \begin{cases} \bigcup_{j=1}^{p_{1i}} s_j, (f_{1i} \text{ is SBF}) \\ f_0, (f_{1i} \text{ is NSBF}) \end{cases}$$

$\because$ $f_0 \propto \bigcup_{j=1}^{p_0} s_j$

$\therefore$ $f_{1i} \propto f_0$

$\therefore$ $f_{1i} \propto \bigcup_{j=1}^{p_0} s_j$

$\therefore$ $$f_{1i} \propto \begin{cases} \bigcup_{j=1}^{p_{1i}} s_j, (f_{1i} \text{ is SBF}) \\ \bigcup_{j=1}^{p_0} s_j, (f_{1i} \text{ is NSBF}) \end{cases}$$

(3) For the features in Level n

$\therefore$ *The rest may be deduced by analogy*

Based on the DLG, for any feature on Level n: $\forall f_{ni}.level = n$

$\because$ $$f_{ni} \propto \begin{cases} \bigcup_{j=1}^{p_{ni}} s_j, (f_{1i} \text{ is SBF}) \\ \bigcup_{j=k_1}^{q_{ni}} f_j, (f_{1i} \text{ is NSBF}) \end{cases}$$

$\therefore$ *if* $f_{ni} \propto \bigcup_{j=k_1}^{q_{ni}} f_j$ *, then* $f_{ni} \propto \bigcup_{j=k_1}^{q_{ni}} (\bigcup_{t-1}^{p_{k_1}} s_t)$

$\therefore$ $$f_{ni} \propto \begin{cases} \bigcup_{j=1}^{p_{ni}} s_j, (f_{1i} \text{ is SBF}) \\ \bigcup_{j=k_1}^{q_{ni}} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is NSBF}) \end{cases}$$

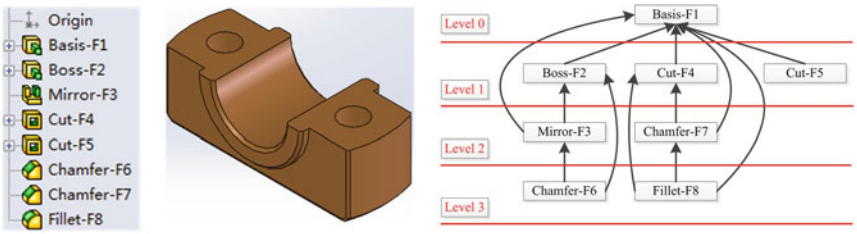
Step 2: To prove the primary shape of any CAD model is finally decided by a group of sketches.

$\because$ *According to Representation (2),* $M \propto \bigcup_{i=1}^{n} f_i$

$\therefore$ $$f_i \propto \begin{cases} \bigcup_{j=1}^{p_i} s_j, (f_{1i} \text{ is SBF}) \\ \bigcup_{j=k_1}^{q_i} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is NSBF}) \end{cases}$$

$\because$ $\begin{cases} \bigcup_{j=1}^{p_i} s_j, (f_{1i} \text{ is SBF}) \\ \bigcup_{j=k_1}^{q_i} (\bigcup_{t-1}^{p_{k_1}} s_t), (f_{1i} \text{ is NSBF}) \end{cases}$ *is a sketch set represented as* S_i

$\therefore$ $M \propto \bigcup_{i=1}^{n} S_i$



(a) the feature tree (b) the CAD model (c) the DLG

Fig. 2 An example of the DLG

Theorem 1 *The shape of a CAD model is decided by all the sketches included in the CAD model.*

Theorem 1 can be proved as Table 2. In order to prove Theorem 1, a Dependence Level Graph (DLG) is defined first.

Definition 5 DLG: For a CAD model M, f_i is a feature and $f_i \in M$, N_i is a node of a DLG. $N_i = (id, level,$ parent$\{\}, children\{\})$. *id* denotes the id of f_i; *level* denotes the level of f_i in the hierarchical DLG (For instance, if the max level value of f_i's parent features is n, the *level* value of f_i is $n + 1$). *parent{}* is a set of f_i's parent features; *children{}* is a set of f_i's children features.

An example is given in Fig. 2. Figure 2a shows the feature tree of a CAD model, Fig. 2b shows the CAD model, and Fig. 2c shows the DLG of the CAD model.

As proved above, because the primary shape of a CAD model is decided by all the sketches belonging to the CAD model, the sketches of the CAD model are its key elements. The encryption of the sketch set in a CAD model realizes its shape encryption, and the encryption of a sub-set of the sketch set in a CAD model realizes its shape encryption.

3.1.1 Encryption of Sketches

The sketch in a CAD model is a 2D or 3D graph. The coordinate of point i in a sketch can be expressed as $(x_{i1}\ x_{i\ldots}x_{in})$, the sketch can be expressed as Representation (4), n denotes the dimension of the sketch and m denotes the number of points in the sketch.

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}, (n = 2 || n = 3) \tag{4}$$

The goal of encrypting sketches is to protect the shape of a CAD model when it is shared and interoperated, so that there are two assumptions for the sketch

encryption: (1) The encryption is secure enough; (2) The encrypted CAD model is valid (remains manifold) which can be shared and interoperated.

To meet the requirements, a random invertible matrix based encryption method is developed with the following characteristics. (1) The random invertible matrix transformation can defend almost all the common attacks. Because the encryption method is based on a random invertible matrix, various attack methods for the periodic matrix based transformation of graph are invalid; since the encrypting key is generated temporarily for every feature, the most dangerous "Known Plaintext Attack" (Rajput and Nishchal 2013) and "Chosen Plaintext Attack" (Barrera et al. 2010) for the periodic matrix based transformation of graph are also invalid; and the random invertible matrix is random, so that it is cannot be guessed. (2) The random invertible matrix transformation can change the shape of a feature, but its topology is not changed to guarantee the validity of the encrypted CAD model.

The realization process of the above is as follows. A_{nn} is a random invertible matrix, and S_{mn} is a sketch, the encryption of S_{mn} is as Representation (5):

$$S_{mn} \times A_{nn} = S'_{mn}, A_{nn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \tag{5}$$

As the random invertible matrix is invertible, the inverse matrix of A_{nn} exists, represented as A_{nn}'. The sketch can be decrypted directly by its inverse matrix, as Representation (6):

$$S_{mn} = S'_{mn} \times A'_{nn} \tag{6}$$

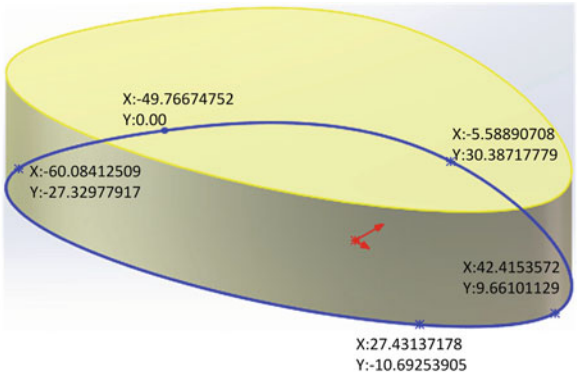
Because the features have a set of constraints, once the shape of a feature is changed, the following features maybe wrong. In order to guarantee the encrypted model is valid, the transformation of the feature should be able to be adjustable to some degrees.

For a point in a sketch, it can be described as $X = (x_1\ x_{2\ldots}x_n)$. According to Representation (4) and Representation (5), the transformation of the X is as Representation (6). Any element in the X' can be expressed as Representation (7):

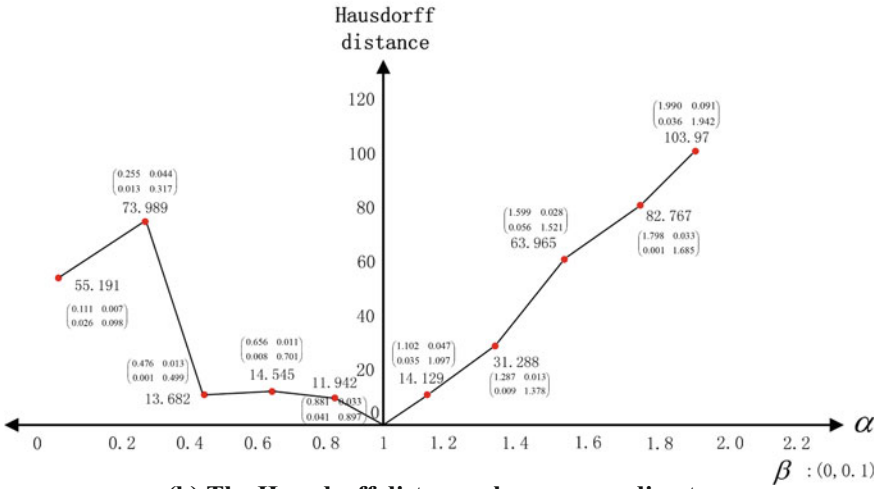
$$X' = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \times \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} x'_1 & x'_1 & \cdots & x'_n \end{pmatrix} \tag{7}$$

$$x'_i = x_i \times a_{ii} + (x_1 \times a_{1i} + x_2 \times a_{2i} + \cdots x_n \times a_{ni}) \tag{8}$$

The polynomial of $(x_1 \times a_{1i} + x_2 \times a_{2i} + \ldots x_n \times a_{ni})$ can be replaced by δ_i, Representation (8) is changed to Representation (9)



(a) The initial feature *f*



(b) The Hausdorff distance change according to α

Fig. 3 The transformation of the feature f

$$x_i^{'} = x_i \times a_{ii} + \delta_i \tag{9}$$

When $\delta_i << x_i \times a_{ii,}$ the transformation of x_i' based on the coefficient a_{ii} is similarly linear. Therefore the random invertible matrix is defined as Representation (10). α, β, Δ_1, Δ_2 are the parameters used to adjust the matrix.

$$A_{nn} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \; a_{ij} \begin{cases} i = j, \; a_{ij} \in (\alpha - \Delta_1, \alpha + \Delta_1) \\ i \neq j, \; a_{ij} \in (\beta - \Delta_2, \beta + \Delta_2) \end{cases}, \; |A_{nn}| \neq 0 \tag{10}$$

When α << β, the transformation of the sketch is controllable. As shown in Fig. 3, the feature *f* is encrypted by different matrices, Fig. 3b shows the Hausdorff distance between the initial feature and the encrypted feature with different values of α (the Hausdorff distance is used to express the degree of similarity between two models (Tang et al. 2009)). When α << β (as the right of the axis), the change of the Hausdorff distance based on the adjustment of α is approximately linear. When the value of α is close to the value of β (as the left of the axis), the change of the Hausdorff distance based on the adjustment of α is uncertain.

Based on the above analysis, the transformation of sketches can be justified by changing the values of α and β to guarantee the validity of the CAD model. According to Representation (10), when $\alpha = 1$ & $\Delta_1 = 0$ and $\beta = 0$ & $\Delta_2 = 0$, the encrypted feature is the same to the initial feature, so the model is valid when the feature is encrypted. When $\beta << \alpha$, according to Representation (10), the effect of δ_i is stable, the transformation degree is mainly affected by the value of α, and the transformation is controllable according to the value change of α; when the β and α are close, according to Representation (6), the effect of δ_i is obvious and the transformation is uncontrollable according to the value change of α.

3.1.2 Encryption Algorithm of CAD Models

In order to support the flexible customized sharing of CAD models, every feature must have its own encryption key. The key generation algorithm based on Representation (10) is shown in Table 3.

Based on Algorithm 1 and Representation (1), the feature encryption algorithm is given in Fig. 4.

Table 3 Key_generation (α, β, Δ1, Δ2, n)

```
1.  //α, β, Δ1, Δ2 arethe adjusting parameters of the key and n is the dimension of
    key
2.  double A[n][n];
3.  do {
4.  for (int i=0; i<n; i++)
5.  for (int j=0; j<n; j++)
6.      {
7.  if i=j
8.  { A[i][j]=Random(α,Δ1); } //means getting a random digit in the(α-Δ1, α+Δ1)
9.  else
10.       { A[i][j]=Random(β,Δ2);}//means getting a random digit in the(β-Δ2, β+Δ2)
11.     }
12. }while (|A|=0)
```

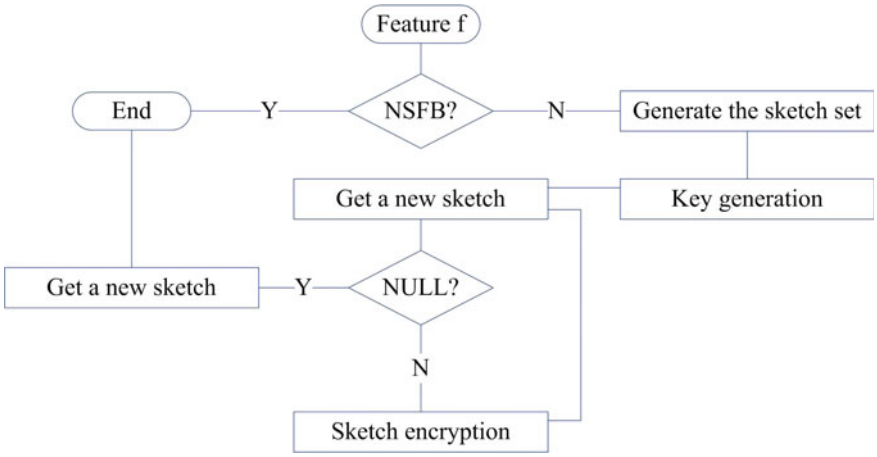


Fig. 4 Feature encryption algorithm

To support the flexible customized sharing of the CAD model, the encrypted model must be valid. According to Representation (1) and Representation (2), the validity of a CAD model in the model encryption is defined as follows.

Definition 6 If the features of the CAD model are created successfully, all the constraints of every feature are valid, so that the CAD model is manifold. As thus, the model is valid.

Based on the Definition 6, three conditions must be satisfied in the encryption process of a CAD model to guarantee the customized encrypted model is valid. The three conditions are as follows.

Condition 1: The CAD model M, is encrypted from bottom to top based on its DLG.

Condition 2: For any feature f in M, after the encryption of f, all the constraints of f are still valid and the M is manifold.

Condition 3: For any feature f in M and its any child feature f', decrypt the f' after the encryption of f, all the constraints of f' are still valid and M is manifold.

A theorem for validity of CAD model is given as Theorem 2.

Theorem 2 *If the above three conditions are satisfied in the encrypting process of a CAD model, no matter which part is encrypted in the model, the encrypted model remains valid.*

The encryption algorithm of CAD models is given in Fig. 5, and Fig. 6 shows the encrypting procedure of a CAD model. When the feature of Cut-F4 is encrypted, Condition 2 is not satisfied, so that the value of α and β are adjusted to satisfy Condition 2. When the feature of Basis-F1 is encrypted, Condition 3 is not satisfied, so that the value of α and β are adjusted to satisfy Condition 3.

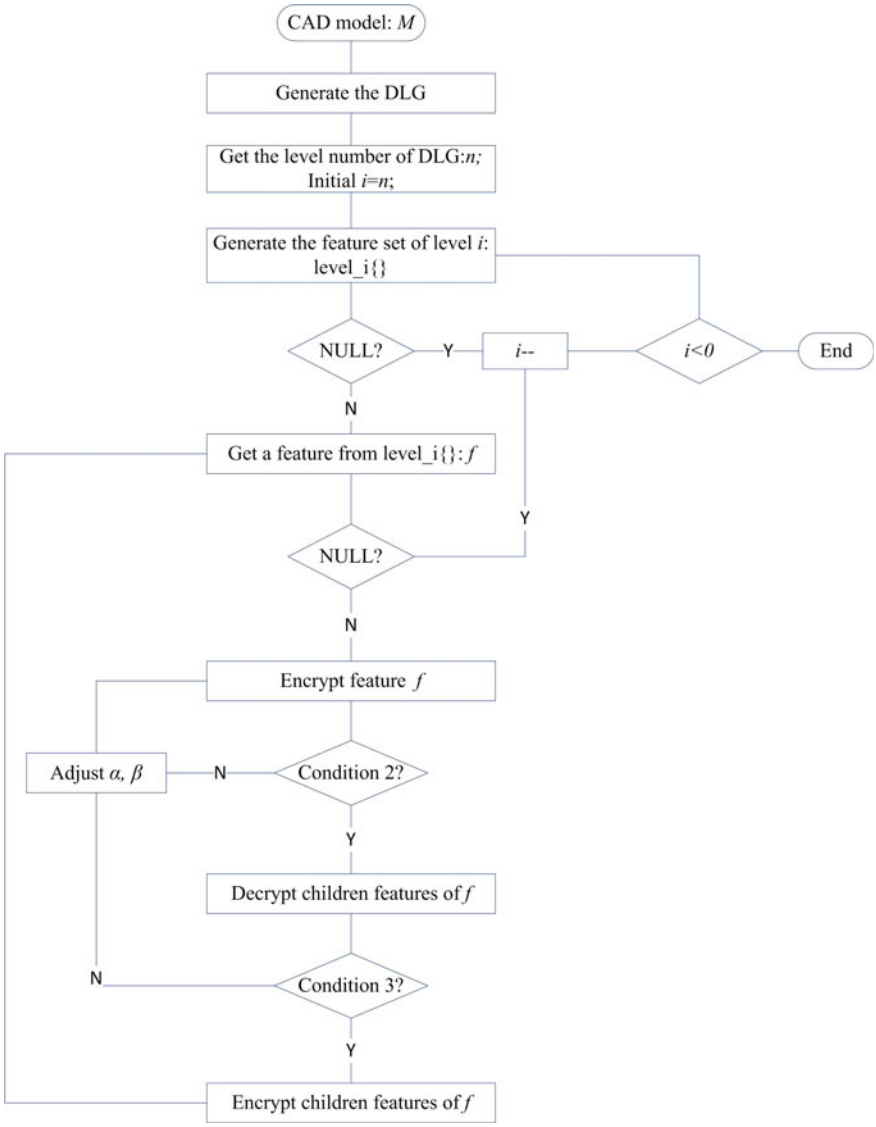


Fig. 5 Encryption algorithm of CAD models

3.2 Encryption Based Secure Sharing of CAD Models

3.2.1 Key-Based Authorization Algorithm

Before a CAD model is shared, the model owner should authorize the shared features for decryption and assign protected and public features. After the

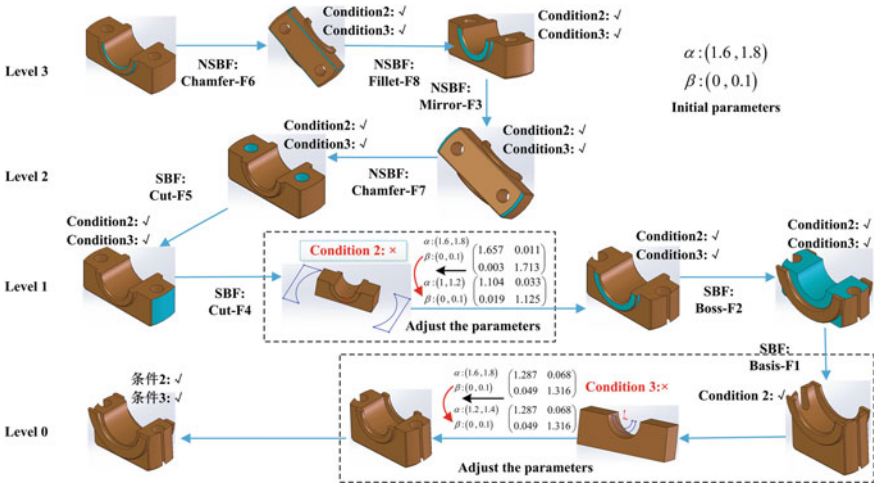


Fig. 6 The encryption procedure of a CAD model

Table 4 Authorization (*M*)

```
1.  get the feature set of M: feature{}
2.  initial key file Key_F.
3.  while(feature{}!=NULL)
4.  {
5.  get fi from feature{}
6.  if fi is public part
7.      {
8.   Key.id= fi.id;
9.    Key. matrix=fi.matrix;
10.  Key. attribution=Public;
11.     }
12. else if fi is sharing part
13.     {
14.  Key.id= fi.id;
15.  Key.matrix=fi.matrix;
16.  Key. attribution=Sharing;
17.     }
18. feature{}= feature{}- fi;
19.    add key to Key_F
20. }
```

authorization is given by the model owner, the keys of shared features (the encryption matrices of the features) are retrieved from the Cloud Databases and recorded in an authorization file. The authorizing process is as in the following Table 4.

3.2.2 Customized Geometric Transformation Algorithm

When an authorized collaborator gets the encrypted CAD model and key file, the collaborator would visualize the model and interoperate on the shared features for collaboration. The CAD model owned by the collaborator has two parts: first part is geometric model and the second part is still feature-based on top of the geometric model. The geometric transformation algorithm contains the following three phases:

- **Model decryption**. The DLG of the encrypted CAD model (M_1) is created first, and then the CAD model is decrypted from top to down according to the key file based on the DLG (the decryption process is the inverse process of encryption). After the decryption, a decrypted model is generated: M_2;
- **Shared feature retrieval**. After the geometric transformation, the topology of the CAD model is changed. However, the constraints among features are based on the topological entities. Therefore it should to map the related topological entities into the decrypted model after the geometric transformation. When every shared feature is decrypted, its related information including the geometric representation of constraints and parameters are retrieved and recorded in an XML file;
- **Geometric transformation**. After the retrieval of the shared features, delete all the shared features from M_2, and the rest model is M_3. Then transform M_3 to M_4 which is a geometric format model. Later, retrieve the information of the shared feature from the XML file, and map the topological entities of position constraints based on their geometric representation. Finally, the shared features are recreated in M_4. After that, the final secure shared CAD model is generated: M_5.

4 Case Study for Approach Validation

A real example (provided by the SolidWorks 2012) is given below to verify the approach presented in this chapter. The propeller is one of the key parts in a plane. The design of vane contains rich design knowledge and semantics, so that in a collaborative scenario this feature and parameters should be protected. The following is the process of the applying the approach.

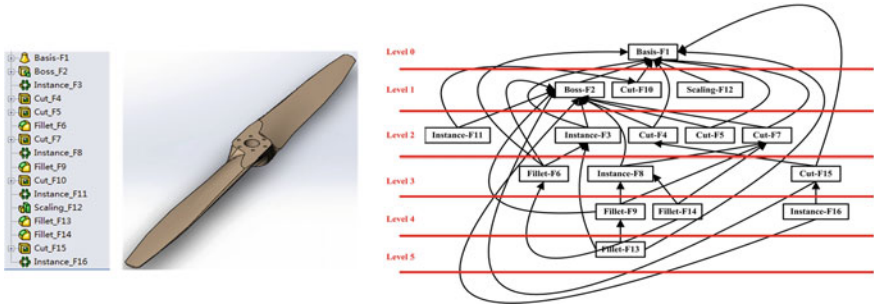
STEP 1: Model encryption

Figure 7a shows the propeller part (M_0) and its feature tree. Based on the feature tree, the DLG is created as Fig. 7b.

According to the encryption algorithm, M_0 is encrypted to M_1. Figure 8b shows the shape comparison between M_0 (in Green) and M_1 (in Red). Table 5 shows the difference of geometry attributions between M_0 and M_1.

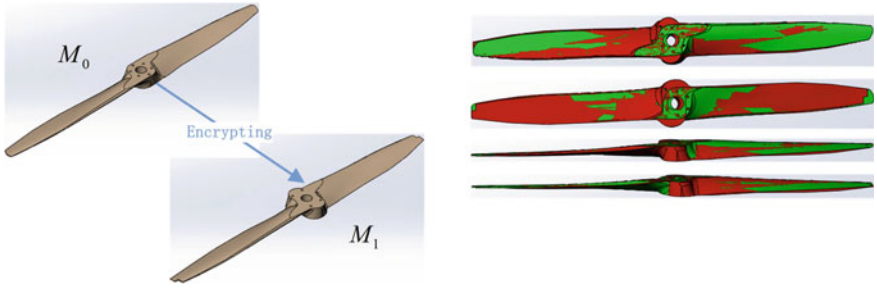
STEP 2: Key-based authorization

As shown in Fig. 9, when the propeller part needs to be shared, the protected features and shared features should to be assigned. The red part is protected part and it contains four features (Basis-F1, Instance-F3, Cut-F10, and Instance-F11), the



(a) The model M_0 and its feature tree (b) The DLG of M_0

Fig. 7 The initial model M_0 and its DLG



(a) The M_0 is encrypted to M_1 (b) The shape comparison between M_0 and M_1

Fig. 8 M_0 is encrypted to M_1

blue part is shared part and it contains two features (Cut-F15 and Instance-F16), and the rest green part is public part and it contains all the rest features (Boss-F2, Cut-F4, Cut-F5, Fillet-F6, Cut-F7, Instance-F8, Fillet-F9, Scaling-F12, Fillet-F13 and Fillet-F14). According to the Authorization algorithm, all the keys of the features belonging to the blue part and green part are recorded into a key file. Finally, the key file and M_1 are sent to the authorized collaborator.

STEP 3: Decrypted model generation

Figure 10 shows the process of secure sharing. The details are below:

(1) According to the key file, M_1 is decrypted to M_2 (as in Fig. 10b).
(2) Retrieve the sharing features into an XML file. Figure 11 shows a part of the XML file and the feature information of Cut-F15.
(3) Delete the sharing features from M_2, and get M_3 (as in Fig. 10c).
(4) Transform M_3 to the geometric model, and get the M_4 (as in Fig. 7d)
(5) Recreate the sharing features based on the XML file in M_4, get the final shared model M_5 (as in Fig. 10e).
(6) M_5 is interoperated as Fig. 10f, and the propeller part is shared in a secure means.

Table 5 Comparison between M_0 and M_1

	Original M_0	Encrypted M_0: M_1
Mass (g)	65.67	77.96
Volume (mm^3)	65673.14	77959.78
Surface area (mm^2)	37741.96	40596.08
Center of mass (mm)	X = −6.90 Y = −1.51 Z = −42.25	X = −6.72 Y = −1.89 Z = −37.99
Principal axes of inertia and principal moments of inertia: (g * mm^2) Taken at the center of mass	Ix = (0.01, −0.00, 1.00) Px = 6700.91 Iy = (1.00, −0.00, −0.01) Py = 578276.11 Iz = (0.00, 1.00, 0.00) Pz = 582857.97	Ix = (0.01, −0.00, 1.00) Px = 11831.11 Iy = (1.00, −0.00, −0.01) Py = 674162.27 Iz = (0.00, 1.00, 0.00) Pz = 683256.19
Moments of inertia: (g * mm^2) Taken at the center of mass and aligned with the output coordinate system	Lxx = 578166.05, Lxy = 0.00, Lxz = 7930.56 Lyx = 0.00 Lyy = 582857.97, Lyz = 0.00 Lzx = 7930.56, Lzy = 0.00, Lzz = 6810.97	Lxx = 674125.01, Lxy = −0.34, Lxz = 4967.97 Lyx = −0.34, Lyy = 683256.19, Lyz = −4.08 Lzx = 4967.97, Lzy = −4.08, Lzz = 11868.38
Moments of inertia: (g * mm^2) Taken at the output coordinate system	Ixx = 695546.85, Ixy = 685.25, Ixz = 27076.50 Iyx = 685.25, Iyy = 703215.49, Iyz = 4195.77 Izx = 27076.50, Izy = 4195.77, Izz = 10088.03	Ixx = 786920.83, Ixy = 992.83, Ixz = 24880.40 Iyx = 992.83, Iyy = 799296.10, Iyz = 5607.88 Izx = 24880.40, Izy = 5607.88, Izz = 15672.27

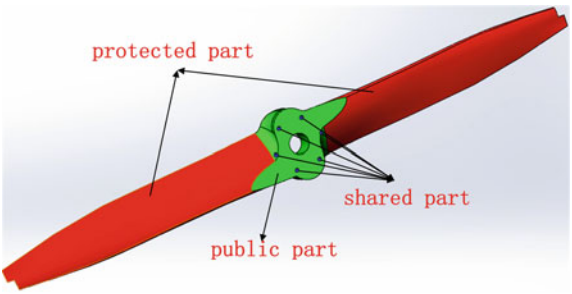


Fig. 9 Key-based authorization of M_1

(7) Figure 10g shows that the propeller part is shared directly without any secure mechanism. Figure 10f shows that the propeller part is shared securely based on the approach presented in this chapter. Figure 10h shows that, in the sharing of the propeller part, the shape of the vanes is protected, the green one is the initial part and the red one is the encrypted one.

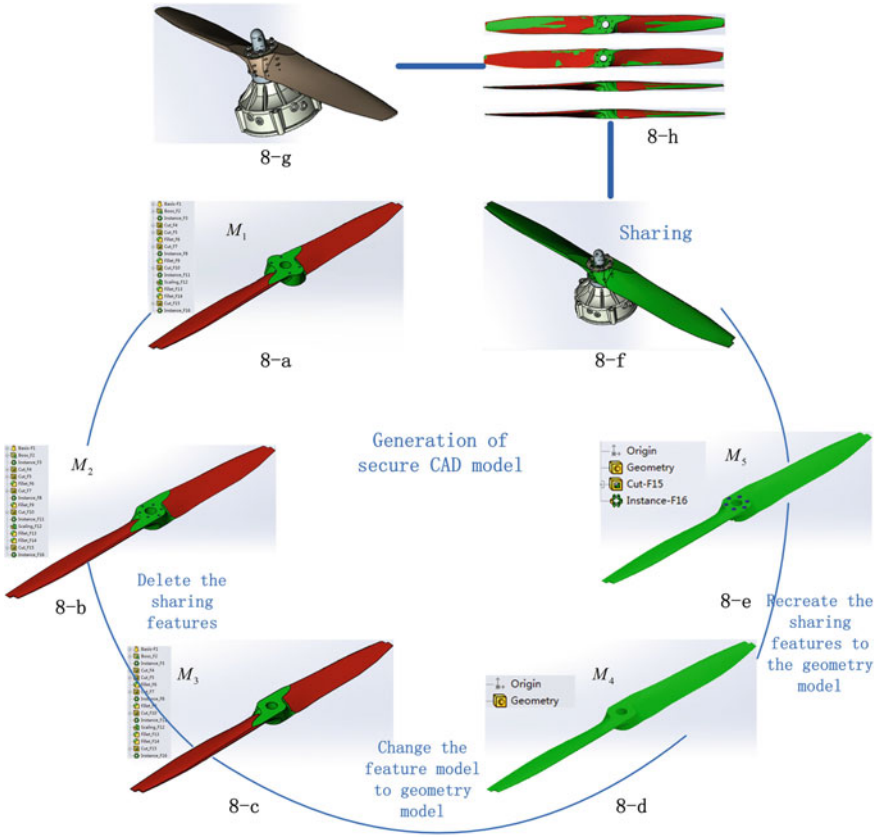


Fig. 10 The secure sharing of the propeller part

5 Conclusion and Future Works

In this chapter, an innovative encryption approach for CAD models in a cloud-enabled collaborative product development is presented.

The unique characteristic of the approach is that protected, shared and public information can be decided by a model owner flexibly. Based on the approach, different features have different keys, supporting the feature-based encryption and decryption of a CAD model under different collaboration scenarios. Besides, the encryption method is robust, so that no matter which feature of the CAD model is encrypted, the CAD model is still valid. Therefore, this approach provides a flexible, customized, and robust collaborative way for CAD model-based cooperation in cloud. A complex case study is used to prove the effectiveness and great potential industrial applicability of the approach.

Fig. 11 Part of the temporary XML file

```
- <F1>
    <F_id>Cut-F15</F_id>
    <Attribution>Sharing</Attribution>
  - <Constraint>
      <Type>Face</Type>
      <Point_x>8.09978176mm</Point_x>
      <Point_y>-42.25mm</Point_y>
      <Point_z>0</Point_z>
      <normal>(0,0,1)</normal>
    </Constraint>
  - <Feature_Info>
      <Type>Cut</Type>
      <Height>35mm</Height>
    - <Sketch1>
      - <Element1>
          <Type>Circle</Type>
          <Center_x>8.09978176mm</Center_x>
          <Center_y>-42.25mm</Center_y>
          <Radius>3.2mm</Radius>
        </Element1>
      </Sketch1>
    </Feature_Info>
</F1>
```

The further research work is ongoing from two aspects. First, the protected and shared features need to be recognized automatically based on the analysis for the semantics of the CAD model. Second, the approach will be expended to the secure sharing of assembled products.

Acknowledgements This work is supported by the National Science Foundation of China (Grant No. 61303215), EU FP7 Smarter project (FP7-PEOPLE-2013-IAPP-610675) and EU FP7 Cloudflow project (FP7-2013-NMP-ICT-FoF-609100).

References

Ai QS, Liu Q, Zhou ZD et al (2009) A new digital watermarking scheme for 3D triangular mesh models. Signal Process 89:2159–2170

Barrera JF, Vargas C, Tebaldi M et al (2010) Chosen-plaintext attack on a joint transform correlate or encrypting system. Opt Commun 283:3917–3921

Belaziz M, Bouras A, Brun JM (2000) Morphological analysis for product design. Comput Aided Des 32(5–6):377–388

Cai XT, Li XX, He FZ et al (2012) Flexible concurrency control for legacy CAD to construct collaborative CAD environment. J Adv Mech Des Syst Manuf 3(6):324–339

Cayre F, Alface PR, Schmitt F et al (2003) Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry. Signal Process 18:309–319

Cera CD, Braude I, Kim T et al (2006) Hierarchical role-based viewing for multilevel information security in collaborative CAD. J Comput Inf Sci Eng 1(6):2–10

Chang HB, Kim KK, Kim YD (2008) The development of security system for sharing CAD drawings in u-environment. Comput Inf 5(27):731–741

Chou CM, Tseng DC (2006) A public fragile watermarking scheme for 3D model authentication. Comput Aided Des 38:1154–1165

Chu CH, Wu PH, Hsu YC (2009) Multi-agent collaborative 3D design with geometric model at different levels of detail. Robot Comput Integr Manuf 25:334–347

Conway R, Maxwell W, Morgan H (1972) On the implementation of security measures in information system. Commun ACM 15(4):211–220

Esam E, Ben A (2011) Secret sharing approaches for 3D object encryption. Expert Syst Appl 38:13906–13911

Han JH, Kim T, Cera CD et al (2003) Multi-resolution modeling in collaborative design. In: Proceedings of the eighteenth international symposium on computer and information Sciences, Antalya, Turkey

Hoppe H (1996) Progressive meshes. In: Proceedings of ACM SIGGRAPH

Huang Z, Liu GD, Ren Z et al (2009) A method of 3D data information encryption with virtual holography. In: Proceedings of SPIE-the international society for optical engineering 7125:71250E1–71250E7

Kim S, Lee K, Hong T, et a1 (2005). An integrated approach to realize multi-resolution of B-rep model. In: Proceedings of the 2005 ACM symposium on solid and physical modeling, Cambridge, Massachusetts

Lampson BW (1974) Protection. Oper Syst Rev 8(1):18–24

Lee JY, Lee JH, Kim H et al (2004) A cellular topology-based approach to generating progressive solid models from feature-centric models. Comput Aided Des 36(3):217–229

Lee SH (2005) A CAD-CAE integration approach using feature-based multi-resolution and multi-abstraction modelling techniques. Comput Aided Des 37(9):941–955

Lee SH, Kwon KR (2012) Robust 3D mesh model hashing based on feature object. Digit Signal Proc 22:744–759

Leong KK, Yu KM, Lee WB (2003) A security model for distributed product data management system. Comput Ind 50:179–193

Li S, Mirhosseini M (2012) A matrix-based modularization approach for supporting secure collaboration in parametric design. Comput Ind 63:619–631

Li WD, Cai YL, Lu WF (2007) A 3D simplification algorithm for distributed visualization. Comput Ind 58:211–226

Li WD and Mehnen J (2013) Cloud manufacturing. Springer series in advanced manufacturing, Springer

Naveen KN, Thomas JN (2011) Flexible optical encryption with multiple users and multiple security levels. Opt Commun 284:735–739

Oh S, Park S (2003) Task-role-based access control model. Inf Syst 28(6):533–562

Park J, Sandhu R (2004) The UCONABC usage control model. ACM Trans Inf Syst Secur 7 (1):128–174

Peng F, Lei YZ, Long M et al (2011) A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion. Comput Aided Des 43:1018–1024

Qiu ZM, Wong YS, Fuh JYH et al (2004) Geomelric model simplification for distributed CAD. Comput Aided Des 36(9):809–819

Rajput SK, Nishchal NK (2013) Known-plaintext attack on encryption domain independent optical asymmetric crypto system. Opt Commun 309:231–235

Rouibah K, Ould-Ali S (2007) Dynamic data sharing and security in a collaborative product definition management system. Robot Comput Integr Manuf 23:217–233

Rutledge LS, Hoffman LJ (1986) A survey of issues in computer network security. Comput Secur 4(5):296–308

Sandhu R, Coyne E, Feinstein H (1996) Role-based access control models. IEEE Comput 29 (2):38–47

Seo J, Song Y, Kim S et a1 (2005) Wrap-around operation for multi-resolution of B-Rep model. In: Proceedings of CAD'05

Speiera C, Whippleb JM, Clossc DJ et al (2011) Global supply chain design considerations: mitigating product safety and security risks. J Oper Manag 29:721–736

Stevens G, Wulf V (2002) A new dimension in access control: studying maintenance engineering across organizational boundaries

Su ZY, Li WQ, Kong JS et al (2013) Watermarking 3D CAPD models for topology verification. Comput Aided Des 45:1043–1052

Tang M, Lee M, Kim YJ (2009) Interactive Hausdorff distance computation for general polygonal models. ACM Trans Graph 28(3): Article 74

Tao H, Zain JM, Ahmed MM et al (2012) A wavelet-based particle swarm optimization algorithm for digital image watermarking. Integr Comput Aided Eng 1(19):81–91

Tirkel AZ, Rankin GA, vanSchyndel RM et al (1993) Electronic water mark, Sydeny, Macquarie University

van der Hoeven A, ten Bosch O, van Leuken R et al (1994) A flexible access control mechanism for CAD frameworks. In: Proceedings of the conference on European design automation. Los Alamito

Wang WB, Zheng GQ, Yong JH et al (2008) A numerically stable fragile watermarking scheme for authenticating 3D models. Comput Aided Des 40:634–645

Xiang H, Li M (2012) The research of network security mechanism based collaborative design. Adv Des Technol 421:406–409

Yao KH, Shao J, Sheng GQ et al (2007) Research on a security model of data in computer supported collaborative design integrated with PDM system. In: IITA 2007: workshop on intelligent information technology application

http://www.springer.com/978-3-319-50659-3

Cybersecurity for Industry 4.0
Analysis for Design and Manufacturing
Thames, L.; Schaefer, D. (Eds.)
2017, XIII, 265 p. 112 illus., 99 illus. in color., Hardcover
ISBN: 978-3-319-50659-3