Integrated Computer-Aided Engineering 22 (2015) 243–260
DOI 10.3233/ICA-150487
IOS Press

Encryption based partial sharing of CAD models

X.T. Cai[a], F.Z. He[a,*], W.D. Li[b], X.X. Li[b,c] and Y.Q. Wu[a]
[a]*School of Computer Science and Technology, Wuhan University, Wuhan, Hubei, China*
[b]*Faculty of Engineering and Computing, Coventry University, Coventry, UK*
[c]*College of Science, Huazhong Agricultural University, Wuhan, Hubei, China*

Abstract. Model security for collaborative product development in a networked environment (or called networked manufacturing, grid manufacturing, and cloud manufacturing) is an important and also challenging research issue. An encryption based partial sharing approach for CAD models has been developed and presented in this paper. First, a random invertible decimal matrix to support the encryption approach is proposed, with which parts of a CAD model can be selected flexibly by the model owner for encrypting by different keys; Second, in order to guarantee the security, a dual-key mode and a key based authorization mechanism are proposed. Based on the model, different levels of security are achieved based on different key spaces, and the key based authorization mechanism is used for the model owner to control the partial access of the CAD model flexibly.

Keywords: CAD, security, collaborative product development

1. Introduction

Collaborative product development (or CPD in the following) is the inevitable development trend [1,2]. In order to optimize design and manufacturing resources, enterprises have been increasingly developing their products within collaborative value chains in a networked environment. CPD can integrate various cross-regional and cross-enterprise superior resources smartly and dynamically [3,4]. For instance, using such a CPD approach, a product development task is decomposed into several sub-tasks by an OEM (Original Equipment Manufacturer), and the sub-tasks are carried out by different suppliers geographically located. Designers from different enterprises design the product by sharing the product model interactively.

A critical research challenge in CPD is how to ensure the security of CAD model sharing. Product design knowledge is the core-competitiveness of an enterprise, and the design data (e.g., CAD models) contain a lot of confidential information (such as design knowledge, design parameters and so on) reflecting the design intent, capacity and capability of the enterprise [5]. Therefore, direct sharing of CAD models during CPD without proper encryption has high risks as follows: (1) The confidential information of design may not be safely kept during the sharing of CAD models; (2) Another critical issue is that if a CAD model is shared to other designers, the reuse and further transmission may be uncontrollable; (3) The CAD model data may be captured by unauthorized users when it transformed in the network [6]. As thus, many enterprises are conservative to take the full potential of the Internet to implement CPD though there is a strong need there. As thus, it is imperative to improve the secure sharing of CAD models for CPD.

In CPD, CAD models may be shared frequently among the distributional users [7]. A typical collaboration scenario is as Fig. 1. *In the local site*, when a CAD model containing design information is shared, some parts of the CAD model should be protected in different security levels according to the access level of users in the design chain. First, if the part of CAD model is private to its designer, it should be hidden and

[*] Corresponding author: F.Z. He, School of Computer Science and Technology, Wuhan University, Wuhan, Hubei, China. E-mail: fzhe@whu.edu.cn.

ISSN 1069-2509/15/$35.00

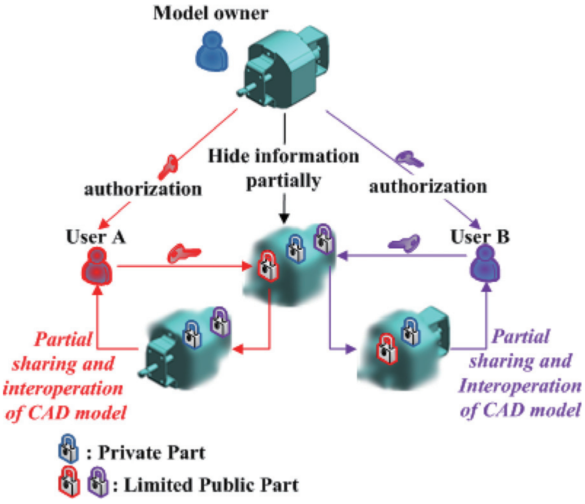

Model owner
Hide information partially
authorization
authorization
User A
User B
Partial sharing and interoperation of CAD model
Partial sharing and Interoperation of CAD model
: Private Part
: Limited Public Part

Fig. 1. A typical scenario of the secure sharing of CAD.

not shown to all the others (private part); Second, if a part of a CAD model is only shared to an authorized user, it should be hidden and can be set to be accessible by this user (limited public part); Third, if the part of a CAD model is public to each users, it needn't to be hidden (public part). *In the remote site*, according to the authorization from the CAD model owner, the related second kind of part is recovered, shared and interoperated. The first kind of parts and unauthorized second kind of parts are still hidden.

Based on the above observations, to ensure the security, there are three needs – partial protection of CAD models, different levels of security and flexible authorization mechanism for partial access of CAD models. Some research works have been presented for the secure sharing of CAD models to support CPD. However, there is yet no sound solution to meet the above requirement effectively. In this paper, an approach of encryption based partial sharing of CAD models is presented. The characteristics of this approach includes: (1) A random invertible decimal matrix for partial encryption of a CAD model is proposed. The sketches of the confidential parts are transformed randomly by a random invertible decimal matrix, and the confidential information can be hidden by the shape change related to this confidential part; (2) The encrypting key spaces for different security levels are different; (3) A dual-key mode is proposed for the generation of the encrypting keys, which can improve the security and provide a flexible authorization mechanism for partial access of CAD models.

The remainder of this article is organized as follows. Section 2 includes the related works about the secure sharing of design data in the CPD. Section 3 introduces the architecture for the encryption based partial sharing of CAD models. Section 4 explains the random invertible decimal matrix for the partial encryption method. Section 5 presents the dual-key model for the partial encryption. Section 6 shows a case study, and some conclusions and comparisons are made in Section 7.

2. Related work

The Internet provides convenience for the information sharing, but simultaneously, also brings the security-risks during sharing. Security-risks have been becoming barriers to implement CPD 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: a unauthorized user cannot access the confidential information; (2) Information authentication: the information has a verification capacity which can ensure the information has not been changed [8]. Various research works about the secure sharing of CAD models have been developed according to the above two requirements [9], and the main approaches can by classified in Table 1. More technical details are expanded below.

2.1. Watermark

The "watermark" concept was first proposed by Tirkel [10]. The digital watermarking technology is used for the intellectual property protection and the integrity authentication of the electronic files. The creation information and logo of a creator are embedded in an electronic file in the form of unaware watermark which cannot be removed during sharing, and the watermark can be detected by a special software package [11,12]. Various watermarking methods were developed for the intellectual property protection of 2D/3D CAD models [13–23]. However, in a CPD environment, CAD models are needed to be shared safely, and watermark is not appropriate for sharing design information (design knowledge, parameters and so on) in a secure means. As thus, the design information can still be obtained by other users and a CAD model can be recreated without the watermark relatively easily.

2.2. Access control

Access control is an important security method in a networked environment, the access of the special re-

Table 1
Security method in the collaborative product development

Security method	Security requirements				Characteristics	
	A	B	C	D	Purpose	Problems
Watermark	√			√	Protect the intellectual property by embedding the watermark in CAD models	The design information (design knowledge, parameters and so on) cannot be hidden by watermark in a safe way.
Access control		√	√		Control the access of the design data (e.g., CAD models) by a user's authorization according to a group of access control rules	Unable to support the partial information protection of a CAD model
Multi-level data sharing based on the multi-resolution approach		√		√	The main purpose of the multi-resolution approach is to simplify a CAD model during the data sharing in a network with limited bandwidth. Few research works used the approach to hide the design information for CPD	It can realize the secure sharing of the partial CAD model to some degrees, but not flexibly
Encryption of CAD models		√		√	Hide the design information by the encryption technology	No research about the encryption of CAD models

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

source in the networked environment is controlled by a user's 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, and later the access control became an important approach for information protection in networked environments [24]. Conway used the concept of secure matrix for access control, and standardized the secure matrix and finally presented the theory of discretionary access control [25]. Later, many access control approaches were developed. Based on the experience of the former research, Sandhu proposed a role based access control approach (RBAC96) [26]. Task-role-based Access Control was proposed by OH [27], and Usage Control called the next generation of access control model was presented [28,29].

The access control approaches of files for CPD. In order to support CPD, many special access control approaches were developed. van der Hoeven proposed an access control based CAD architecture [30], but the access control is still file based. Stevens developed an ADOSX system which can handle CPD between two enterprises, while the system just focuses on the access control of files [31]. Cera developed a secure access control mechanism for 3D models [32], but the method mainly supports the collaborative view of product models not the full-scale collaborative design. Leong devised a security approach for a distributed product data management system, which combines the Lampson's access matrix and Bell and LaPadula's security labels, and it is still file based [33].

The sharing space based access control approaches for CPD. Considering the frequent sharing of design data, sharing space based access control methods were proposed, in which a secure sharing space was designed. Bullock developed a space approach for the 2D/3D collaborative environment [34]. Kamel presented a dynamic data sharing and security approach for CPD [35], and Chang developed the security system for sharing engineering drawings in the sharing space [36].

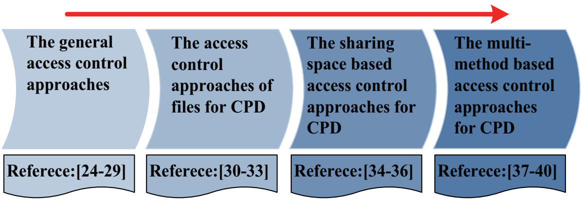

The general access control approaches
The access control approaches of files for CPD
The sharing space based access control approaches for CPD
The multi-method based access control approaches for CPD
Referece:[24-29]
Referece:[30-33]
Referece:[34-36]
Referece:[37-40]

Fig. 2. The evolvement process of the access control method for the collaborative product development environment.

The multi-method based access control methods for CPD. In order to improve the security of CPD, multi-method based access control methods were proposed, and some other security methods are combined with the access control to ensure better security. Yao devised a security model of data for collaborative design and management system combining multi security methods with the access control [37]. Chang developed a security system for sharing CAD drawings which used a multi-method approach [38]. Speiera also used a multi-method approach to mitigate product safety and security risks [39]. Hao defined a network security mechanism for the collaborative combined VPN (Virtual Private Network) and access control [40].

The access control method constructs a secure CPD environment based on the architecture-level, and the evolvement process is shown in Fig. 2. Unfortunately, all the existed general and special access control approaches used in CPD are file based, and they cannot handle the case that the CAD model contains both confidential information and sharing information.

2.3. Multi-level design data sharing based on the multi-resolution models

The multi-resolution model can be used for the secure sharing of partial CAD models. The multi-resolution model is an important information simplification and hidden approach.

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 [41]. Han proposed a multi-resolution modeling approach of CAD models to support collaborative design [42], Qiu designed a T-Curve based simplification method for CAD models [43], and Li present a 3D simplification algorithm for distributed visualization [44]. All of the methods are mesh model based. However, a mesh model lacks design information (history, features, parameters and so on) to support interoperation in CPD.

Multi-resolution B-rep, solid and feature modeling. Belaziz provided an analysis tool of a B-rep model, which can delete some features without any complex Boolean operations [45]. Seo proposed a B-rep based multi-resolution modeling method based on the Wrap-Around [46]; Kim integrated Wrap-Around, Smooth-Out and Thinning to develop a new B-rep based multi-resolution modeling method [47]. Lee designed the Progressive Solid Model (PSM) to support the multi-resolution solid model [48]. Lee developed a feature based multi-resolution modeling method [49,50], which is based on the calculation of the "valid volume".

Combination of the multi-resolution feature model and the access control. Cera combined the multi-resolution modeling and access control to realize the access control of multi-level CAD model [51,52]; Chu focused on multi-level data sharing based on the multi-LOD (Level of Detail) models in CPD [53,54]. Li proposed a matrix-based modularization approach for supporting secure collaboration in parametric design [55].

The multi-level design data sharing based on the multi-resolution models can realize the secure sharing of a partial CAD model in some degrees, and its evolvement process is as Fig. 3. However, this method is not flexibly enough due to the following limitations: 1) The information hidden is in a total mode; 2) The hidden information cannot be selected by the model owner; 3) The approaches cannot support interoperation freely because the sharing model is not complete.

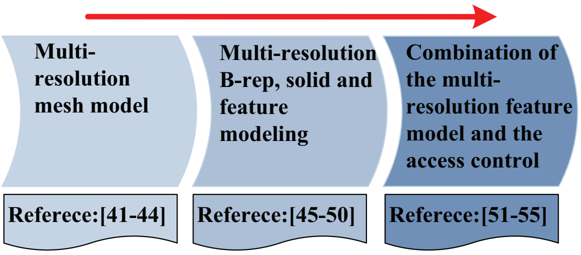

Multi-resolution mesh model
Multi-resolution B-rep, solid and feature modeling
Combination of the multi-resolution feature model and the access control
Referece:[41-44]
Referece:[45-50]
Referece:[51-55]

Fig. 3. The evolvement process of the multi-level design data sharing based on the multi-resolution models.

2.4. Data encryption

Data encryption is an important approach for the information hidden in the network. It can ensure that the hidden information cannot be obtained by unauthorized users [56,57]. 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 proposed a method of encrypting 3D data information with virtual holography [58]. Esam proposed secured sharing approaches for 3D mesh model encryption [59]. Naveen developed an encryption based multi-level data access control for the partial data sharing of the images in the collaborative environment [60] On the other hand, until now, there are few research works about the encryption of CAD models.

2.5. Summary of the related work

As discussed earlier, the requirements for sharing CAD models are complex. Based on the above discussion, the existing research works for the secure sharing of design data have following main shortages: 1) Lack of flexible partial protection mechanisms; 2) Lack of the different levels of security; 3) Lack of flexible authorization mechanisms for partial access of CAD models.

3. The architecture for the encryption based secure sharing of the CAD model

A novel approach of encryption based partial sharing for CAD models is presented in this paper. The innovations of the approach include: 1) Partial encryp-

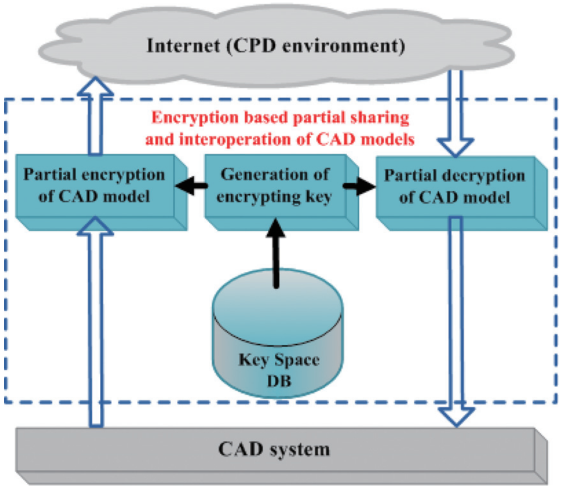

Internet (CPD environment)
Encryption based partial sharing and interoperation of CAD models
Partial encryption of CAD model
Generation of encrypting key
Partial decryption of CAD model
Key Space DB
CAD system

Fig. 4. The architecture for the encryption based secure sharing of the CAD model.

tion for CAD models, which means that the encrypted parts are decided by a model owner; 2) Different levels of security, i.e., three security levels are proposed and different key spaces are generated for different security levels. 3) Key based authorization mechanism for partial access of CAD models, with which the CAD model owner can authorize other users to access related parts of a CAD model by encrypting keys.

The architecture for the developed approach is shown as Fig. 4. The kernel of the architecture contains four main components: 1) Partial encryption; 2) Partial decryption; 3) Generation of encrypting keys; 4) Key space Database (DB). In CPD, two types of CAD models are defined as follows.

Definition 1. *Local CAD Model.* The CAD model is owned in a local site.

Definition 2. *Remote CAD Model.* The CAD model is received from a remote site.

3.1. Partial encryption

This component is used to encrypt a CAD model partially according to the intention of the model owner. In a local site, before a CAD model is shared, some parts should be partially encrypted to protect the confidential information.

In CPD, the partial secure demand of a CAD model contains the following three cases: 1) The part of a CAD model is private, which can't be shared by the others; 2) The part of a CAD model can be shared by the authorized users; 3) The part of a CAD model is public, which can be shared by all the others. According to the secure demand, three security levels are defined as follow:

Definition 3. *Security levels*

(1) *Private Level.* The *Private Part* of a CAD model is closed to all the other users.
(2) *Limited Public Level.* The *Limited Public Part* of a CAD model is only shared with the authorized users but inaccessible to other unauthorized users.
(3) *Public Level.* The *Public Part* of a CAD mode is public to all the others.

The Private Part and the Limited Public Part should be determined by the model owner. Different Levels are encrypted hierarchically by keys from different key spaces and different parts of the same level are encrypted by different keys from the same key space. The encrypted CAD model would be sent to the users who would share the model, and the related key which is sent with the encrypted CAD model is the authorization to share the related part of the CAD model.

3.2. Partial decryption

This component is used to decrypt the shared parts of the CAD model. In the remote site, when a shared CAD model is received, it is decrypted partially according to the authorization from the model owner.

3.3. Key space DB

The key space DB stores two key spaces which are matrixes and used to generate the encrypting key. According to the security levels, the two key spaces are given as follows.

Definition 4. *Private Key Space*. It is used to generate the encrypting key for the encryption of the Private Part

Definition 5. *Public Key Space*. It is used to generate the encrypting key for the encryption of the Limited Public Part.

3.4. Generation of encrypting key

This component is used to generate the encrypting key. According to the key spaces, two types of keys are defined as follows.

Definition 6. *Private Key*. The key is used to encrypt the Private Part.

Definition 7. *Public Key*. The key is used to encrypt the Limited Public Part.

4. Random invertible decimal matrix based partial encryption method of the CAD model

According to the fundamental principle of the cryptology, the goal of the cryptology is to prevent the information leakage in the information dissemination. The initial information (plain-text) is transformed to a group of special signs (encryption) which should not be understood by the unauthorized users following some designated rules, and the transformed signs (cipher-text) can just be recovered by the authorized persons (decryption). The authorization means the user gets the decrypting information (key) legally [56,57]. Nowadays, most of the CAD systems are feature based. As thus, for a CAD model, the partial shape and features contain abundant design knowledge (design semantic, design parameters, etc.) which is confidential to the competitors. Therefore, the partial shape and features are the plaintext of a CAD model needed to be encrypted.

A CAD model is made up of various features in a certain order and structure. The features can be classified according their sketches as follows: The first kind of feature is created based on one or more sketches, and the sketches decide the shape of the feature and finally affect the partial shape of the CAD model directly, such as the extrusion, sweep and so on; The second kind of feature is created without any sketch, and this kind of feature is always dependent on the other features, so its shape is affected by the sketches of the other features indirectly, such as a chamfer, draft and so on. As thus, the encryption of sketches can change the shape and features of CAD models, and the confidential information (such as design parameters, semantics and knowledge) of the CAD model can be hidden effectively.

4.1. Encryption of sketch

A sketch is composed by sketch elements (such as line, arc, curve and so on) and constraint elements (such as two parallel lines, a fixed vertex and so on). Therefore, the sketch (S) can be represented as Formula (1)

$$S = \bigcup_{i=1}^{m} e_i \cup \bigcup_{j=1}^{n} c_j \tag{1}$$

e_i denotes a sketch element of S, and c_j denotes a constraint element of S.

The sketch elements contain the design parameters and decide the shape of the sketch, the encryption of the sketch can be achieved by the transformation of the sketch elements, and the sketch elements are the plaintext in the encryption of sketch. Since a constraint limits the change of sketch element but does not decide the shape of the sketch, in order to transform the sketch, the constraint elements should be moved. The sketch without constraint elements can be described as Formula (2)

$$S' = S - \bigcup_{j=1}^{n} c_j = \bigcup_{i=1}^{m} e_i \tag{2}$$

The shape and parameters of S' is the same to those of S. For the encryption of S', the plaintext is $\bigcup_{i=1}^{m} e_i$.

It is known that the sketch elements can be changed by a transition matrix. The encryption of S' can be describe as Formula (3)

$$S'_{\textit{encrypted}} = \bigcup_{i=1}^{m} (e_i \times A) = \bigcup_{i=1}^{m} e'_i \tag{3}$$

A is the transition matrix, and $\bigcup_{i=1}^{m} e'_i$ is the cipher-text of S'.

Finally, the encryption of S is as Formula (4)

$$\begin{aligned} S_{\textit{encrypted}} &= \left\{ S'_{\textit{encrypted}}, \bigcup_{j=1}^{n} c_j \right\} \\ &= \left\{ \bigcup_{i=1}^{m} (e_i \times A), \bigcup_{j=1}^{n} c_j \right\} \end{aligned} \tag{4}$$

A random invertible matrix is given as the transition matrix. Since the matrix is invertible, the cipher-text can be recovered by the inverse matrix of the transition matrix directly. On the other hand, considering the invertible matrix is random, it is difficult to be cracked. At last, in order to improve the randomness of the matrix and limit the position change of the sketch, the values of the elements in A are in the $(-1, 0) \cup (0, 1)$. The transition matrix (A) is defined as follow.

Definition 9. *Transition matrix A*

(1) $A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$;

(2) $|A| \neq 0, \{a_{ij} | a_{ij} \in (-1, 0) \cup (0, 1),\ i \in [1, 3],\ j \in [1, 3]\}$

The encryption algorithm of a sketch is detailed as Algorithm 1.

Algorithm 1. Random invertible decimal matrix based encryption algorithm of sketch: Sketch_Encryption (s, A)

```
Input:
 1. The sketch $S$
 2. The encrypting random invertible decimal matrix
    is $A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$
Function:
1.  Retrieve the element set of $S$: $E\_set\{e_i\}_1^n$
2.  Retrieve the constraint set of $S$: $C\_set\{c_j\}_1^m$
3.  Record the $C\_set\{c_j\}_1^m$ in the auxiliary file
4.  for (int $j = 0; j < n; j++$)
    {
5.    get the coordinate set of $e_i$: $Co\_set\{co_k\}_1^m$
6.    for (int $s = 0; s < m; s++$)
      {
7.      if $co_{s+1}$ is in a 3D coordination system
8.      $\{co'_{s+1} = co_{s+1} \times A$
        $= (x_{(s+1)}, y_{(s+1)}, z_{(s+1)}) \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$
        }
9.      else if $co_{s+1}$ is in a 2D coordination system
10.     $\{(co'_{s+1}, z_{s+1}) = (co_{s+1}, 1) \times A =$
        $(x_{(s+1)}, y_{(s+1)}, 1) \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$
        }
      }
11.   get the new coordination set of $e_i$:
      $Co\_set'\{co'_k\}_1^m$
12.   create the new element $e'_i$ by $Co\_set'\{co'_k\}_1^m$
    }
13. get the new element set of $S$: $E\_set'\{e'_i\}_1^n$
14. Create the encrypted sketch $S'$ by the
    $E\_set'\{e'_i\}_1^n$
15. Return $(S')$
```

An example shown in Fig. 5 is used to illustrate the above algorithm. The CAD model contains a sweep feature (F), and F contains two sketches $\{S_1, S_2\}$, in which S_1 is a 2D sketch and S_2 is a 3D sketch. Figure 5(a) is the initial CAD model, Fig. 5(b) is the initial S_1 and Fig. 5(c) is the initial S_2.

The sketch element set ($E_1\_set\{\}$) and the constraint set ($C_1\_set\{\}$) of S_1 are as follow:

$$E_1\_set\{e_i\}_1^4 =$$
$$\{(line1, (-27, 30), (-35, 20)), (line2, (27, 30), (35, 20)), (arc1, (0, 20), (35, 20), (-35, 20)) (B\_spline\_curve1, (-27, 30), (-22, 40), (-35, 45), (0, 80), (35, 45), (22, 40), (27, 30))\}$$
$$C_1\_set\{c_i\}_1^6 =$$
$$\{(P2, fixed), (P4, fixed), (P6, fixed), (P7, fixed), (P12, fixed), (P13, fixed)\}$$

The sketch element set ($E_2\_set\{\}$) and the constraint set ($C_2\_set\{\}$) of S_2 are as follow:

$$E_2\_set\{e_i\}_1^1 =$$
$$\{(3D\_curve, (0, 0, 0), (10, 10, 10), (30, 40, 50), (90, 100, 200))\}$$
$$C_2\_set\{\} = NULL$$

A random invertible decimal matrix is given as follow:

$$A = \begin{bmatrix} 0.931 & 0.874 & 0.936 \\ 0.254 & 0.539 & 0.172 \\ 0.673 & 0.511 & 0.902 \end{bmatrix}$$

According to the random matrix based encryption algorithm, S_1 is encrypted as Fig. 5(e) and the S_2 is encrypted as Figs 5(f) and (d) show the final encrypted CAD model.

The decryption is the inverse process of the random invertible decimal matrix based encryption. The detail of the decryption algorithm of sketch is as Algorithm 2.

4.2. Partial encryption algorithm of CAD models

The CAD model is composed by a group of features, and it can be represented as the Formula (5).

$$M = \bigcup_{i=1}^{n} F_i \tag{5}$$

The M denotes a CAD model, F_i is the ith feature of M. A feature is generated by the related sketches and parameters in a certain modeling rule. M can be described as the Formula (6).

$$M = \bigcup_{i=1}^{n} F_i = \bigcup_{i=1}^{n} \left(\bigcup_{j=1}^{m_i} S_{ij} \otimes \bigcup_{k=1}^{s_i} P_{ik} \right) \tag{6}$$

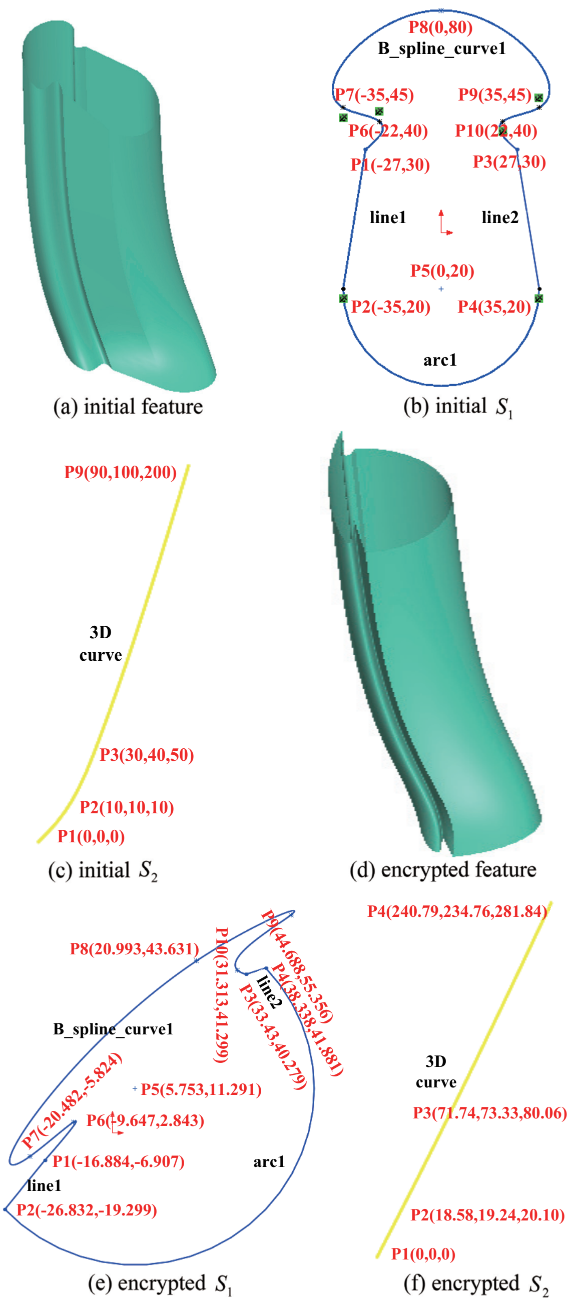
Algorithm 2. Decryption algorithm of sketch: Sketch_Decryption (S', A)

```
Input:
1. The encrypted sketch $S'$
2. The encrypting random invertible decimal matrix is
   $A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$
Function:
 1. Retrieve the element set of $S'$: $E\_set'\{e'_i\}_1^n$
 2. for (int $j = 0; j < n; j++$)
    {
 3.     get the coordination set of $e'_i$: $Co\_set'\{co'_k\}_1^m$
 4.     for (int $s = 0; s < m; s++$)
        {
 5.         if $co'_{s+1}$ is in a 3D coordination system
 6.         { calculate the inverse matrix of $A$: $A^{-1} = \frac{1}{|A|}\begin{bmatrix} a_{22}a_{33}-a_{23}a_{32} & a_{13}a_{32}-a_{12}a_{33} & a_{12}a_{23}-a_{13}a_{22} \\ a_{23}a_{31}-a_{21}a_{33} & a_{11}a_{33}-a_{13}a_{31} & a_{13}a_{21}-a_{11}a_{23} \\ a_{21}a_{32}-a_{22}a_{31} & a_{12}a_{31}-a_{11}a_{32} & a_{11}a_{22}-a_{12}a_{21} \end{bmatrix}$
 7. $co_{s+1} = co'_{s+1} \times A^{-1} = (x'_{(s+1)}, y'_{(s+1)}, z'_{(s+1)}) \times A^{-1}\}$
 8.         else if $co'_{s+1}$ is in a 2D coordination system
 9.         $\{co_{s+1} = ((x'_{(s+1)} - a_{31}), (y'_{(s+1)} - a_{32})) \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} \frac{1}{(a_{11}a_{22} - a_{21}a_{12})}$
            }
        }
10.     Recover the coordinate set of $e_i$: $Co\_set\{co_k\}_1^m$
11.     Recover the element $e_i$ by $Co\_set\{co_k\}_1^m$
    }
12. Recover the element set of $S$: $E\_set\{e_i\}_1^n$
13. Get the constraint set of $S$: $C\_set\{c_j\}_1^m$ from the auxiliary file
14. Recover the encrypted sketch $S$ by the $E\_set\{e_i\}_1^n$
15. Return $(S)$
```

S_{ij} denotes the j_{th} sketch of F_i, P_{ik} denotes the k_{th} parameter of F_i, and '$\otimes$' denotes the modeling rules.

For the CAD model (M), $\{F_i\}_1^n$ denotes its feature set, and a part of M can be described as $\{F_i\}_j^k, (1 \leqslant j \leqslant k \leqslant n)$. The CAD model can be also represented as the Formula (7).

$$M = \bigcup_{i=1}^{n} F_i = \left(\bigcup_{i=1}^{j-1} F_i\right)\left(\bigcup_{i=j}^{k} F_i\right)\left(\bigcup_{i=k+1}^{n} F_i\right) \tag{7}$$



(a) initial feature

(b) initial S_1

(c) initial S_2

(d) encrypted feature

(e) encrypted S_1

(f) encrypted S_2

Fig. 5. Example for the encryption of the sketch.

According to the Formulas (4), (6) and (7), the partial encryption algorithm of a CAD model can be represented as the Formula (8)

$$M_{partial\_encrypted} = \left\{\left(\bigcup_{i=1}^{g-1} F_i\right)\left(\bigcup_{i=g}^{s}\left(\bigcup_{j=1}^{m_i}\left(\bigcup_{s=1}^{u_{ij}}(e_{ijs} \times A)\right.\right.\right.\right.$$

$$\otimes \bigcup_{k=1}^{s_i} P_{ik} \Bigg)\Bigg)\Bigg(\bigcup_{i=s+1}^{n} F_i \Bigg),$$

$$\bigcup_{i=g}^{s}\Bigg(\bigcup_{j=1}^{m_i}\Bigg(\bigcup_{r=1}^{w_{ij}} c_{ijr}\Bigg)\Bigg)\Bigg\} \qquad (8)$$

According to the Formula (8), the result of the partial encryption of the CAD model contains two parts,

$$\Bigg(\bigcup_{i=1}^{g-1} F_i\Bigg)\Bigg(\bigcup_{i=g}^{s}\Bigg(\bigcup_{j=1}^{m_i}\Bigg(\bigcup_{s=1}^{u_{ij}}(e_{ijs}\times A)$$

$$\otimes \bigcup_{k=1}^{s_i} P_{ik}\Bigg)\Bigg)\Bigg(\bigcup_{i=s+1}^{n} F_i\Bigg)$$

means the final encrypted CAD model, and

$$\bigcup_{i=g}^{s}\Bigg(\bigcup_{j=1}^{m_i}\Bigg(\bigcup_{r=1}^{w_{ij}} c_{ijr}\Bigg)\Bigg)$$

means all the initial constraints of a CAD model. When a CAD model is encrypted, all the initial constraints of the CAD model have been stored independently for the recovery of the CAD model.

4.2.1. *Encryption and decryption of single feature*

The encryption of the single feature is the basis of the partial encryption of a CAD model, and the detail encryption algorithm and decryption algorithm are as follows.

Algorithm 3. Encryption algorithm of feature: Feature_Encryption (F)

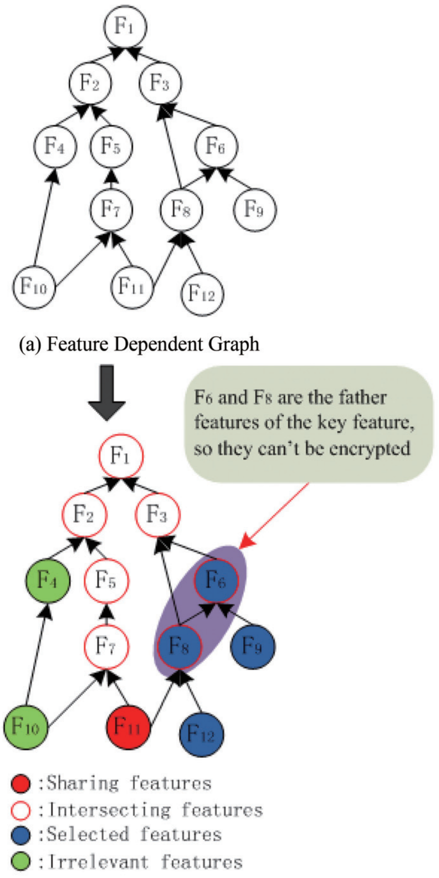
```
Input:
1. The initial feature: $F$
2. The encrypting matrix: $A$
Function:
1. Retrieve the type of the initial feature: $F$
2. Retrieve the sketch set: $S\_set\{s_i\}_1^n$
3. for (int $j = 0; j < n; j++$)
   {
4.    Record the constraint information of $s_i$ in the
      auxiliary file
5.    $s_i'$ = Sketch_Encryption ( $s_i$ , $A$ )
   }
6. Get the encrypted sketch set $S'\_set\{s_i'\}_1^n$
7. Recreate the feature base on the $S'\_set\{s_i'\}_1^n$: $F'$
8. Return ($F'$)
```

Algorithm 4. Decryption algorithm of feature: Feature_Decryption (F')

```
Input:
1. The encrypted feature: $F'$
2. The encrypting matrix: $A$
Function:
1. Retrieve the type of the encrypted feature: $F'$
2. Retrieve the sketch set: $S'\_set\{s_i'\}_1^n$
3. for (int $j = 0; j < n; j++$)
   {
4.    $s_i$ = Sketch_Decryption ($s_i'$, $A$)
5.    Get the constraint information of $s_i$ from
      auxiliary file and add it to the $s_i$
   }
6. Get the decrypted sketch set $S\_set\{s_i\}_1^n$
7. Recover the initial feature base on the
   $S\_set\{s_i\}_1^n$: $F$
8. Return ($F$)
```

Algorithm 5. Screening algorithm of the encrypting features: Screening ($F\_set_{select}\{\}$, $F\_set_{share}\{\}$)

```
Input:
1. Select the encrypting features interactively:
   $F\_set_{select} = \{f\_select_i\}_1^n$
2. Select the sharing features interactively:
   $F\_set_{share} = \{f\_share_j\}_1^m$
Function:
1. Create the Feature Dependent Graph (FDG) of
   $M$
2. The intersecting feature set which can not be en-
   crypted: $F\_set_{intersect} = NULL$
3. The final feature set which can be encrypted:
   $F\_set_{screen} = NULL$
4. for (int $k = 0; K < m; K++$)
   {
5.    for the feature $F$ whose id is $f\_share_k$, re-
   trieve
      the ids of $F$'s parent features
6.    add the ids in to $F\_set_{intersect}\{\}$
   }
7. for (int $p = 0; p < n; p++$)
   {
8.    if $f\_select_p \in F\_set_{intersect}\{\}$, delete
      $f\_select_p$ from $\{f\_select_i\}_1^n$
9.    $n--$
   }
10. $F\_set_{screen} = F\_set_{select}$
11. Return ($F\_set_{screen}$)
```



(a) Feature Dependent Graph

F6 and F8 are the father features of the key feature, so they can't be encrypted

(b) Classification of features

Fig. 6. The example for the selection of the encrypted features.

4.2.2. *Screening algorithm of the encrypting features*

According to the intention of the CAD model owner, all the features selected should be encrypted. However, sometimes, direct encryption of the selected features may lead to the sharing failure of the other parts, because some selected features may be the parent of the features in the sharing part and the encrypting transformation of the parent features may lead to the shape and position change of the features in a sharing part. In order to ensure the sharing of the other parts without affection, the selected features should be screened.

For the CAD model (M), according to the dependent relation of the features in M, a Feature Dependent Graph (FDG) can be created (as Fig. 6(a)). Based on the selected features, sharing features and dependent relations, the features of M can be classified into four parts as follows.

- *Selected feature:* The features which are selected as candidate encrypted features.
- *Sharing feature:* The features which are needed to be shared by the other users.
- *Intersecting feature:* The feature is a Selected Feature, meanwhile, it is also a Sharing Feature or the parent of some Sharing Features.
- *Irrelevant features:* The features excluded from the above three types

In order to maintain the sharing part for other users, the intersecting features should be excluded from the feature set needed to be encrypted. As Fig. 6(b), the purple shadow region shows the intersection features, meaning the F6 and F8 can not be encrypted. The screening algorithm of the encryption features is as Algorithm 5.

4.2.3. *Partial encryption of the CAD model*

Because of the dependent relations, the later features may be influenced by the encrypting transformation of the former features. The encrypting order must be from a later feature to the former feature. Based on the Formula (8) and the above algorithms, the partial encryption algorithm of the CAD model is detailed as Algorithm 6.

Algorithm 6. Encryption algorithm of partial CAD model: Partial_Encryption (M)

```
Input:
The initial CAD model: $M$
Function:
Add the basic information into the auxiliary file
Generate the encrypting key: $K =$
    Key_Generation() //described in the next section
$A_{3\times3}$ = Matrix_Generation($K$) //described in the next section
$F\_set_{screen}\{\} =$
    Screening ($F\_set_{select}\{\}, F\_set_{share}\{\}$)
Arrange the $F\_set_{screen}\{\}$ according to the creating order of features from the former to latter in the feature tree and get the new partial order encrypting feature set $F\_set_{encrypt}\{\} = \{f\_encrypt_i\}_1^n$
for (int $q = n; q > 1; q - -$)
{
    Add the feature id into the XML
    Feature_Encryption ( $f\_encrypt_q$ )
} //Generate the encrypted CAD model: $M'$
Add the $K$ into auxiliary file
Return $(M')$
```

For the same reason, when decrypting the CAD model, the decrypting order is converse to the encrypting order. The partial decrypting algorithm is as Algorithm 7.

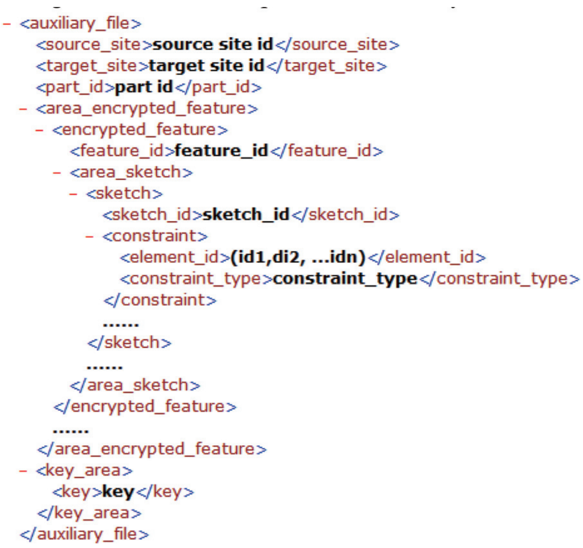
```
Algorithm 7. Decryption algorithm of partial CAD model: Partial_Decryption ($M'$)
Input:
1. The encrypted CAD model: $M'$
Function:
1. Get the basic information from the auxiliary file
2. Get the encrypting key: $K$
3. $A_{3\times 3}$ = Matrix_Generation($K$) (described in the next section)
4. Get the encrypting feature set $F_{select\_set} = \{f\_select_i\}_1^n$ from the auxiliary file
5. Arrange the $F_{select\_set} = \{f\_select_i\}_1^n$ according to the creation order of features from the former to latter in the feature tree and get the new partial order encrypting feature set $F_{decrypt\_set}\{\} = \{f\_decrypt_i\}_1^n$
6. for (int $q = 1; q < n; q++$)
   {
      Feature_Decryption ($f\_encrypt_q$)
   } //Generate the decrypted CAD model: $M$
7. Return ($M$)
```

4.2.4. *Auxiliary file*

For the partial encryption of a CAD model, some important information should be stored independently. The information is recorded in an auxiliary file (in this paper, a XML file is used as the auxiliary file). The auxiliary file includes the following three kinds of information.

(1) *Basic information:* The IDs of source site and the target site
(2) *Encrypting information:* The IDs of the encrypted features and the constraints of the sketches in the encrypted features.
(3) *Encrypting Key:* The Key for this encrypted model

Figure 7 shows the example of the auxiliary file.



```
- <auxiliary_file>
    <source_site>source site id</source_site>
    <target_site>target site id</target_site>
    <part_id>part id</part_id>
  - <area_encrypted_feature>
    - <encrypted_feature>
        <feature_id>feature_id</feature_id>
      - <area_sketch>
        - <sketch>
            <sketch_id>sketch_id</sketch_id>
          - <constraint>
              <element_id>(id1,di2, ...idn)</element_id>
              <constraint_type>constraint_type</constraint_type>
            </constraint>
            ......
          </sketch>
          ......
        </area_sketch>
      </encrypted_feature>
      ......
    </area_encrypted_feature>
  - <key_area>
      <key>key</key>
    </key_area>
  </auxiliary_file>
```

Fig. 7. The example of the auxiliary file.

4.2.5. *Time complexity of encryption/decryption*

According to the algorithms of sketch encryption/decryption, if a sketch contains n points, the coordinate transformation is executed for n times in the sketch encryption/decryption, so that the time complexity of the sketch encryption/decryption is O(n).

Because the encryption/decryption of CAD models is based on the encryption/decryption of its sketches, if a CAD model contains m sketches, the sketch encryption/decryption is executed for m times. As thus, for the encryption/decryption of CAD models, its time complexity is O(n^2).

5. Generation of the encryption key

5.1. *Dual-key mode*

According to the security principle in the encryption based communication system, in order to prevent cryptanalysis, it needs: 1) The encryption is at least secure in computation; 2) The security of the information relies on the security of the key; 3) The encryption algorithm fits all the elements in the key space. Based on the security principle, a dual-key mode is proposed. The dual-key is made up of the key space and the encrypting key, the encrypting random invertible decimal matrix is generated by the encrypting key space and the key. The Key Space is defined as follow.

Definition 10. *Key Space* (KS)

(1) $KS = M_{n\times n} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & \vdots \\ a_{31} & a_{32} & a_{33} & & \vdots \\ \vdots & & & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & \cdots & a_{nn} \end{bmatrix}$

(2) $n > 3, \{a_{ij} | a_{ij} \in (-1,0) \cup (0,1), i \in [1,n], j \in [1,n]$

(3) For any two elements of $M_{n\times n}$: (a_{ij}, a_{pq}), if $(i \neq p \cup j \neq q)$, then $(a_{ij} \neq a_{pq})$

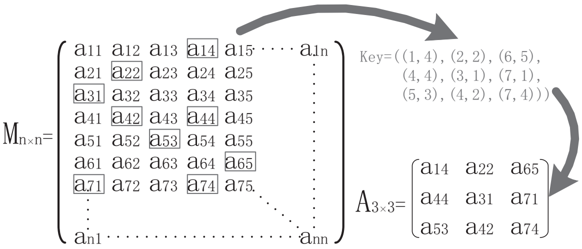


Fig. 8. Generation of random invertible decimal matrix.

If a CPD task is initiated, a Public Key Space is generated: KS_{public}. When a new user is added in the task, the KS_{public} is backup locally, and at the same time a Private Key Space is generated locally: $KS_{private}$.

Before the encryption, the encrypting key is generated from the key space, which is defined as follow.

Definition 11. *Encrypting Key* (K)

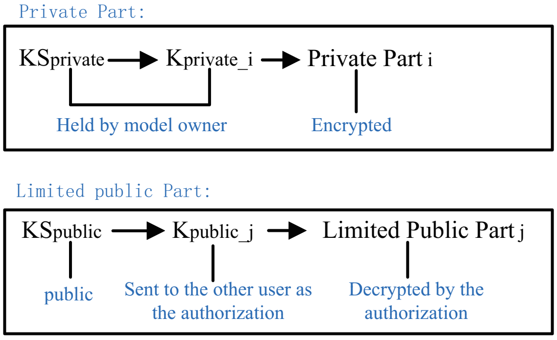
(1) $K = \{(k_{i1}, k_{i2})|(k_{i1} \in [1, n], k_{i2} \in [1, n])\}_1^9$

(2) if $(((k_{i1}, k_{i2}) \in K) \cup ((k_{j1}, k_{j2}) \in K) \cup (i \neq j))$, then $((k_{i1}, k_{i2}) \neq (k_{j1}, k_{j2}))$

(3) $$f\left(A_{3\times 3} = \begin{bmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ b_7 & b_8 & b_9 \end{bmatrix} \cup (b_i = a_{(k_{i1},k_{i2})} inKS)\right), \text{ then } (|A_{3\times 3}| \neq 0)$$

Based on the KS and K, the final random invertible decimal matrix can be generated. The generation algorithms of the encrypting key and matrix are as the Algorithm 8 and Algorithm 9. And the Fig. 8 shows the generation process of the encrypting key and matrix.

```
Algorithm 8. Key generation algorithm:
Key_Generation()
Function:
If the part of the CAD model is private
{ Get the $KS_{private}$;
    Generate the $K_{private}$ according to the definition
    of the Encrypting Key
}
Else
{ Get the $KS_{public}$;
    Generate the $K_{public}$ according to the definition
    of the Encrypting Key
}
Return the Encrypting Key: $K$
```


Private Part:

KSprivate → Kprivate_i → Private Part i

Held by model owner

Encrypted

Limited public Part:

KSpublic → Kpublic_j → Limited Public Part j

public

Sent to the other user as the authorization

Decrypted by the authorization

Fig. 9. Key based authorization mechanism.

```
Algorithm 9. Generation algorithm of encrypting matrix: Matrix_Generation($K$)
Input:
1. The encrypting key: $K$
Function:
If the CAD model is local model and the decrypted part is Private Part
{
    Get the local $KS_{private}$
    Generate the encrypting matrix according the
    $K$ and $KS_{private}$
}
Else
{
    Get the $KS_{public}$
    Generate the encrypting matrix according the
$K$
    and $KS_{private}$
}
Return the encrypting matrix: $A$
```

5.2. *Different levels of security*

According to the security levels defined above, when a CAD model is partially encrypted, the related key space is selected to generate the encrypting key according to the security level of the related part.

5.3. *Key based authorization mechanism*

In order to control the access of the protected parts flexibly, a key based authorization mechanism is proposed as Fig. 9.

Before a CAD model is shared, the Private Parts and Limited Public Parts are selected by the model owner, and every part is encrypted by different keys. (1) For the Private Parts, they cannot be decrypted by any other

Table 2
Key spaces for different security levels

Security level	Protected part	Key space	Key
Private level	Private part	Private key space	Private key
Limited public level	Limited public part	Public key space	Public key
Public level	Public part	No key space	No key

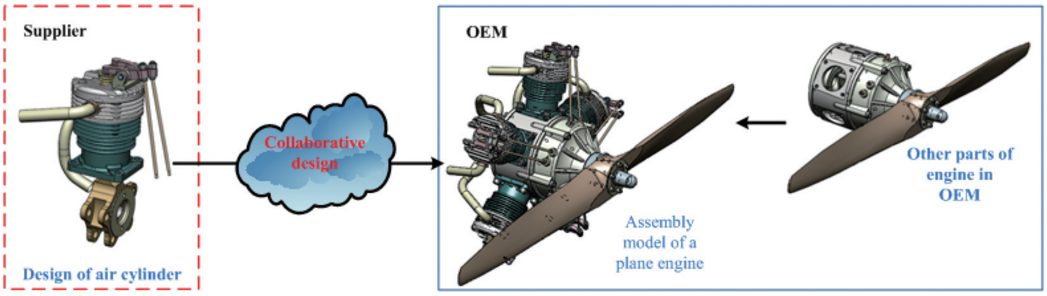

Supplier
Design of air cylinder
Collaborative design
OEM
Assembly model of a plane engine
Other parts of engine in OEM

Fig. 10. Collaborative design of a plane engine.

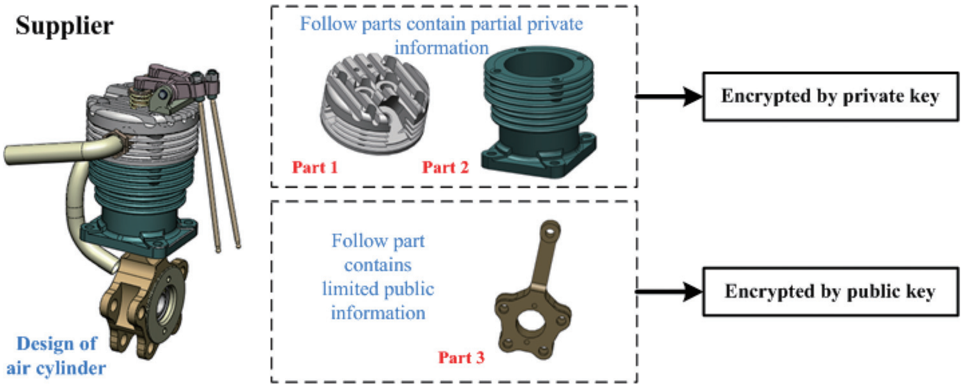

Supplier
Design of air cylinder
Follow parts contain partial private information
Part 1
Part 2
Encrypted by private key
Follow part contains limited public information
Part 3
Encrypted by public key

Fig. 11. Encrypting analysis of the air cylinder.

users except the model owner, considering the Private Key Space is only kept by the model owner. (2) For one of the Limited Public Parts, if the model owner wants to authorize any user to access it, he/she can send the related key (K) to the user as the authorization, considering the Public Key Space is backup by all the uses in CPD. Any one getting the authorization can decrypt the related Limited Public Part, but the others who do not get the authorization cannot decrypt it. Therefore, the authorization can be controlled flexibly by the model owner based on the encrypting key.

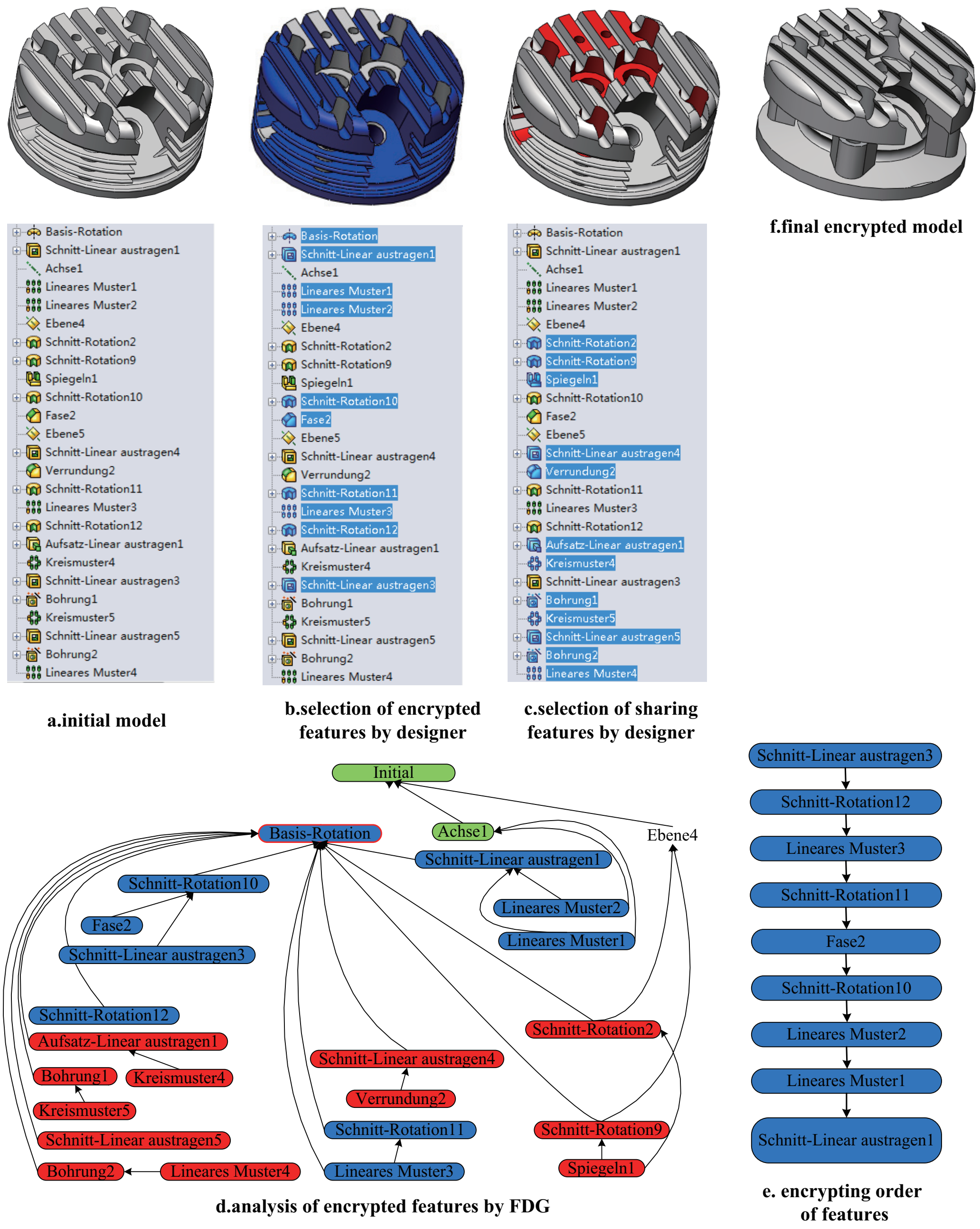
5.4. Security analysis

Because of the random invertible matrix based encryption and the dual-key mode, the existing attacks is invalid for the method presented in this paper, the security analysis is detailed as follows.

(1) Because the encryption method proposed in this paper is not based on the periodic matrix but the random invertible decimal matrix, various attack methods for the periodic matrix based transformation of graph are invalid for the encryption method proposed in this paper.

(2) Since the encrypting key is generated temporarily when a CAD model is encrypted, the encrypting keys are different each time. The most dangerous “Known Plaintext Attack” and “Chosen Plaintext Attack” for the periodic matrix based transformation of graph are also invalid for the encryption method proposed in this paper.

(3) The order of the Key Space is n, and the elements of the Key Space are m decimal, the random invertible decimal matrix has $O(10^{mn^2})$ possibility. If the ‘n’ and ‘m’ are large enough,



a.initial model

b.selection of encrypted features by designer

c.selection of sharing features by designer

f.final encrypted model

d.analysis of encrypted features by FDG

e. encrypting order of features

Fig. 12. The partial encryption of Part 1.

the random invertible decimal matrix cannot be guessed.

(4) The encryption method proposed in this paper is based on the dual-key mode, as thus, the encrypted CAD model cannot be decrypted if any one of the Key Space and Encrypting Key is captured by the others. It can guarantee the secure transmission of the encrypted CAD model.

6. Case study

A real example (based on the SolidWorks 2010) is given as the following to verify the architecture, methods and algorithms presented in this paper.

In this case, there are two distributed sites for an OEM and a Supplier. In the two sites, a plane engine is designed collaboratively. During the process of the

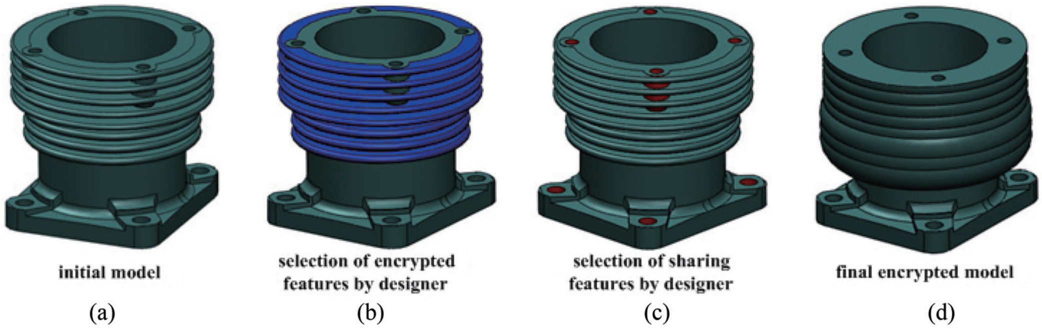

initial model
(a)
selection of encrypted features by designer
(b)
selection of sharing features by designer
(c)
final encrypted model
(d)

Fig. 13. The partial encryption of Part 2.

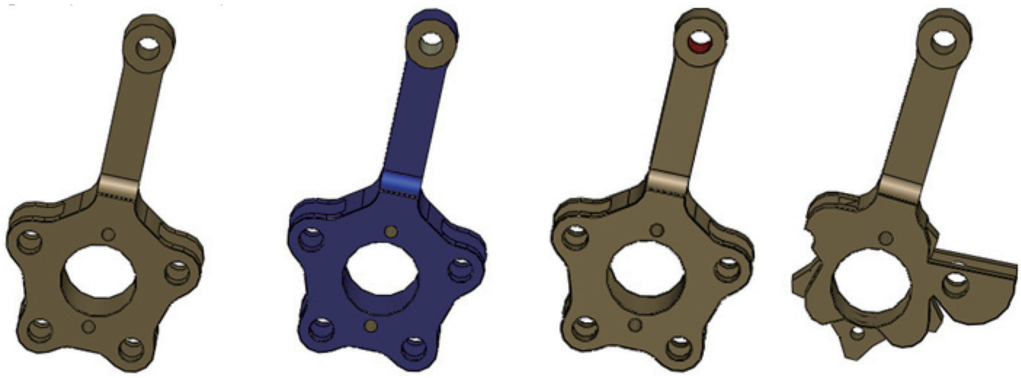


Fig. 14. The partial encryption of Part 3.

collaborative design, the cylinder model created by the supplier should be shared by the OEM, as Fig. 10.

When the Supplier adds into this task, two Key Spaces are generated as follows:

$$M_{private} =$$

$$\begin{bmatrix} 0.786 & 0.775 & 0.997 & 0.654 & 0.954 & 0.221 & 0.002 & 0.886 \\ 0.102 & 0.790 & 0.323 & 0.993 & 0.811 & 0.013 & 0.225 & 0.336 \\ 0.961 & 0.497 & 0.308 & 0.746 & 0.675 & 0.265 & 0.354 & 0.874 \\ 0.634 & 0.654 & 0.253 & 0.234 & 0.457 & 0.875 & 0.946 & 0.120 \\ 0.523 & 0.886 & 0.673 & 0.563 & 0.647 & 0.321 & 0.903 & 0.773 \\ 0.674 & 0.324 & 0.653 & 0.776 & 0.997 & 0.610 & 0.110 & 0.222 \\ 0.562 & 0.887 & 0.769 & 0.394 & 0.700 & 0.801 & 0.831 & 0.654 \\ 0.265 & 0.654 & 0.882 & 0.999 & 0.231 & 0.001 & 0.300 & 0.911 \end{bmatrix}$$

$$M_{public} =$$

$$\begin{bmatrix} 0.986 & 0.215 & 0.347 & 0.674 & 0.994 & 0.991 & 0.202 & 0.546 \\ 0.002 & 0.120 & 0.113 & 0.893 & 0.941 & 0.321 & 0.987 & 0.361 \\ 0.747 & 0.254 & 0.651 & 0.003 & 0.871 & 0.132 & 0.942 & 0.431 \\ 0.887 & 0.199 & 0.965 & 0.804 & 0.213 & 0.563 & 0.845 & 0.009 \\ 0.345 & 0.873 & 0.837 & 0.575 & 0.080 & 0.777 & 0.043 & 0.227 \\ 0.823 & 0.285 & 0.979 & 0.747 & 0.879 & 0.021 & 0.190 & 0.011 \\ 0.654 & 0.748 & 0.548 & 0.901 & 0.606 & 0.090 & 0.033 & 0.119 \\ 0.802 & 0.356 & 0.776 & 0.345 & 0.920 & 0.391 & 0.237 & 0.999 \end{bmatrix}$$

For the supplier, some CAD models of the air cylinder contains important confidential information which is closed to the other designers, and some CAD models of the air cylinder should be shared by the OEM for the assembly analysis, as Fig. 11.

Both Part 1 and Part 2 contain some Private Information, so they should be encrypted by the Private Key.

- Partial encryption of Part 1
  The generated Encrypting Key and matrix of the Part 1 are as follow.

$$A_{3\times 3\_private1} = \begin{bmatrix} 0.997 & 0.102 & 0.457 \\ 0.321 & 0.001 & 0.300 \\ 0.354 & 0.120 & 0.886 \end{bmatrix},$$

$$key_{private1} = \{(1,3),(2,1),(4,4),(5,6),$$
$$(8,6),(8,7),(3,7),(4,8),(1,8)\}$$

  The partial encryption of the Part 1 is as Fig. 12. Figure 12(a) shows the initial model of the Part 1 and its feature tree; Fig. 12(b) shows the selected features of the Part 1 by the creator (the blue region); Fig. 12(c) shows the sharing features of the Part 1 needed by the OEM (the red region); Fig. 12(d) is the screening of the final encrypted features based on the FDG; Fig. 12(e) shows the final encrypting array and its encrypting order of the Part 1; Fig. 12(f) shows the final partial encrypted result of Part 1.
- Partial encryption of Part 2
  The generated Encrypting Key and the encrypting matrix of Part 2 are as follows.

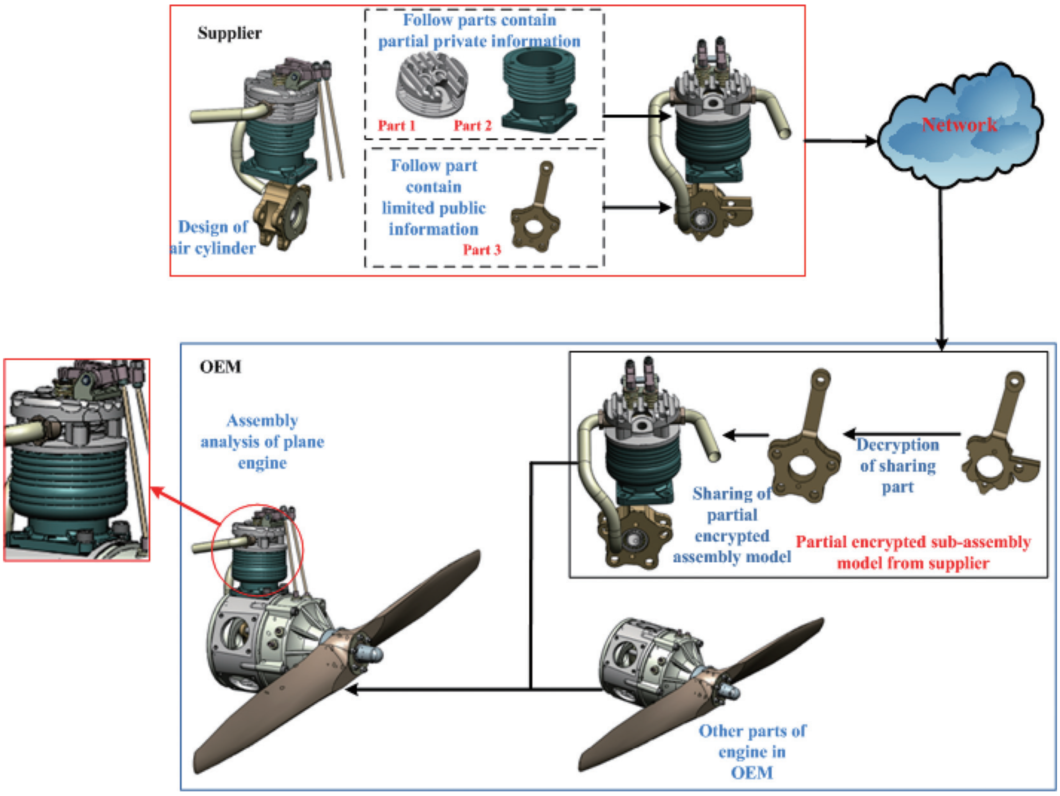

Supplier
Follow parts contain partial private information
Part 1
Part 2
Follow part contain limited public information
Part 3
Design of air cylinder
Network
OEM
Assembly analysis of plane engine
Decryption of sharing part
Sharing of partial encrypted assembly model
Partial encrypted sub-assembly model from supplier
Other parts of engine in OEM

Fig. 15. An example for the encryption based secure partial sharing of the CAD model.

$$A_{3\times 3\_private2} = \begin{bmatrix} 0.786 & 0.654 & 0.110 \\ 0.231 & 0.773 & 0.308 \\ 0.253 & 0.225 & 0.997 \end{bmatrix},$$

$$key_{private2} = \{(1,1),(4,2),(6,7),(8,5),$$
$$(5,8),(3,3),(4,3),(2,7),(1,3)\}$$

The partial encryption of Part 2 is as Fig. 13.
Part 3 is needed by the OEM for assembly analysis and contains some Limited Public Part, so it should be encrypted by the Public Key.

- Partial encryption of Part 3
The generated Encrypting Key and the encrypting matrix of Part 3 are as follows.

$$A_{3\times 3\_public} = \begin{bmatrix} 0.986 & 0.254 & 0.606 \\ 0.011 & 0.999 & 0.345 \\ 0.202 & 0.651 & 0.546 \end{bmatrix},$$

$$key_{public} = \{(1,1),(3,2),(7,5),(6,8),$$
$$(8,8),(5,1),(1,7),(3,3),(1,8)\}$$

The partial encryption of the Part 3 is as Fig. 14. After the partial encryption of the air cylinder, it is sent to the OEM for sharing as in Fig. 15. In the supplier the partial encryption doesn't influence the assembly of Part 1, Part 2 and Part 3. When the encrypted model of air cylinder is sent to OEM, the Part 3 is partially decrypted for the assembly analysis, and Part 1 and Part 2 are not partially decrypted for their Private Information.

7. Conclusion

In this paper, an encryption based partial sharing approach for a CAD model is proposed. The characteristics and contributions of this new approach are summarized as follows.

(1) A random invertible decimal matrix based partial encryption method for a CAD model is proposed. The sketches of the confidential parts are transformed randomly by a random invertible decimal matrix. The confidential information can be hidden by the shape change of the confidential part which is achieved by the transformation of the sketches. Based on this method,

the encrypted parts are decided by the model owner flexibly.

(2) A dual-key mode is developed for the generation of the encrypting keys. The mechanism can improve the security of the key transmission. Based on the dual-key mode, two key spaces (Private Key Space and Public Key Space) are designed for the different levels of security. Also a flexible key based authorization mechanism for partial access of CAD model is adopted, the model owner can authorize the user to share any Limited Public Part flexibly according to the related encrypting key.

The *partial encryption method of an assembly model* is proposed as future research topic.

(1) The partial encryption method proposed in this paper is based on the single CAD model. Although the screening algorithm of the encrypting features ensures the successful assembly of the CAD model, partial encryption of the assembly is achieved by the partial encryption of the features one by one. Therefore, a partial encryption method of assembly model should be proposed in future. Based on this method, a group of CAD models in the assembly model can be selected to be encrypted, and the assembly features of every CAD models can be excluded automatically which can ensure the successful assembly of the encrypted CAD models.

(2) Different from the single CAD model, the structure of the assembly model is the important information to be protected in the partial sharing of the assembly model, the partial encryption method of assembly model should have the capability of hidden the partial structure of the assembly model.

Acknowledgments

This paper is supported by the National Science Foundation of China (Grant No. 61303215 and No. 61472289) and EU FP7 CAPP-4-SMEs project (FP7-2012-NMP-ICT-FoF-314024).

References

[1] L.H. Wang, W.M. Shen, H.L. He et al., Collaborative conceptual design-state of the art and future trends, *Computer-Aided Design* **34** (2002), 981–996.

[2] X.D. Zhang, Y.Z. Li, S. Zhang et al., Modelling and simulation of the task scheduling behavior in collaborative product development process, *Integrated Computer-Aided Engineering* **1**(20) (2013), 31–44.

[3] Y. Cheng, F.Z. He, X.T. Cai and D.J. Zhang, A group undo/redo method in 3D collaborative modeling systems with perfor-mance evaluation, *Journal of Network and Computer Applica-Tions* **36**(6) (2013), 1512–1522.

[4] O.F. Valilai and M. Houshmand, A collaborative and integrated platform to support distributed manufacturing system using a service-oriented approach based on cloud computing paradigm, *Robotics and Computer-Integrated Manufacturing* **29** (2013), 110–127.

[5] Y. Zeng, L. Wang, X. Deng et al., Secure collaboration in global design and supply chain environment: Problem analysis and literature review, *Computers in Industry* **63** (2012), 545–556.

[6] A. Marucheck, N. Greis, C. Mena et al., Product safety and security in the global supply chain: Issues, challenges and research opportunities, *Journal of Operations Management* **29** (2011), 707–720.

[7] X.X. Li, F.Z. He, X.T. Cai et al., A method for topological entity matching in the integration of heterogeneous CAD systems, *Integrated Computer-Aided Engineering* **1**(20) (2013), 15–30.

[8] L.S. Rutledge and L.J. Hoffman, A survey of issues in computer network security, *Computers and Security* **4**(5) (1986), 296–308.

[9] S. Hauck and S. Knol, Data security for Web-based CAD, *Design Automation Conference, San Francisco* (1998), 788–793.

[10] A.Z. Tirkel, G.A. Rankin, R.M. vanSchyndel et al., Electronic water mark, sydeny, *Macquarie University* (1993), 56–58.

[11] A.Z. Tirkel, C.F. Osborne and T.E. Hall, Image and watermark registration, *Signal Processing* **3**(66) (1998), 373–383.

[12] H. Tao, J.M. Zain, M.M. Ahmed et al., A wavelet-based particle swarm optimization algorithm for digital image watermarking, *Integrated Computer-Aided Engineering* **1**(19) (2012), 81–91.

[13] Z.Q. Yu, H.S. Horace and L.F. Kwok, A robust watermarking scheme for 3D triangular mesh models, *Pattern Recognition* **36** (2003), 2603–2614.

[14] F. Cayre, P.R. Alface, F. Schmitt et al., Application of spectral decomposition to compression and watermarking of 3D triangle mesh geometry, *Signal Processing* **18** (2003), 309–319.

[15] R.D. Newbould, D.L. Irby, J.D. Carothers et al., Mixed signal design watermarking for IP protection, *Integrated Computer-Aided Engineering* **3**(10) (2003), 249–265.

[16] C.M. Chou and D.C. Tseng, A public fragile watermarking scheme for 3D model authentication, *Computer-Aided Design* **38** (2006) 1154–1165.

[17] S.H. Lee and K.R. Kwon, A watermarking for 3D mesh using the patch CEGIs, *Digital Signal Processing* **17** (2007), 396–413.

[18] W.B. Wang, G.Q. Zheng, J.H. Yong et al., A numerically stable fragile watermarking scheme for authenticating 3D models, *Computer-Aided Design* **40** (2008), 634–645.

[19] Q.S. Ai, Q. Liu, Z.D. Zhou et al., A new digital watermarking scheme for 3D triangular mesh models, *Signal Processing* **89** (2009), 2159–2170.

[20] S.H. Lee and K.R. Kwon, CAD drawing watermarking scheme, *Digital Signal Processing* **20** (2010), 1379–1399.

[21] F. Peng, Y.Z. Lei, M. Long et al., A reversible watermarking scheme for two-dimensional CAD engineering graphics based on improved difference expansion, *Computer-Aided Design*

43 (2011), 1018–1024.

[22] S.H. Lee and K.R. Kwon, Robust 3D mesh model hashing based on feature object, *Digital Signal Processing* **22** (2012), 744–759.

[23] Z.Y. Su, W.Q. Li, J.S. Kong et al., Watermarking 3D CAPD models for topology verification, *Computer-Aided Design* **45** (2013), 1043–1052.

[24] B.W. Lampson, Protection, *Operatin System Rev* **8**(1) (1974), 18–24.

[25] R. Conway, W. Maxwell and H. Morgan, On the implementation of security measures in information system, *Communcations of the ACM* **15**(4) (1972), 211–220.

[26] R. Sandhu, E. Coyne and H. Feinstein, Role-based access control models, *IEEE Computer* **29**(2) (1996), 38–47.

[27] S. Oh and S. Park, Task-role-based access control model, *Information System* **28**(6) (2003), 533–562.

[28] J. Park and R. Sandhu, Towards usage control models: Beyond traditional access control, *Proceedings of the 7th ACM Symp On Access Control Models and Technologies, California* (2002), 57–64.

[29] J. Park and R. Sandhu, The UCONABC usage control model, *ACM Transaction on Information and System Security* **7**(1) (2004), 128–174.

[30] H.A. van der, O. ten Bosch, R. van Leuken et al., A flexible access control mechanism for CAD frameworks, *Proceedings of the Conference on European Design Automation Los Alamito* (1994), 188–193.

[31] G. Stevens and V. Wulf, A new dimension in access control: Studing maintenance engineering across organizational boundaries, *Proceedings of 2002 ACM conference on CSCW* (2002), 196–205.

[32] C.D. Cera, T. Kim, I. Braude et al., Role-based viewing for secure collaborative modeling, *Pennsylvania: Technical Report DU-CS-03–04, Drexel University, Department of Computer Science* (2003).

[33] K.K. Leong, K.M. Yu and W.B. Lee, A security model for distributed product data management system, *Computers in Industry* **50** 179–193.

[34] B. Adrian and B. Steve, An access control framework for multi-user collaborative environment, *Proceedings of the international ACM SIGGROUP Conference on Supporting Group Work* (1999), 140–149.

[35] K. Rouibah and S. Ould-Ali, Dynamic data sharing and security in a collaborative product definition management system, *Robotics and Computer-Integrated Manufacturing* **23** (2007), 217–233.

[36] H.B. Chang, K.K. Kim and Y.D. Kim, The research of security system for sharing engineering drawings, *IEEE Computer Society, Washington, USA* (2007), 319–322.

[37] L.H. Yao, J. Shao, G.Q. Sheng et al., Research on a security model of data in computer supported collaborative design integrated with PDM system, *IITA 2007: Workshop on Intelligent Information Technology Application* (2007), 91–94.

[38] H.B. Chang, K.K. Kim and Y.D. Kim, The development of security system for sharing CAD drawings in U-environment, *Computing and Informatics* **5**(27) (2008), 731–741.

[39] C. Speiera, J.M. Whippleb, D.J. Clossc et al., Global supply chain design considerations: Mitigating product safety and security risks, *Journal of Operations Management* **29** (2011), 721–736.

[40] H. Xiang and M. Li, The research of network security mechanism based collaborative design, *Advanced Design Technology* **421** (2012), 406–409.

[41] H. Hoppe, Progressive meshes, *Proceedings of ACM SIGGRAPH* (1996), 99–108.

[42] J.H. Han, T. Kim, C.D. Cera et al., Multi-resolution modeling in collaborative design, *Proceedings of the Eighteenth International Symposium on Computer and information Sciences, Antalya, Turkey* (2003).

[43] Z.M. Qiu, Y.S. Wong, J.Y.H. Fuh et al., Geomelric model simplification for distributed CAD, *Computer-Aided Design* **36**(9) (2004), 809–819.

[44] W.D. Li, Y.L. Cai and W.F. Lu, A 3D simplification algorithm for distributed visualization, *Computers in Industry* **58** (2007), 211–226.

[45] M. Belaziz, A. Bouras and J.M. Brun, Morphological analysis for product design, *Computer-Aided Design* **32**(5–6) (2000), 377–388.

[46] J. Seo, Y. Song, S. Kim et al., Wrap-around operation for multi-resolution of B-rep model, *Proceedings of CAD'05* **2** (2005), 67–76.

[47] S. Kim, K. Lee, T. Hong et al., An integrated approach to realize multi-resolution of B-rep model, *Proceedings of the 2005 ACM Symposium on Solid and Physical Modeling, Cambridge, Massachusetts* (2005), 153–162.

[48] J.Y. Lee, J.H. Lee, H. Kim et al., A cellular topology-based approach to generating progressive solid models from feature-centric models, *Computer-Aided Design* **36**(3) (2004), 217–229.

[49] S.H. Lee, A CAD-CAE integration approach using feature-based multi-resolution and multi-abstraction modelling techniques, *Computer-Aided Design* **37**(9) (2005), 941–955.

[50] S.H. Lee, Feature-based multi-resolution modeling of solids, *ACM Transactions on Graphics* **4**(24) (2005), 1417–1441.

[51] C. D Cera, I. Braude, T. Kim et al., Hierarchical role-based viewing for multilevel information security in collaborative CAD, *Journal of Computer and Information Science in Engineering* **1**(6) (2006), 2–10.

[52] T. Kim, C.D. Cera, W.C. Regli et al., Multi-Level modeling and access control for data sharing in collaborative design, *Advanced Engineering Informatics* **20** (2006), 47–57.

[53] C.H. Chu, Y.H. Chan and P.H. Wu, 3D streaming based on multi-LOD models for networked collaborative design, *Computers in Industry* **59** (2008), 863–872.

[54] C.H. Chu, P.H. Wu and Y.C. Hsu, Multi-agent collaborative 3D design with geometric model at different levels of detail, *Robotics and Computer-Integrated Manufacturing* **25** (2009), 334–347.

[55] S. Li and M. Mirhosseini, A matrix-based modularization approach for supporting secure collaboration in parametric design, *Computers in Industry* **63** (2012), 619–631.

[56] C.E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal* **4**(28) (1949), 656–715.

[57] W. Diffie and M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **6**(22) (1976), 644–655.

[58] Z. Huang, G.D. Liu, Z. Ren et al., A method of 3D data information encryption with virtual holography, *Proceedings of SPIE-The International Society for Optical Engineering* **7125** (2009), 71250E1–71250E7.

[59] E. Esam and A. Ben. H, Secret sharing approaches for 3D object encryption, *Expert Systems with Applications* **38** (2011), 13906–13911.

[60] K.N. Naveen and J.N. Thomas, Flexible optical encryption with multiple users and multiple security levels, *Optics Communications* **284** (2011), 735–739.