Advanced Engineering Informatics 33 (2017) 374–387

Contents lists available at ScienceDirect

Advanced Engineering Informatics

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

Full length article

An encryption approach for product assembly models

X.T. Cai [a,b], S. Wang [b], X. Lu [b], W.D. Li [b,*]

[a] School of Computer Science and Technology, Wuhan University, Wuhan, China
[b] Faculty of Engineering, Environment and Computing, Coventry University, Coventry, UK

ARTICLE INFO

Article history:
Received 4 July 2016
Received in revised form 4 December 2016
Accepted 12 December 2016
Available online 28 December 2016

Keywords:
Assembly encryption
Assembly features
Encrypted features
Feature classification

ABSTRACT

In a collaboration environment, it is a challenge how to effectively share the information needed for collaboration while protecting other confidential information in a product assembly model. In this paper, an innovative encryption approach for assembly models to support collaboration is presented. This approach is content based encryption and effective for the secure sharing of feature-based assembly models. In the approach, a classification algorithm for features in an assembly model to be shared or protected during collaboration has been first developed. An encryption algorithm for a feature has been then designed to ensure the parameterization, topological and geometrical validity, and self-adaptability of the encrypted feature. An algorithm for parts with multiple encryption features has been developed. Based on the above algorithms, parts are finally assembled and the geometry and topology of the assembling structure are kept un-changed to enhance collaborators' interoperability. The characteristics and innovations of the approach include: (1) the approach is feature based, integrative into the main-stream commercial Computer Aided Design (CAD) systems, and flexible to meet various users' needs for encrypting features selected by users during collaboration, (2) in the approach, the topological and geometrical validity of an assembly model after encryption is maintained to ensure effective collaboration on the assembly, and (3) the approach is parametrically controlled through adjusting position and size parameters so as to ensure the user friendliness of using the approach. A case study with complex geometries and assembly structures has been used to validate the effectiveness and robustness of the approach in industrial applications.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Product development enterprises consider their product models as core intellectual properties [1,2]. In order to support collaborative product development effectively, flexible encryption approaches on product models (e.g., Computer Aided Design (CAD) models) are imperative to ensure effective information sharing for collaboration as well as protection of other private information in the models [3,4].

An assembly contains critical assembly structure information and the parts in it contain abundant design features, design procedure and feature parameters. However, the related security research on assemblies has focused on the part level. It is still far away from meeting industrial requirements [5]. To protect the assemblies as well as supporting the flexibly sharing and collaboration in a network based manufacturing environment, an innovative encryption approach for product assembly models is presented in this paper. The innovations of the approach include:

(1) The approach is feature based and can be integrated to main-stream feature based CAD systems that have been widely used in industries. Through the feature based encryption mechanism for an assembly model, users' needs of encrypting selected features will be met, and the assembly features and structure will be maintained to facilitate collaboration;
(2) The approach is based on the geometrical deformation of features. By maintaining assembly features while deforming other selected features in an assembly model, the validity of the structure in the assembly model is ensured while other features to be protected by geometrical deformation;
(3) The approach is designed based on a parametrically controlled mechanism to enhance user friendliness. Geometrical deformation for encrypting features in an assembly model is controllable by users through adjusting position and size parameters defined in the parametric mechanism of the encryption approach.

The remainder of this paper is organized as follows. In Section 2, related research work is surveyed. Section 3 introduces the details of the encryption approach for assembly models. A case study to

[*] Corresponding author.
E-mail address: aa3719@coventry.ac.uk (W.D. Li).

http://dx.doi.org/10.1016/j.aei.2016.12.001
1474-0346/© 2016 Elsevier Ltd. All rights reserved.

validate the approach is given in Section 4. Finally, conclusions are given in Section 5.

2. Related work

In the past years, a number of related research projects have been conducted. The research can be classified as three categories [6] - (1) collaboration access control, (2) simplification of product models for collaboration, and (3) feature-based product model encryption. The related work are summarized below:

Collaboration access control has been widely used for data security in a network environment. Mechanisms were designed to authorize users to access the shared data. In early times, generic access control methods were used for protecting product models during collaboration [7–11]. Later on, in consideration of the complexity of design data, some dedicated access control methods were developed, such as access control based CAD architecture [12], ADOSX system that can handle CPD (collaborative product development) between two enterprises by Stevens [13], a secure access control mechanism for 3D models [14], and a security approach for a distributed product data management system [15]. Moreover, taking account of the frequent sharing of design data, sharing space based access control methods were developed, in which a secure sharing space was designed [16–18]. Moreover, for further improving model security during collaboration, access control mechanisms were reinforced by introducing digital signature or watermark mechanisms for product model protection [19–22]. Generally speaking, although different access levels for the models can be defined, the protecting granularity is not small enough and the confidential information of every access level cannot be arranged flexibly by the model owner. As such, the developed methods on product models are still not flexible enough to support collaboration.

In order to protect the private information of product models during collaboration, methods for simplification of product models (e.g., as different Level Of Details (LODs)) were developed. Cera proposed a LOD based access control method for CAD models [23,24]. Chu developed a mechanism for sharing of LOD CAD models for product collaboration [25,26]. Li proposed a matrix-based modularization approach for CAD models [27]. The above approaches are mainly aimed at part models. To support assembly based collaboration, some research work focus on the mechanism of simplifying assemblies. In the simplification process of assembly models, internal parts and features that are not visible from outside are the first to be removed. Kanai and Yu detected invisible features by pre-rendering the models from multiple view directions [28,29]. Han proposed an approach to automatically create a simplified assembly models with the desired LOD value [30,31]. The simplification methods were mainly designed for the purpose of efficient model sharing via the Internet with limited bandwidth to support collaboration. The levels of details cannot be designated by the model owner. As such, users' collaboration requirements on secure sharing of assemblies could not be addressed effectively.

Encryption research was conducted to protect CAD models. Special encryption of for 3D models was proposed [32]. However, the developed encryption methods are not feature based, which are not easily integrated with the main-stream CAD systems used in industries and inflexible to operate during collaboration.

The authors of this paper have actively developed related research in recent years. The feature based encryption methods developed by the authors have provided flexible mechanisms for users to select features for encryption, and the encryption process on features can be controlled by users in a parametric means [33,34]. On the other hand, collaboration is usually carried out in an assembly level, while the related research conducted on the feature level has limited the effectiveness of the methods in applications.

3. Encryption approach for assembly models

A collaboration application scenario for encrypting an assembly model is illustrated in Fig. 1. For instance, there are two collaborators to work on an assembly model. Part 1 and Part 2 are designed by Collaborator 1 as a sub-assem_1, to be assembled with Part 3 designed by Collaborator 2 as an assembly model. During collaboration, assembly features and associate features are kept the same to indicate the assembly relationships while other features are encrypted for design information protection.

The encryption process of the approach is depicted in Fig. 2. The approach is implemented through the following three algorithms:

(1) **Classification algorithm for assembly features, dependent features and encrypted features -** In order to satisfy assembly constraints, assembly relations and related features should be maintained after the encryption of other features and the parts. A classification algorithm is developed for

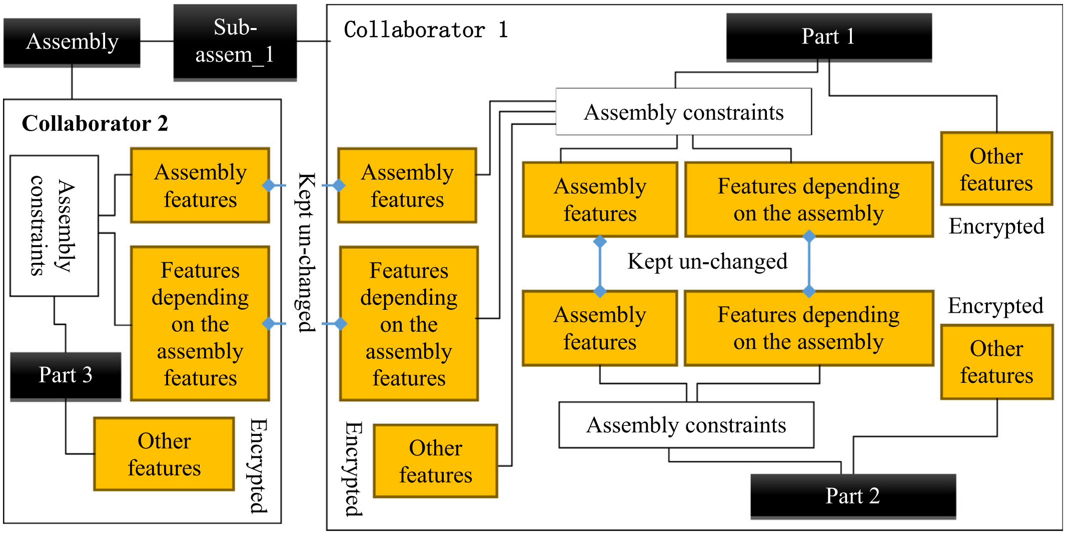

Fig. 1. The collaboration scenario for encrypting an assembly model.

Download English Version:

https://daneshyari.com/en/article/6478399

Download Persian Version:

https://daneshyari.com/article/6478399

Daneshyari.com