УДК 658.512.011.56

ВЫБОР ОБЪЕКТОВ ДЛЯ БЫСТРОГО ВЫЧИСЛЕНИЯ ХЕША ДОКУМЕНТОВ МОДЕЛЕЙ CAD-СИСТЕМ

Сергей Борисович КОРШИКОВ родился в 1981 г. в деревне Обновленный труд Истринского района Московской области. Старший преподаватель МАИ. Кандидат технических наук. Основные научные интересы — в области систем геометрического моделирования, защиты информации. Автор пяти научных работ. E-mail: s.b.korshikov@gmail.com

Sergey KORSHIKOV, Ph.D., was born in 1981, in Moscow Region. He is senior assistant professor at the MAI. His major research interests are in CAD/CAM/CAE system and information security. He has published 5 technical papers. E-mail: s.b.korshikov@gmail.com

В статье рассмотрен способ быстрого вычисления хеша документа CAD-системы с помощью использования информационной выборки из документа модели, что обеспечивает сокращение времени на подписание документа электронной цифровой подписью и ее проверку.

In this article we are reviewing method of fast calculation of CAD documents hash. This method based on information selection from model document, that reduce time for making document's digital signature and authentication against it.

Ключевые слова: модели CAD-систем, хеш, электронная цифровая подпись.

Key words: model CAD, hash, digital signature.

Одной из основных проблем при использовании САПР является определение персональной ответственности исполнителя конкретной модели (файла, чертежа). В случае использования традиционной («бумажной») технологии мера и объем ответственности конкретного исполнителя определяется его подписью на чертеже. Для безбумажной технологии такого однозначного критерия нет. Поэтому довольно часто используют гибридные методы — наряду с электронной моделью оформляется «эскизный» бумажный чертеж, который подписывается исполнителем модели. При всей кажущейся простоте такого подхода наличие бумажной документации существенно увеличивает сроки работы над изделием и в некоторых случаях полностью нивелирует выгоду от использования САПР, так как подписанный чертеж или иной бумажный документ необходимо сканировать и внести в базу данных, и при этом легитимностью обладают только подписанные бумажные документы [1].

Фактически единственным способом достоверной аутентификации автора электронного документа является электронная цифровая подпись (ЭЦП) [2,3]. Наряду с определением авторства использование ЭЦП позволяет осуществить контроль целостности документа, защиту от подделки и невозможность отказа от авторства. Однако из-за особенностей документов CAD-систем использование ЭЦП сопряжено с некоторыми трудностями.

Обычно документы CAD/CAM/CAE-систем имеют достаточно большой информационный объем (например, размер файла модели детали со сложной геометрией может достигать сотен Мб). Из-за этого временные затраты на вычисление ЭЦП такого документа модели часто являются неприемлемыми, и вместо подписания документа модели вычисляется ЭЦП хеша документа. Но вычисление хеша также занимает некоторое время (например, при аппаратной реализации вычисление хеша по ГОСТ 3.11-94 производится со скоростью 3Мб/с [4]).

Поэтому следует рассмотреть структуру документа CAD и выбрать минимальное количество объектов, на основе которых можно вычислять хэш документа.

Условно можно считать, что в документе модели детали хранятся геометрические данные, негеометрические данные и служебная информация. К геометрическим данным относятся данные топологии и конструкции, к негеометрическим — информация о весе, плотности и т.п. и атрибуты документа, к служебной информации — специфические данные, зависящие от формата представления документа (т.е. от конкретной CAD-системы).

Очевидным является то, что следует выбирать для вычисления хеша те блоки информации, которые наиболее часто изменяются при редактировании документа. При рассмотрении типичных атрибутов документа CAD-системы наиболее подвер-

женными изменению будут две категории атрибутов:

- атрибуты файла;
- атрибуты модели.

К атрибутам файла относятся: продолжительность работы с файлом, дата и время последнего сохранения, размер файла. К атрибутам модели однозначно относятся весовые характеристики (для твердотельных моделей) и часть атрибутов документа (например, время редактирования, версия файла, номер лицензии продукта и т.п.). Однако такая информация может быть легко фальсифицирована, и соответственно ее недостаточно для вычисления хеша.

Если рассмотреть структуру геометрических данных, хранимых в документе модели детали, то вне зависимости от используемой CAD-системы и метода создания модели (параметрическая или синхронная модель) в ней будут присутствовать вершины первого порядка, заданные своими координатами в некоторой базовой системе координат. Действительно, представление вершин более высокого порядка (ребра, грани и т.д.) зависит от конкретной CAD-системы (например, ребра могут быть смоделированы как структурами крыльевых ребер, так и полуребер).

Изменения, вносимые в геометрию модели, всегда приводят к модификации списка вершин (или координат хотя бы одной вершины). Естественно, даже минимального изменения этого списка достаточно, чтобы избежать коллизий первого рода благодаря лавинному эффекту, обеспечиваемому хешированием по ГОСТ 3.11-94 [5], а также другими распространенными алгоритмами. При этом координаты списка вершин практически невозможно фальсифицировать, так как невозможно получить две (или больше) модели нетривиальной геометрии с полностью совпадающим списком вершин, и, следовательно, выборка вершин не подвержена коллизиям второго рода.

Исходя из изложенного выше, список вершин фактически не подвержен подделке и фальсификации. Однако для документов деталей с несложной геометрией (тела вращения и т. п) список вершин может быть относительно мал, чтобы сформировать хеш рекомендуемой длины (от 256 бит). Поэтому в набор информации для хеша следует включить отобранные атрибуты документа.

Получение координат вершин модели из документа модели может быть реализовано с использованием внутренних функций CAD-системы и не представляет сложности.

Таким образом, для вычисления хеша документа модели следует использовать набор выборок из негеометрической и геометрической информации. При этом выборка геометрической информации обеспечивает сложность фальсификации документа, а выборка негеометрической информации дополняет набор до необходимого размера и гарантирует учет «негеометрических» изменений документа, например изменение материала, из которого должна быть изготовлена деталь.

Единственным недостатком предложенного способа выборки информации для вычисления хэша является необходимость разработки и внедрения специального программного обеспечения, однако оно может быть интегрировано в программное обеспечение, реализующее механизмы ЭЦП.

Выводы

Предложенный механизм выделения инвариантных относительно CAD-систем характеристик документов модели в качестве исходных данных для хеша ЭЦП позволит сократить время, затрачиваемое на вычисление и проверку ЭЦП документов моделей деталей. Более того, использование координат вершин позволяет обеспечить практически одинаковое время вычисления хеша для документов различного информационного объема. Полученный результат может быть легко распространен на вычисление хешей электронных макетов изделий.

Работа выполнена в рамках НИР (ГК П1959) по ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

Библиографический список

1. *Пиликов Н.* Электронный документооборот и цифровая подпись в условиях использования CAD/CAM-систем конструкторско-технологической подготовки производства // CADmaster. 2006. №3. С. 56-59.

2. ФЗ РФ «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ

3. ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». — М.: Госстандарт России, 2001. 16 с.

4. Информационный буклет об изделии «Шипка» [Электронный ресурс]/ Веб-сайт компании ОКБ САПР; — Электрон. дан. — М., 2007. — 26 с. Режим доступа: http://www.accord.ru/Docs/2007/buklet_shipka.pdf, свободный.

5. ГОСТ Р 34.11-94. «Информационная технология. Криптографическая защита информации. Функция хэширования». — М.: Госстандарт России, 1994.

Московский авиационный институт
Статья поступила в редакцию 19.11.2009

Сдано в набор 03.12.09. Подписано в печать 29.12.09.
Бумага офсетная. Формат 60×84 1/8. Печать офсетная.
Усл. печ. л. 29,29. Уч.-изд. л. 31,50. Тираж 200 экз.
Заказ 4404/303.

Издательство МАИ-ПРИНТ
(МАИ), Волоколамское ш., д. 4, Москва, А-80, ГСП-3 125993
Типография Издательства МАИ
(МАИ), Волоколамское ш., д. 4, Москва, А-80, ГСП-3 125993