УДК: 004.056

ЗАЩИТА ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

В. А. Голуб, И. В. Цветков

Воронежский государственный университет

Поступила в редакцию 10.10.2009

Аннотация. В работе рассматриваются методы зашиты цифровых графических файлов от несанкционированного копирования. Предлагаются алгоритмы и программное обеспечение для решения этой задачи.

Ключевые слова: защита информации, защита от копирования, защита цифровых изображений.

Abstract. The methods of protecting of files which contain digital images from illegal copying are discussed. It also describes algorithms and software program which solve this problem.

Key words: information security, protection against copying, digital images protection.

ВВЕДЕНИЕ

В настоящее время широко распространена передача цифровых изображений от авторов потребителям или посредникам средствами Internet, а так же на различных цифровых носителях. Легкость копирования таких изображений приводит к тому, что постоянно возрастает число нарушений авторских прав на графические работы, в связи с незаконным использованием этих работ, в частности, путем их несанкционированного размещения в интернет-галереях. Таким образом, актуальной является проблема защиты прав авторов цифровых графических работ, техническое решение которой базируется, прежде всего, на предотвращении незаконного копирования и распространения цифровых изображений.

Программное обеспечение, предназначенное для защиты авторских прав на графические работы, может представлять интерес для специалистов, занимающихся дизайном, фотографией, графикой и т.п., которым необходимо, с одной стороны, представлять свои работы потенциальному заказчику, а с другой стороны, быть застрахованными от возможного нарушения авторских прав, связанного с незаконным использованием их работ. В настоящее время авторы вынуждены представлять потртфолио, зачастую содержащее сильно уменьшенные цифровые изображения (preview), качество которых специально занижено, что не позволяет в полной мере оценить их достоинства. В этой связи, приложение, позволяющее предоставить изображения в оригинальном разрешении, но без возможности их копирования, представляет значительный практический интерес для широких кругов специалистов, работающих в области дизайна, фотографии, digital art и т.д.

Данная работа посвящена решению задачи защиты цифровых изображений от несанкционированного копирования. Для этого необходимо предложить методы и алгоритмы для противодействия копированию цифровых графических файлов в процессе их просмотра и хранения, а так же разработать программное обеспечение, реализующее такие алгоритмы. Таким образом, целью работы является разработка приложения, предназначенного для просмотра цифровых изображений, без возможности их копирования, а также не позволяющее стороннему программному обеспечению работать с этой графической информацией.

1. АНАЛИЗ СУЩЕСТВУЮЩИХ СПОСОБОВ ЗАЩИТЫ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

В настоящее время используются следующие способы решения задачи защиты авторских прав на изображения в цифровом виде.

1. Использование различных символов, наносимых на изображение при помощи специальных приложений таких, как, например, Photo Watermark Professional. Данный способ защиты изображений не защищает их от копирования и распространения в различных сетях. Специальные символы часто отвлекают от просмотра изображения, портят его, если являются громоздкими, или могут быть удалены с него в графическом редакторе, если они достаточно малы [1].

2. Использование изображений уменьшенного размера или изображений с низким разрешением. Такие изображения используются при продаже фотографий через Интернет в качестве образца продаваемого изображения и не представляют серьезной ценности.

Понятно, что описанные способы в ряде случаев не позволяют получить необходимый результат, когда изображение имеет высокое качество, но при этом надежно защищено от несанкционированного копирования. Решение такой задачи предполагает обеспечение защищенного хранения и просмотра цифровой графической информации. Для этого, во-первых, необходимо решить задачу защищенного хранения цифровых изображений. Для ее решения можно использовать шифрование оригинала изображения и хранение его в шифрованном виде. Использование такого подхода требует решения задач хранение ключа шифрования и зашифрованного изображения. В качестве решения этой проблемы можно использовать другой формат файла, содержащего шифрованное изображение, что также может повысить скорость работы приложения, за счет того, что в таком файле можно хранить превью изображения для быстрого просмотра. Ключ шифрования можно хранить различными способами в различных составляющих файла. Во-вторых, необходимо решить задачу защиты цифрового изображения от копирования на стадии просмотра. Существует множество способов копирования информации, представленной на рабочем столе (например, Print Screen). Необходимо суметь перехватывать соответствующие команды и модифицировать используемую ими информацию.

2. ОПИСАНИЕ АЛГОРИТМОВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Таким образом, разрабатываемое приложение для защиты графических файлов должно быстро работать с большими объемами информации (качественные графические файлы имеют большой объем) и обеспечивать контроль доступа к этой информации. При этом изображение не должно быть доступно в незащищенном виде ни на одном из этапов его передачи.

Одним из направлений решения поставленной задачи является использование специального формата файла в сочетании с применением криптографических методов защиты, а именно, шифрования данных. Предлагаемый формат файла имеет следующую структуру (при условии чтения файла побайтно):

1) записывается информация о превью изображении в формате BitMap(подробнее о приложении в [2]);

2) записывается само изображение без записи информации о конце файла изображения;

3) записывается размер файла превью и размер файла, содержащего ключ шифрования;

4) записывается информация о BitMap-файле и признак конца фала превью;

5) записывается файл, содержащий ключ шифрования;

6) записывается фал с шифрованным изображением.

При использовании такого формата файла появляется возможность просматривать превью стандартными средствами Windows, что позволяет облегчить процесс просмотра изображений.

Принципиально важным моментом является организация хранения криптографического ключа. Для хранения ключа шифрования используется отдельный файл, содержащий BitMap рисунок 170x170 пикселей. Данный файл создается на основе специально сгенерированной псевдослучайной последовательности, со-

держащей числа от 1 до 999 включительно. Три цифры, составляющие число выступают в качестве rgb-параметров при заполнении каждого пикселя данного изображения. Таким образом, изображение содержит 86700 цифр [3].

Шифрованное изображение, записанное побайтно, хранится в полученном файле после файла-ключа и не может быть открыто сторонними приложениями, предназначенными для просмотра изображений.

Отдельной важной задачей является противодействие копированию изображения с использованием функции Print Screen, представляющей самый простой и распространенный из нескольких возможных способов доступа к графической информации, представленной на рабочем столе. Для защиты от такого способа несанкционированного копирования необходимо программными средствами обеспечить перехват нажатий клавиши <Print Screen> и после этого подменить изображение, размещенное в буфере обмена на некоторое изображение, подготовленное заранее, например, черный квадрат, как реализовано в описываемой программе. Данный способ защиты реализуется функцией, контролирующей ввод с клавиатуры, и изменяющей информацию в буфере обмена после вызова функции Print Screen.

Кроме этого, необходимо решить задачу защиты цифрового изображения от копирования при помощи сторонних приложений, делающих копии экрана (скрин-шот) на стадии просмотра. Наиболее эффективной защитой от программ, делающих скрин-шот при помощи API-функций, является выведение изображения не на стандартном компоненте, а на канве, рисуемой над канвой рабочего стола. Также возможно контролировать вызов WIN API функций и при вызове функций, копирующих изображение, скрывать выведенное изображение, либо запрещать вызов данной функции системными средствами [4].

Описанные выше принципы защиты цифровых изображений от несанкционированного копирования были программно реализованы в специальном приложении. Приложение состоит из двух самостоятельных программ: утилиты шифрования цифрового изображения и программы для расшифровки и просмотра. Первая из них предназначена для авторов, владеющих правами на изображения, и предназначена для создания зашифрованной копии изображения, которое может быть открыто с помощью любых программ-просмотрщиков, но только в виде превью очень малого размера. В полном размере и хорошем качестве зашифрованное изображение не может быть просмотрено никакими средствами, кроме специального просмотрщика-расшифровщика, представленного второй программой. Программа-просмотрщик предназначена для тех пользователей, которые заинтересованы в оценке качественных полноразмерных изображений, но не должны иметь возможности копировать их без разрешения автора.

Интерфейс программы шифрования цифрового изображения организован таким образом, что пользователь может выбрать предназначенный для шифрования графический файл из списка, содержащего разделы жесткого диска, дерево папок и список файлов, находящихся в выбранной папке. При этом для облегчения и ускорения поиска нужного файла используется фильтр графических файлов по расширениям, а выделенное изображение отображается справа от списка папок в уменьшенном виде. После выбора файла изображения запускается процесс его шифрования, в результате которого формируется новый файл с именем исходного файла и расширением JPGX. В начало файла записывается уменьшенная незашифрованная копия изображения — превью, для облегчения в дальнейшем поиска нужного изображения без его расшифрования.

Программа просмотра зашифрованного изображения обеспечивает выбор требуемого графического файла. При этом для ускорения и облегчения выбора графического файла в окне программы отображается извлеченное из файла малоразмерное превью. По завершении процесса расшифрования на экран выводится полноразмерное изображения, масштаб которого может быть изменяем. Какие-либо другие действия с расшифрованным изображением, в том числе его копирование, блокируются.

Тестирование разработанного программного обеспечения показало корректную и стабильную его работу. В частности, как это и должно быть, копирование с использованием функции Print Screen оказалось заблокировано, а попытки использовать графические редакторы и программы-просмотрщики для получения исходного полноразмерного изображения оказались безрезультатными. Стандар-

тные средства Windows, например Paint, позволяли открыть только малоразмерные специально созданные превью-изображения. Также было подтверждено, что в процессе шифрования-расшифрования изображений не происходит их искажений.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе предложен метод защиты цифровых изображений от несанкционированного копирования, использующий разработанные алгоритмы для защиты цифрового изображения на стадии просмотра. Разработано программное обеспечение, включающее два приложения: первое позволяет при помощи алгоритма шифрования RC-6 создавать предназначенные для распространения шифрованные защищенные от копирования и модификации копии изображений, второе предназначено для просмотра шифрованного изображения также без возможности его копирования и модификации. Предлагаемый программный продукт обеспечивает сохранность изображения как в процессе хранения, так и в процессе его просмотра.

СПИСОК ЛИТЕРАТУРЫ

1. PhotoWatermark Professional official web site. — (www.photowatermark.com).

2. База знаний Delphi — Файловаясистема — Файлы. — (http://www.kansoftware.ru/?did=188).

3. Графический формат BMP. — (http://forum.vingrad.ru/articles/topic-94227.html).

4. Список приложений, позволяющих делать «снимки» экрана. — (http://www.softsoft.ru/search/3634/index.htm).

Голуб Владимир Александрович — кандидат технических наук, доцент кафедры рекламы и дизайна Воронежского государственного университета. Тел. (4732) 530-530. E-mail: vgol@list.ru.

Цветков Илья Владимирович — студент 4 курса кафедры математического обеспечения факультета прикладной математики, информатики и механики ВГУ. Тел. (4732) 42-67-12. E-mail: cvetkov@inbox.ru.

Golub Vladimir Aleksandrovich — Candidate of Technical Sciences, Associate Professor, Department of Advertisement and Design, Voronezh State University. Tel. (4732) 530-530. E-mail: vgol@list.ru.

Tsvetkov Ilia Vladimirivich — 4-th year student, Department of applied Mathematics, Informatics and Mechanics Voronezh State University. Tel. (4732) 42-67-12,e-mail: cvetkov@inbox.ru.