УДК 004.9

МЕТОДЫ ЗАЩИТЫ ИЗОБРАЖЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ НА ВЕБ-РЕСУРСАХ

Навка Е. А., Павлий В. А.
Донецкий национальный технический университет
Кафедра компьютерных систем мониторинга
E-mail: navka.e@gmail.com

Аннотация

Навка Е. А., Павлий В. А. Методы защиты изображений от несанкционированного копирования на веб-ресурсах. *Выполнен анализ существующих методов защиты изображений от несанкционированного копирования. Предложен собственный метод защиты изображений, основанный на особенностях восприятия изображения глазом человека.*

Общая постановка проблемы

В связи с высокой популярностью сети Интернет и большого количества графического материала на информационных порталах перед авторами ресурса нередко стоит задача защиты данного материала от несанкционированного копирования. Данная статья посвящена анализу потенциальных угроз, связанных с копированием графического материала, а также проблемам защиты данного материала на веб-ресурсах. Наиболее популярными угрозами являются:

использование команды Printscreen;

сохранение изображения при помощи контекстного меню браузера;

открытый или завуалированный путь к изображению в исходном html-коде;

непосредственный доступ к изображению на сервере.

Далее будут рассмотрены основные способы защиты графического материала, которые сегодня используются на веб-ресурсах.

Существующие методы защиты графической информации на веб-ресурсах

Метод защиты изображений при помощи водяного знака

Самым распространенным и действенным методом от нежелательного использования изображений является наложение водяного знака. Данный способ является самым простым и может быть реализован при помощи:

• графических редакторов – начиная со встроенного в ОС Windows редактора Paint, заканчивая специально разработанным плагином для Photoshop под названием Digimark. Данный способ требует ручного редактирования изображений и не является эффективным при достаточно большом количестве изображений;

• серверных скриптов, которые в online-режиме накладывают водяной знак на исходное графическое изображение и отправляют данное изображение пользователю.

При этом водяные знаки принимают различные формы (рис. 1 – рис. 3).

На рисунке 1 показано изображение, которое для защиты использует водяной знак крупного размера. Пользователь, который скопирует себе подобное изображение, вряд ли сможет без весомого ущерба устранить его. Преимуществом данного метода является практически абсолютная защита от дальнейшего распространения. Недостаток метода заключается в том, что подобные знаки отвлекают внимание пользователя от сути изображения и мешают его работе с материалом.

Рисунок 1 – Прозрачный водяной знак

На рисунке 2 показано изображение, которое использует водяные знаки малого размера, размещаемые в углу изображения. Подобный способ защиты менее бросок, однако его недостаток заключается в том, что от него легко можно избавиться путем кадрирования изображения. При этом само изображение в большинстве случаев смысла не теряет.

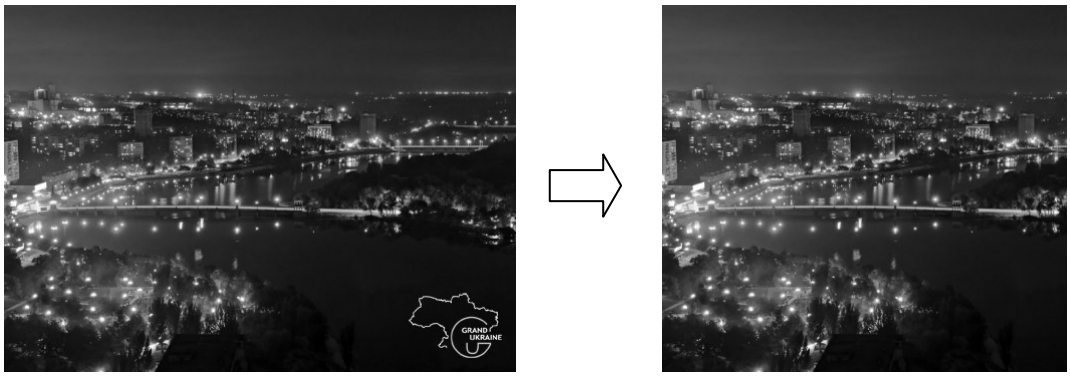

Рисунок 2 – Кадрирование изображения с целью удаления водяного знака

На рисунке 3 показан способ защиты графического материала путем наложения полупрозрачных клеток на исходное изображение. Данный способ защиты является наиболее эффективным ввиду того, что на нем не акцентируется внимание пользователя, а также в силу того, что убрать такой водяной знак достаточно трудоемко. Недостатком данного способа является искажение графического материала.

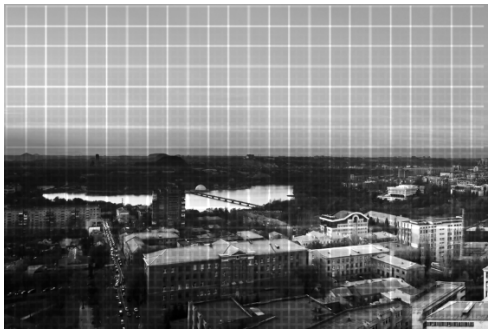

Рисунок 3 – Водяной знак, оставляющий полупрозрачные клетки на изображении

Указанный метод защиты изображений в ряде случаев не является достаточно эффективным ввиду возможного удаления водяного знака без потери смысла изображения.

Кроме того, наличие водяного знака отвлекает внимание пользователя и мешают его работе с материалом.

Метод защиты изображений при помощи сокрытия части изображения

Одним из методов защиты изображения является метод сокрытия части изображения. Данный метод основан на уменьшении размеров контейнера, в который помещается изображение на величину копирайта [1].

Рисунок 4 – Сокрытие части изображения

Наиболее типичный способ реализации указанного метода заключается в изменении размеров контейнера таким образом, чтобы изображение кадрировалось на величину копирайта. Это можно сделать при помощи следующего html-кода:

```
<div style="height:330px; width:500px; overflow:hidden;">
        <img src="image.jpg" width="500" height="400" />
</div>
```

Достоинством данного метода является то, что он не искажает графический материал, а недостатком – низкая эффективность подобной защиты.

Метод защиты изображений при помощи расслоения изображения

Данный метод защиты графического материала заключается в разбиении исходного изображения на несколько частей, которые при наложении друг на друга формируют конечное изображение [2]. При сохранении подобного изображения, у пользователя окажется сохраненной только его часть, либо прозрачный рисунок. Подобный метод реализуется при помощи следующего html-кода:

```
<div style=`background-image: url(image_part1.png)`>
        <div style=`background-image: url(image_part2.png)`>
                <div style=`background-image: url(image_part3.png)`>
                        <img src=`opacity.png`>
                </div>
        </div>
</div>
```

Ввиду того, что CSS 3.0 позволяет оперировать с несколькими фоновыми изображениями одновременно, для реализации указанного метода может быть использован только один контейнер, как показано в html-коде ниже:

```
<div style=`background-image: url(image_part1.png) url(image_part2.png) … `>
```

<img src=`opacity.png`>

Изображения image_part1 – image_partN могут быть получены автоматически из исходного изображения при помощи серверных скриптов (PHP, Python и др.).

Метод защиты графических данных путем разрезания изображения на части

Суть данного метода состоит в том, что изображение разрезается на множество блоков, как показано на рисунках 5 – 6. Каждый блок выводится в отдельной ячейке таблицы. Данный метод можно реализовать как вручную, так и при помощи специальных программных продуктов. Например, в Ulead PhotoImpact, можно разрезать изображение на нужное количество частей и сохранить результат в HTML.

Рисунок 5 – Исходное изображение

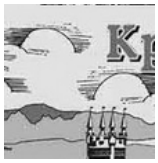

Рисунок 6 – Сохранение фрагмента изображения при помощи контекстного меню браузера

В случае применения данного метода защиты графических данных пользователю придется объединять все сохраненные фрагменты в единое изображение при помощи графических редакторов, на что затрачивается время. Недостатком данной технологии является слишком большое количество запросов на сервер, что в свою очередь может привести к замедлению загрузки страницы.

Следовательно, любой из перечисленных методов защиты от копирования изображений, не дает гарантированного результата. Кроме вышеперечисленных методов рекомендуется выкладывать изображения с низким или средним разрешением (около 72 пикс/дюйм). Изображения подобного качества не могут быть использованы для полноценной печати [3].

Анализ существующих методов с точки зрения угроз

В таблице 1 показаны результаты анализа, иллюстрирующие сопротивление вышеперечисленных методов защиты изображений существующим угрозам.

Таблица 1 Сопротивление различных методов защиты существующим угрозам

Методы защиты / Угрозы	1	2	3	4
Метод защиты изображений при помощи водяного знака	±	±	–	–
Метод защиты изображений при помощи сокрытия части изображения	–	±	–	–
Метод защиты изображений при помощи расслоения изображения	–	+	±	–
Метод защиты изображений при помощи разрезания изображения на части	–	+	±	–

Обозначения: 1 – использование команды Printscreen; 2 – сохранение изображения при помощи контекстного меню браузера; 3 – открытый или завуалированный путь к изображению в исходном html-коде; 4 – непосредственный доступ к изображению на сервере.

Анализ таблицы 1 показывает, что рассмотренные методы защиты в большинстве случаев являются малоэффективными и не покрывают весь спектр существующих угроз.

Предлагаемый метод защиты графической информации на веб-ресурсах

По результатам проведенного анализа угроз и методов защиты был разработан новый метод защиты изображений на веб-ресурсах от несанкционированного копирования.

Данный метод реализуется с помощью технологии «canvas», которая доступна в HTML, начиная с версии 5.0. В большинстве современных браузеров указанная технология поддерживается на настоящий момент.

На первом этапе изображение разделяется на части. В элементе «canvas» при помощи JavaScript в каждый момент времени отображается только половина исходного изображения.

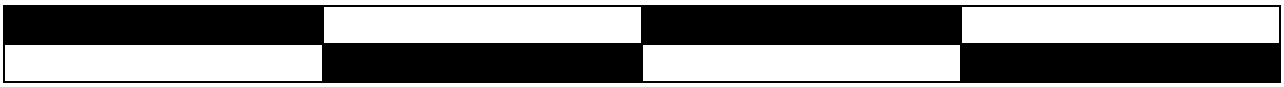

Рисунок 7 – Отображение частей изображения

На рисунке 7 черным цветом показаны части изображения, которые отображаются сразу при загрузке веб-страницы. Через 1/25 долю секунды отображаются элементы, отмеченные белым цветом. Установлено, что человеческий глаз не замечает смены изображений с частотой более 20 кадров в секунду, поэтому графическое изображение кажется цельным. В то же время команда PrintScreen не сможет скопировать видимое изображение с экрана, а сохранит только его четную или нечетную часть в зависимости от момента времени. Также при помещении изображения в элемент «canvas», оно становится защищенным от сохранения через контекстное меню браузера.

Итак, главным преимуществом данного метода является защита от команды PrintScreen, от которой ранее рассмотренные методы не давали полной защиты. Если предложенных средств защиты будет недостаточно, есть возможность хранить графические файлы на сервере в бинарных полях соответствующих таблиц базы данных. Достоинством предлагаемого метода является относительная простота реализации и отсутствие видимых признаков защиты.

Выводы

В данной работе проведен сравнительный анализ существующих методов защиты графического материала, размещаемого на веб-ресурсах. Показано, что данные методы в большинстве случаев являются малоэффективными и не покрывают весь спектр существующих угроз. Также предложен собственный метод защиты изображений, основанный на особенностях восприятия изображения глазом человека.

Список литературы

1. Защита данных на веб-сайтах от копирования / Интернет-ресурс. - Режим доступа: www/ URL: http://webmastak.com/article.aspx?id=25
2. SoftKey.info: Статьи - Простейшая защита от копирования изображений / Интернет-ресурс. - Режим доступа: www/ URL: http://softkey.info/reviews/review.php?ID=581&referer1=softkey_info&compid=1
3. HTML форум RSS лента/ Интернет-ресурс. - Режим доступа: www/ URL:
4. http://www.html.by/threads/7420-Zaschita-sajta-ot-kopirovanija-informacii-i-mnogoe-dugoe