Применение цифровых водяных знаков для защиты цифровых фотографий

Ю.А. Грачёва
Московский государственный университет печати,
кафедра "Медиасистемы и технологии"
J_grachjova@mail.ru

В настоящее время в связи с развитием глобальных сетей большую важность приобретает задача защиты фотографий от незаконного тиражирования. Много исследований посвящено использованию стеганографии в качестве защиты графической информации.

Стеганография – это наука о скрытой передаче информации путём сохранения в тайне самого факта её передачи. К примеру, в цифровое изображение можно встроить некое сообщение, позволяющее идентифицировать автора этого изображения. Такое цифровое изображение со встроенной в него информацией называется ***стегосистемой***, а исходное изображение – ***контейнером*** или ***стегоконтейнером***.

К методам цифровой стеганографии при создании стегосистемы применяются такие требования как ***робастность*** (устойчивость скрытой информации к различного рода искажениям), ***прозрачность*** (отсутствие различий между исходным и модифицированным изображениями), ***устойчивость к атакам*** (попыткам удаления или искажения встроенного сообщения), а также ***секретность маркировки***.

В чём же удобство защиты изображений с помощью стеганографии?

Во-первых, у такого контейнера, как изображение, заранее известен размер, а значит, становится проще подобрать нужный объём встраиваемой информации. Во-вторых, у цифровых изображений относительно большой объём их представления, что позволяет повышать робастность внедрения скрытой информации. Также в фотографиях зачастую присутствуют зашумлённые текстурные области, удобные для встраивания сообщений, и при этом человеческий глаз обладает слабой чувствительностью к незначительным изменениям цветности, яркости, контрастности и шума в изображениях.

В настоящее время существует много методов цифровой обработки изображений, но это усложняет задачу обеспечения робастности информации: чем более совершенны методы сжатия изображений, тем труднее будет задача внедрения посторонних сообщений.

Наиболее востребованный для защиты авторских прав на фотоизображение метод стеганографии – это встраивание так называемых цифровых водяных знаков (ЦВЗ), настроенный на внедрение в мультимедийный файл скрытых маркеров, устойчивых к различным атакам. Встроенные ЦВЗ анализируются специальным декодером, выносящим решение об их корректности. В качестве ЦВЗ могут использоваться данные автора или аутентичный код, а также какая-нибудь управляющая информация.

До встраивания информации в изображение в качестве ЦВЗ необходимо преобразовать её к подходящему виду, то есть в двумерный массив бит. Также обычно применяют помехоустойчивое кодирование или широкополосные сигналы для повышения устойчивости ЦВЗ к искажению. Важнейшая предварительная обработка скрытого сообщения и контейнера – это вычисление их обобщенного преобразования Фурье, что позволяет реализовать встраивание ЦВЗ в спектральной области для повышения его устойчивости к искажениям. При предварительной обработке сообщений часто применяют ключи с целью повышения секретности встраивания информации. Следующий этап – это уже непосредственно внедрение ЦВЗ в изображение, часто с использованием так называемого ***стегоключа*** (псевдослучайной последовательности бит, полученной от определенного генератора). Незаметность ЦВЗ возможна благодаря большой психовизуальной избыточности изображений для системы восприятия человека.

Наиболее распространённый метод встраивания начинается с выбора ***стегопутей***, то есть бит контейнера, которые можно модифицировать без заметных искажений, после чего с помощью ключа из них выбираются биты, заменяемые битами сообщения. Обычно применяют такие методы, как инверсия, вставка или удаление бита, а также использование пороговых бит или различных таблиц значений.

Выделение скрытого в защищаемом изображении ЦВЗ происходит в стегодетекторе с помощью стегоключа, использованного при внедрении информации. Этот ключ может быть как общедоступным, так и предназначенным для узкого круга лиц. Если он общедоступен, то такой стегосистеме сложно противостоять возможным атакам со стороны злоумышленников. Кроме того, само защищаемое изображение может быть изменённым, например, из-за атак на него или операций обработки сигнала. Результатом таких модификаций и атак становится невозможность обнаружения ЦВЗ в стегодетекторе, поэтому учёт этих факторов позволяет строить более эффективные защитные стегосистемы.

Стегодетекторы делятся на две категории. Одни из них предназначены для обнаружения наличия ЦВЗ, другие – для его выделения (такие детекторы называются стегодекодерами). В свою очередь, ЦВЗ-стегосистемы делятся на три класса: открытые, полузакрытые и закрытые (имеющие наибольшую устойчивость к внешним воздействиям). Соответственно, для защиты изображений от незаконного использования лучше всего использовать ***закрытые*** стегосистемы.

ЦВЗ бывают трёх типов: хрупкие, полухрупкие и робастные. Хрупкие ЦВЗ обычно разрушаются при изменении стегоконтейнера и применяются для аутентификации сигналов. Робастные ЦВЗ устойчивы к различным видам воздействия на контейнер, поэтому именно этому типу меток посвящено множество разработок. Полухрупкие ЦВЗ обычно бывают стойкими к одному виду воздействий, но неустойчивыми по отношению к другим. Строго говоря, робастные ЦВЗ тоже можно отнести к полухрупким, поскольку абсолютной устойчивости меток добиться очень сложно. Для защиты цифровых фотографий лучше использовать робастные ЦВЗ, поскольку у изображений могут быть отредактированы такие параметры, как цветовая гамма, яркость, оно может быть отмасштабировано или повёрнуто. Кроме того, такие ЦВЗ должны обнаруживаться только одной стороной, чтобы злоумышленник не мог их выделить и уничтожить.

Вполне логично, что защищённая ЦВЗ фотография должна быть визуально неотличима от исходной. Проще всего встраивать информацию в незначащие биты изображения (LSB-метод), поскольку модификация младших битов в большинстве случаев не вызывает значительной трансформации изображения и не обнаруживается

визуально. Но поскольку эти же области используются алгоритмами сжатия, то при такого рода деформации ЦВЗ будет разрушаться.

Существуют стегосистемы, в которых разделены этапы обнаружения и аутентификации, в результате чего ЦВЗ легко обнаруживается, но удалить его непросто. Такие системы строятся на основе ЦВЗ с нулевым знанием и вполне могут быть использованы для защиты цифровых фотографий.

Современный подход к защите цифровых фотографий с использованием ЦВЗ заключается во встраивании информации в те области изображения, разрушение которых приведёт к его необратимой порче. При этом стегоалгоритмы учитывают как сжатие изображений, так и свойства человеческого зрения.

На стегосистему с использованием ЦВЗ могут быть направлены следующие атаки:

- направленные на модификацию изображения-контейнера;
- направленные на уничтожение ЦВЗ;
- криптографические;
- против протокола встраивания и проверки ЦВЗ.

Атаки, направленные на уничтожение ЦВЗ – это атаки, основанные на том предположении, что эти метки являются статистически описываемым шумом. К этой группе атак относятся перемодуляция, квантование, а также коллизии, усреднение и просто очистка изображения от шумов. Атаки, направленные на модификацию изображения, ЦВЗ не удаляют, но изменяют его с помощью временных искажений или аффинных преобразований, которые бывают локальными и глобальными. Криптографические атаки на ЦВЗ имеют аналоги в криптографии и обычно требуют наличия детектора. К атакам против используемого протокола относится так называемая инверсная атака, при которой нарушитель заявляет, что в защищённом изображении есть его ЦВЗ, после чего создаёт ложный оригинал с вычитанием этой части данных. Ситуация становится спорной, и не всегда разрешимой даже при наличии исходной фотографии.

Обеспечение робастности к некоторым видам атак, например, к глобальным аффинным преобразованиям, уже давно является решённой задачей, вопросы же защиты от других атак до сих пор остаются открытыми.

В стегоалгоритмах обычно используются преобразования, свойственные современным алгоритмам сжатия. Поскольку основными форматами выкладываемых во всемирную сеть фотографий являются JPEG и JPEG2000, то для защиты этих изображений используются соответственно дискретное косинусное преобразование (ДКП) и вейвлет-преобразование.

Если для защиты информации используется тот же алгоритм, что и для его сжатия, то такой стегоалгоритм будет робастным по отношению к дальнейшей компрессии. И, соответственно, ЦВЗ, созданный с использованием ДКП, не обязательно будет робастным по отношению к вейвлет-сжатию, и наоборот.

Если речь идёт о формате JPEG, то защищаемая фотография первоначально разбивается на блоки 8x8 элементов, к каждому из которых применяется ДКП. Назначением ДКП является осуществление перераспределения энергии: значимые коэффициенты группируются в левом верхнем углу квадрата спектральных коэффициентов, в то же время соседние пиксели изображения будут коррелированы. После этого происходит равномерное табличное квантование коэффициентов, кодирование длин серий и кодирование Хаффмана. Вейвлет-преобразование тоже перераспределяет энергию изображения. Компактность энергии ведет к эффективному применению скалярных квантователей, но они не учитывают сохраняющуюся в вейвлет-коэффициентах остаточную структуру. Современные алгоритмы сжатия все тем или иным образом используют эту структуру высокочастотных субполос для повышения эффективности сжатия.

Список литературы

1. *Гаврилов. Э.П.* Комментарий к Закону Российской Федерации "Об авторском праве и смежных правах". М.: Издательство "Спарк", Фонд "Правовая культура", 1996 г.
2. *Липкес А.М.* Право интеллектуальной собственности. М.: Издательство РИОР, 2006 г.
3. Википедия. http://ru.wikipedia.org
4. *Генне О. В.* Основные положения стеганографии. "Защита информации. Конфидент", №3, 2000 г.
5. *Барсуков В.С., Романцов А.П.* Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века. "Специальная Техника" №4-5 1998 г.
6. *Барсуков В.С., Шувалов А.В.* Ещё раз о стеганографии – самой современной из древнейших наук. "Специальная Техника" №2, 2004 г.
7. *Ю.А. Грачёва* Несколько слов о стеганографии – методе защиты графической информации от нарушения авторских прав.
8. *А.А. Хотов* Цифровые водяные знаки. Автореферат.
9. *Г.Ф. Коханович, Ю.А. Пузыренко* Компьютерная стеганография. Теория и практика. Киев, 2006 г.
10. *А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников* Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009 г.