С. 102-111.

6. Кузнецов А.А., Евсеев СП. Разработка теоретико-кодовых схем с использованием эллиптических кодов. // Системи обробки шформацп. - Харюв: ХВУ. -2004 - Вип. 5. - С 127-132.

7. Евсеев СП. Несимметричные криптосистемы на ЭК для каналов с автоматическим переспросом. // Збірник наукових праць ХУ ПС. - Харків: ХУПС. - 2007. - Вип. 5 (63). - С 134-137.

8. Евсеев СП. Криптографическое преобразование информации в кодовых криптосистемах на эллиптических кодах для каналов с автоматическим переспросом. // Збірник наукових праць ХУ ПС - Харків: ХУПС. - 2007. - Вип. 8 (66).-С. 29-32.

Надійшла 3.12.2007р.

УДК 004.7.056.5

Нетров А.С., Минин А.В.

ОСОБЕННОСТИ ОПТИМИЗАЦИИ СТЕГОАЛГОРИТМОВ ДЛЯ ВИДЕОКОНТЕЙНЕРА

Прогресс в области компьютерной стеганографии позволяет сильно изменить существующие подходы к проблеме информационной безопасности. В связи с этим актуальной является задача построения цифровых контейнеров, в которых можно скрывать данные, не подлежащие огласке. Каждый месяц появляются новые стегоалгоритмы и алгоритмы стегоанализа. На данном этапе основное внимание в стеганографии уделено цифровым статическим изображениям и цифровым аудиофайлам. Методы стеганографии для встраивания скрытой информации в видеофайлы в настоящее время пока еще находятся на стадии исследований и носят фрагментарный характер.

Информационная последовательность, в которую встраивается сообщение, принято называть контейнером. В нашем случае это видеоконтейнер. Пока видеофайл не попал в стегокодер - это пустой видеоконтейнер, после стегокодера - заполненный видеоконтейнер, или стегофайл. Стегофайл должен быть визуально неотличим от пустого видеоконтейнера. Различают два основных типа видеоконтейнеров: потоковый и фиксированный.

Потоковый видеоконтейнер представляет собой непрерывно следующую последовательность бит. Сообщение вкладывается в него в реальном масштабе времени, так что стегокодеру заранее неизвестно, поместится все сообщение в видеоконтейнер или нет. В один видеоконтейнер большого размера может быть встроено и несколько сообщений. Интервалы между встраиваемыми битами определяются генератором псевдослучайной последовательности с равномерным распределением интервалов между отсчетами. Основная трудность заключается в осуществлении синхронизации, определении начала и конца последовательности. Если в данных контейнера имеются биты синхронизации, заголовки пакетов и т.д., то скрываемая информация может располагаться сразу после них. Трудность обеспечения синхронизации превращается в достоинство с точки зрения обеспечения скрытности передачи. На практике востребованность стегоалоритмов для работы с потоковым видеоконтейнером очевидна: представьте себе, например, стегоприставку к обычному компьютеру или мобильному телефону с встроенной веб-камерой. Вы проводите веб-конференцию или видеозвонок, разговариваете на отвлеченные темы, а параллельно передаете секретную информацию. Не удивительно, что работ в этом направлении практически не встречается.

У фиксированного видеоконтейнера размеры и характеристики заранее известны. Это позволяет осуществлять вложение с оптимальным результатом.

Видеоконтейнер может быть выбранным, случайным или навязанным.

Выбранный видеоконтейнер зависит от встраиваемого сообщения, а в предельном случае является его функцией. Этот тип видеоконтейнера больше характерен для стеганографии.

Навязанный видеоконтейнер может появиться в сценарии, когда лицо, предоставляющее видеоконтейнер, подозревает о возможной скрытой переписке и желает предотвратить ее.

На практике же чаще всего сталкиваются со случайным видеоконтейнером.

Для того, чтобы обеспечить надежность стегосистемы, на этапе её создания надо придерживаться определенных требований [5]:

- Безопасность системы должна полностью определяться секретностью ключа. Это означает, что нарушитель может полностью знать все алгоритмы работы стегосистемы, и это не даст ему никакой дополнительной информации о наличии или отсутствии сообщения в данном видеоконтейнере.
- Знание нарушителем факта наличия сообщения в каком-либо видеоконтейнере не должно помочь ему при обнаружении сообщений в других видеоконтейнерах.
- Заполненный видеоконтейнер должен быть визуально неотличим от незаполненного. Для удовлетворения этого требования надо, казалось бы, внедрять скрытое сообщение в визуально незначимые области сигнала. Однако, эти же области используют и алгоритмы сжатия. Поэтому, если видеоконтейнер будет в дальнейшем подвергаться сжатию, то скрытое сообщение может разрушиться. Следовательно, биты должны встраиваться в визуально значимые области, а относительная незаметность может быть достигнута за счет использования специальных методов, например, модуляции с расширением спектра.
- Стегосистема должна иметь низкую вероятность ложного обнаружения стего в сигнале, его не содержащем.

Стегосистема должна иметь приемлемую вычислительную сложность. При этом возможна асимметричная система, то есть сложный стегокодер и простой стегодекодер.На данный момент работать с видеофайлами можно на многих домашних ПК. Но процесс встраивания информации в видео поток требует больших машинных ресурсов, поэтому программные продукты стеганографии для работы с видео требуют постоянной оптимизации.

Одним из важных критериев, влияющих скорость работы стегоалгаритма, является правильный выбор формата видеофайла используемого в качестве контейнера. Понятно что этот файл должен быть широко распространенного формата, чтобы не привлекать к себе внимания своей экзотичностью. В настоящее время для видеосжатия применяется наиболее распространенный формат DivX, использующий стандарт видеосжатия MPEG-4.

Он состоит из трех видов кадров:

I-фремы - это кадры, закодированные как неподвижные изображения - без ссылок на последующие или предыдущие. Они используются как стартовые.

P-фреймы - это кадры, предсказанные из предыдущих I- или P-кадров. Каждый макроблок в P-фрейме может идти с вектором и разностью коэффициентов ДКП от соответствующего блока последнего раскодированного I или P, или может быть закодирован как в I, если соответствующего блока не нашлось.

И, наконец, существуют B-фреймы, которые предсказаны из двух ближайших I или P-фреймов, одного предыдущего и другого - последующего. Соответствующие блоки ищутся в этих кадрах и из них выбирается лучший. Ищется прямой вектор, затем обратный и вычисляется среднее между соответствующими макроблоками в прошлом и будущем. Если это не работает, то блок может быть закодирован как в I-фрейме [4].

В качестве контейнера предлагается использовать стандарт видеосжатия MPEG для видео конференций. В этом стандарте качество изображения низкое, поэтому при работе с опорными кадрами визуально качество картинки не изменится.

С целью оптимизации работы стегоалгоритма предлагается использовать генератор псевдослучайной последовательности, для выбора I-кадров, в которые будет встраиваться информация, из цепочки этих кадров в случайной последовательности, с низкими системными требованиями, но высокой степенью случайности.

Есть два основных типа генераторов, для производства псевдослучайных последовательностей: генераторы случайных чисел RNGs, и генераторы псевдослучайных чисел PRNGs. Для криптографических приложений, оба из этих типов генераторов производят поток нулей и единиц, которые могут быть разделены на подпотоки или блоки случайных чисел. [3]

Первый тип генератора последовательности - генератор случайных чисел (RNG). RNG использует недетерминированный источник (то есть, источник энтропии), наряду с некоторой функцией обработки (то есть, процесс дистилляции энтропии), чтобы произвести случайность. Использование процесса дистилляции необходимо, чтобы избежать любую слабость в источнике энтропии, которая приводит к получению неслучайных чисел (например, возникновение длинных строк нулей или единиц). Источник энтропии типично состоит из некоторых физических величин, типа шума в электрической схеме, выбора времени, пользовательских процессов (например, нажатия клавиш или движения мыши), или квантовых эффектов в полупроводниках. Могут использоваться различные комбинации этих источников. Кроме того, генерация высококачественных случайных чисел может быть слишком трудоёмкой, делая эту процедуру нежелательной, когда необходимо большое количество случайных чисел. Чтобы производить большие количества случайных чисел, псевдослучайные генераторы могут быть предпочтительнее.

Второй тип генераторов - псевдослучайный генератор (PRNG). Для получения множества псевдослучайных чисел PRNG использует один или более входящих начальных значения.

В контексте, в котором непредсказуемость необходима, само начальное число должно быть случайно и непредсказуемо. Следовательно, по умолчанию, PRNG должен получить начальное число от выводов RNG; то есть, PRNG требует RNG как компаньона [3].

Как ни странно, псевдослучайные числа часто кажутся более случайными, чем случайные, полученные из физических источников. Если псевдослучайная последовательность должным образом сформирована, каждое значение в последовательности произведено от предыдущего значения через преобразования, которые вводят дополнительную случайность. Ряд таких преобразований может устранить статистическую автокорреляцию между начальным значением и полученным результатом. Таким образом, последовательности PRNG могут иметь лучшие статистические свойства и могут генерироваться быстрее, чем RNG. Их достоинствами являются колоссальный период (2^{19937}-1), равномерное распределение в 623 измерениях (линейный конгруэнтный метод даёт более или менее равномерное распределение от силы в 5 измерениях), быстрая генерация случайных чисел (в 2-3 раза быстрее, чем стандартные RNGs, использующие линейный конгруэнтный метод).

При оптимизации важное место занимает метод встраивания информации.

В большинстве методов встраивания информации в изображения используется та или иная декомпозиция изображения - контейнера. Среди всех линейных ортогональных преобразований наибольшую популярность в стеганографии получили вейвлет-преобразование и ДКП, что отчасти объясняется их успешным применением при сжатии изображений. Кроме того, желательно применять для скрытия данных то же преобразование изображения, как и то, которому оно подвергнется при возможном дальнейшем сжатии. В стандарте JPEG используется ДКП, а в JPEG2000 - вейвлет-преобразование. Стегоалгоритм может быть весьма робастным к дальнейшей

компрессии изображения, если он будет учитывать особенности алгоритма сжатия. При этом, конечно стегоалгоритм, использующий ДКП, вовсе не обязательно будет робастным по отношению к вейвлетному алгоритму сжатию. Стегоалгоритм, использующий вейвлеты, может быть неробастным к сжатию с применением вейвлетов.

Еще большие трудности возникают с выбором преобразования при скрытии данных в потоковой видеопоследовательности. Причина заключается в том, что при сжатии видео основную роль играет кодирование векторов компенсации движения, а не только неподвижного кадра. Робастный стегоалгоритм должен учитывать это.

Предлагается использовать метод встраивания информации за счет энергетической разности между коэффициентами. Сущность этого метода состоит в том, что внедрение битов информации происходит в области I-того кадра. I кадр разбивается на блоки 8*8 коэффициентов дискретного косинусного преобразования (ДКП). [2]

Изображение представляется в формате YUV, то есть одним каналом яркости и двумя каналам цветности. Изображение в канале яркости – это, по существу, черно-белое изображение. Известно, что зрительная система человека более чувствительна к изменениям в канале яркости, нежели в каналах цветности. Поэтому компоненты U и V могут быть подвергнуты большему сжатию, чем Y.

Каждый компонент I-кадра разбивается на блоки 8*8 пикселов, затем каждый блок подвергается дискретному косинусному преобразованию (ДКП).

После ДКП в каждую ячейку блока вместо значения яркости (цветности) ставится коэффициент ДКП. Таким образом, получается двумерный энергетический спектр участка изображения. Энергетический спектр изображения обычно сосредотачивается в низкочастотных коэффициентах. Чем меньше отличаются друг от друга значения соседних пикселов, тем ближе к нулю значения более высокочастотных коэффициентов ДКП. Коэффициенты ДКП квантуются.[1]

ДКП концентрирует энергию в области низких частот, а, так как человеческий глаз менее чувствителен к высокочастотным колебаниям, то ВЧ компоненты могут быть оцифрованы более грубо. Коэффициент ДКП с индексом (0,0) называется DC-коэффициентом (постоянного тока), и он представляет среднее значение по блоку пикселов. Другие коэффициенты ДКП называются AC-коэффициентами (переменного тока).

Бит сообщения внедряется в выбранную область модификацией разности энергий D между высокочастотными коэффициентами ДКП верхней части этой области (субобласть A) и ее нижней части (субобласть B). Подмножество ВЧ коэффициентов обозначается S(c).

Энергия субобласти A вычисляется по формуле [1]

$$E_A(c,n,Q) = \sum_{d=0}^{n/2-1} \sum_{i \in S(c)} \left(\left[\theta_{i,d} \right]_Q \right)^2,$$

где $\theta_{i,d}$ - коэффициент ДКП с индексом i из d-го блока коэффициентов ДКП субобласти A; $[\,]_Q$ - означает, что энергия вычисляется у квантованных коэффициентов.

Энергия субобласти B вычисляется аналогичным способом.

Подмножество S(c) определяется на основе выбранного порога [1]

$$S(s) = \{h \in \{1,63\} \mid (h \geq c)\}$$

Выбор подходящего значения порога крайне важен, так как этим определяется стойкость стегоалгоритма. Когда порог для каждой области определен, разность энергий определяется следующим образом:

$$D(c,n,Q) = E_A(c,n,Q) - E_B(c,n,Q)$$

Значение внедряемого бита определяет знак энергетической разности. Если значение бита "0" то D > 0, в противном случае D < 0. Следовательно, процедура встраивания

информации модифицирует энергии E_A или E_B , чтобы встроить информацию в разность энергий D. Если встраивается нуль, то в блоках по 8*8 коэффициентов субобласти B после пороговой обработки энергия будет удалена, а коэффициенты ДКП приравнены нулю так, что [1]

$$D = E_A - E_B = E_A - 0 = +E_A$$

Если встраивается единица, то высокочастотные коэффициенты ДКП в субобласти A приравниваются нулю [1]

$$D = E_A - E_B = 0 - E_B = -E_B$$

Как правило, метод встраивания информации за счет энергетической разности между коэффициентами является более устойчивым, чем битовые технологии, тем не менее существует выбор между количеством скрытой информации и достигаемой устойчивостью. Также этот метод может устоять при переводе из форматов без потерь в форматы с потерями, при записи на аналоговые носители.

А для того чтобы увеличить объем встраиваемой информации, в видеофайле можно использовать и аудиосигнал, с применением метода внедрение информации модификацией фазы аудиосигнала [1]. Внедрение информации модификацией фазы аудиосигнала – это метод, при котором фаза начального сегмента аудиосигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз. Это необходимо потому, что к разности фаз человеческое ухо более чувствительно. Фазовое кодирование, когда оно может быть применено, является одним из наиболее эффективных способов кодирования по критерию отношения сигнал-шум [6].

В данной статье приведены лишь некоторые особенности по оптимизации стегоалгоритмов для видеоконтейнеров. В настоящее время нами выполнены разработки в этом направлении и накоплена статистика по результатам внедрения различных методов и алгоритмов в стегопродукты. В результате этих работ получен стойкий и не требующий больших машинных ресурсов стегоалгоритм для работы с потоковым видео.

Список литературы

1. *Грибунин В.Г.* и др. Цифровая стеганография. М.: СОЛОН-Пресс, 2002.

2. *Петров А.С., Минин А.В., Струнина В.Н.* «Разработка программы для встраивания данных в видеопоток»// Вісник Східноукраїнського національного університету ім. В. Даля, №5 (111), 2007, Ч. 1. – с.270

3. *Валуйский Е.А., Петров А.С.* «Программный пакет NIST STATISTICAL TEST SUITE. Стратегия тестирования и интерпретация результатов»// Вісник Східноукраїнського національного університету ім. В. Даля, №9 (103), 2006 – с.284

4. www.elecard.com

5. www.autex.spb.ru

6. *Конахович Г.Ф.* Компьютерная стеганография. Теория и практика, К.: МК-Пресс, 2006.

Надійшла 11.12.2007р.