Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Матюшик
Виталий Николаевич

Методы и средства стеганографии для защиты графических образов

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный уководитель
Ярмолик В.Н.
д.т.н., профессор

Минск 2014

Библиотека БГУИР

ВВЕДЕНИЕ

В современном обществе информация является одним из ценнейших предметов, поскольку благодаря развитию технологий она стала широкодоступной, а легкость доступа значительно повысила угрозу нарушения безопасности данных при отсутствии мер относительно их защиты. Для защиты информации уже придумано множество методов и алгоритмов, которые можно отнести к одному из двух направлений: криптография, стеганография.

Скрытие самого факта существования секретных данных при их передаче или обработке является задачей стеганографии – науки, изучающей способы и методы скрытия конфиденциальных сведений. Под скрытием существования информации подразумевается невозможность возникновения любых подозрений на наличие скрытых данных в контейнере.

Исторически направление стеганографического скрытия информации предшествовало криптографии. Однако со временем исследования в области стеганографии значительно сократились, и данная наука во многих сферах была вытеснена криптографией. Интерес возродился лишь в последние десятилетия в связи с распространением мультимедийных технологий и новых типов каналов передачи информации.

На сегодняшний день стеганография является наукой, которая быстро развивается, использую достижения криптографии, цифровой обработки сигналов, теории связи и информации. Существует два ключевых направления использования классической стеганографии: связанное с цифровой обработкой сигналов и не связанное. В первом случае секретное сообщение встраивается в цифровые данные, а во втором – в заголовки файлов или пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и/или уничтожения скрытой информации. Подавляющее большинство текущих исследований в сфере стеганографии так или иначе связано именно с цифровой обработкой сигналов.

На сегодняшний день актуальна научно-техническая проблема усовершенствования алгоритмов и методов проведения стеганографического скрытия конфиденциальных данных или защиты авторских прав на определенную информацию.

Наиболее распространенными типами контейнеров в компьютерной стеганографии на данный момент являются изображения и аудиоданные, представленные в цифровой форме, и видеопоследовательности. Довольно большая доля современных систем компьютерной стеганографии использует в качестве контейнеров растровые графические изображения различных форматов, которые и рассматриваются в данной работе.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является разработка протокола внедрения информации в графический файл для защиты авторских прав на него. Для достижения поставленной цели необходимо решить следующие задачи:

6. Исследование существующих методов внедрения информации в графические образы, классификация внедряемых данных согласно решаемым задачам, анализ цифровых водяных знаков.
7. Детальный анализ атак на стеганографические системы и системы внедрения цифрового водяного знака.
8. Выбор и подробный анализ методов одной из групп с целью разработки протокола внедрения информации, в основе которого лежит наиболее устойчивый к атакам злоумышленника и обладающий наибольшей емкостью внедрения метод.
9. Экспериментальный анализ полученных результатов, выявление недостатков разработанного протокола с целью внесения модификаций в метод внедрения.
10. Определение приоритетных направлений дальнейшей работы.

Объектом исследования являются системы защиты графической информации. *Предметом* исследования являются стеганографические методы внедрения информации в графические образы.

Связь работы с приоритетными направлениями научных исследований

Работа выполнялась в соответствии научно-техническими заданиями и планами работ кафедры «Программное обеспечение информационных технологий», и хозяйственными договорами с предприятиями Республики Беларусь: «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы » (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР – В. В. Бахтизин).

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем путем анализа предметной области и проведение экспериментов. Вклад научного

Библиотека БГУИР

руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Результаты проведенных исследований были представлены на Международной научной конференции «Информационные технологии и системы», III Международной научно-практической конференции «Приоритетные направления развития науки и образования» и Международной заочной научно-практической конференции «Наука, образование, общество: тенденции и перспективы».

Опубликованность результатов диссертации

По теме диссертации опубликовано 3 печатных работ в виде тезисов международных конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников, списка публикаций автора. В первой главе представлен анализ предметной области, выявлены основные аспекты решения поставленной проблемы, приводится анализ существующих методов внедрения информации в наименее значащие биты графического файла, относящихся к выбранной группе алгоритмов. Во второй главе рассматривается наиболее совершенный метод внедрения, который используется для разработки протокола. В третьей главе проводятся эксперименты разработанного протокола с целью сравнения с возможными альтернативными его реализациями, предлагается и апробируется модификация протокола.

Общий объем работы составляет 60 страниц, из которых основного текста – 40 страниц, 37 рисунков, 5 таблиц, список использованных источников из 37 наименований на 3 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

1 Внедрение водяных знаков в статические изображения

Всё множество разработанных методов внедрения водяных знаков в графические изображения можно разделить на 5 групп.

– статистические методы – методы, изменяющие статистические свойства контейнера;

Библиотека БГУИР

– методы, использующие пространство различных преобразований – методы, основывающиеся на описании изображения коэффициентами некоторого преобразования (преобразования Фурье, косинус-преобразования или вейвлет-преобразования);

– методы младшего значащего бита (Least Significant Bit, LSB) – наиболее простые методы, использующие замены наименее значимых бит в байтах контейнера на биты секретного сообщения;

– методы преобразований в частотной области (Transform Domain Techniques) – внедрение секретной информации в частотной области сигнала;

– искажающие методы – методы, основывающиеся на том факте, что получателю известен исходный контейнер и он может отследить модификации отправителя.

В данной работе рассматриваются наиболее популярные методы, относящиеся к группе изменений младшего значащего бита.

2 Встраивание сообщений в незначащие элементы контейнера

2.1 LSB

Метод замены наименее значащего бита наиболее распространен среди методов замены в пространственной области. Достоинствами данного метода являются простота и сравнительно большой объем встраиваемых данных. Однако он имеет серьезные недостатки. Во-первых, скрытое сообщение легко разрушить. Во-вторых, не обеспечена секретность встраивания информации. Для преодоления последнего недостатка было предложено встраивать скрытое сообщение не во все пикселы изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известному только законному пользователю. Пропускная способность при этом значительно уменьшается.

2.2 BPCS

В BPCS графический образ разбивается на битовые плоскости, которые используются в качестве носителя информации для замены сложных областей каждой битовой плоскости на значения, получаемые с помощью определенного шаблона, неразличимые для человеческих глаз.

Алгоритм сокрытия данных согласно BPCS состоит в последовательном

Библиотека БГУИР

выполнении следующих шагов:

– разбиение на битовые плоскости,

– разбиение на блоки,

– вычисление меры сложности каждого блока,

– вычисление меры сложности секретного сообщения,

– замена сложного блока изображения на блок сообщения.

При внедрении используются наиболее сложные области изображения. Для этого чаще всего используют метрику длины черно-белой границы.

Процедура извлечения секретных данных противоположна процедуре внедрения и состоит из следующих шагов:

– разбиение на битовые плоскости,

– разбиение на блоки,

– вычисление меры сложности каждого блока,

– извлечение карты внедрения (содержится в первом шумоподобном блоке),

– извлечение сообщения.

Реализации алгоритма BPCS могут варьироваться в зависимости от следующих параметров:

– встраивание порогового значения $\alpha 0$,

– последовательность внедрения блоков секретного сообщения,

– способ шифрования карты конъюнкций,

– параметры шифрования сообщения,

– параметры сжатия сообщения.

Однако вне зависимости от выбранного варианта реализации алгоритма BPCS в контейнер с высокой долей вероятности будут внесены заметные искажения, которые можно обойти с помощью алгоритма ABCDE.

2.3 ABCDE

ABCDE (A Block Complexity Based Data Embedding) базируется на тех же принципах, что и BPCS, но BPCS использует операцию конъюнкции для преобразования простого блока в сложный, а для выявления сложных блоков – меру длины черно-белой границы. ABCDE использует две метрики для выявления регулярной структуры блока: метрику «неравномерности длин серий» и метрику зашумленности границ. Алгоритм внедрения информации по методу ABCDE включает следующие шаги:

– компрессия исходного сообщения,

– перераспределение пикселов контейнера в поток блоков, составляющих М-последовательность,

Библиотека БГУИР

– установка пороговых значений для мер сложности β и γ для LSB-плоскостей: β_t^π и γ_t^π,

– внедрение ключа М-последовательности,

– формирование заголовочной секции и встраивание ее после конвертирования с помощью MBCS,

– внедрение секций сообщения после конвертирования с помощью MBCS,

– формирование выходного потока из последовательности М-блоков.

Алгоритм извлечения сообщения состоит из следующих шагов:

– перераспределение пикселов контейнера в поток блоков, составляющих М-последовательность,

– извлечение пороговых значений для мер сложности для LSB-плоскостей β_t^π и γ_t^π. Если данные параметры не были встроены, пороги принимают значения по умолчанию,

– извлечение ключа М-последовательности. Если данный ключ не был встроен, его значение в контейнере будет заведомо ложным, т.е. говорящим, что ключ будет во внешнем источнике. По значению ключа восстанавливается М-последовательность,

– извлечение заголовочной секции и извлечение параметров внедрения. К таковым могут относится размер сообщения, размер секции,

– извлечение исходного сообщения.

3 Схема работы с водяным знаком

Для внедрения водяного знака используются следующие параметры, задаваемые пользователем:

– m – число строк в блоке данных (по умолчанию используется значение 8);

– n – число столбцов в блоке данных (по умолчанию используется значение 8);

– r – число бит, внедряемых в блок данных;

– $\beta_t^0 \ldots \beta_t^7$ – пороговые значения неравномерностей длин серий для каждой битовой плоскости (используются значения по умолчанию);

– $\gamma_t^0 \ldots \gamma_t^7$ – пороговые значения зашумлённости границ для каждой битовой плоскости (используются значения по умолчанию).

Внедрение водяного знака состоит из следующих этапов:

– сгенерировать ключ K и матрицу весов W;

– выделить из битовой плоскости блок размерностью $m*n$; если блок является сложным, то внедрить в него r бит; если блок после внедрения данных уже не является сложным, то восстановить исходный блок данных;

– повторить предыдущий шаг для всего внедряемого водяного знака.

Библиотека БГУИР

Обнаружение водяного знака состоит из следующих этапов:

– выделить из битовой плоскости блок размерностью $m*n$; если блок является сложным, то получить r внедрённых бит;

– повторить предыдущий шаг для обнаружения внедрённого водяного знака.

4 Экспериментальная часть

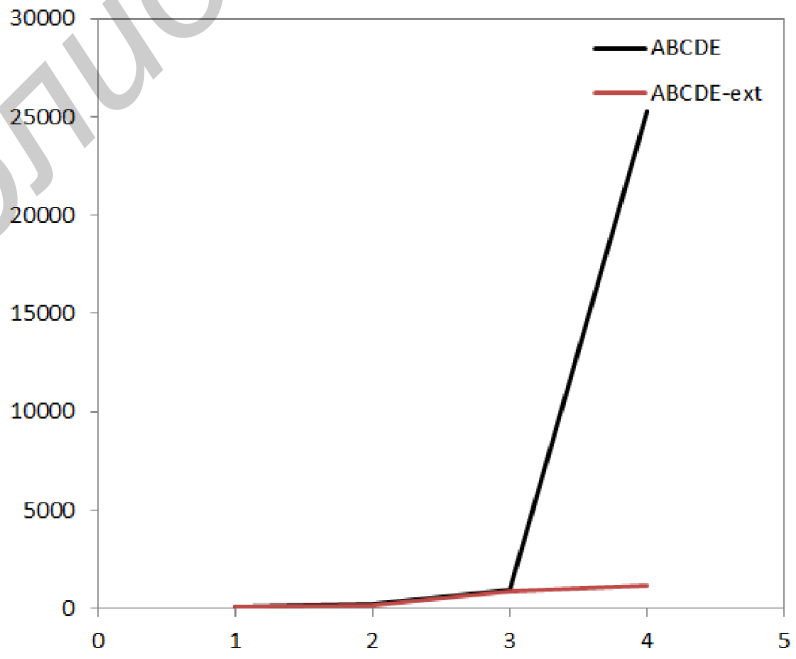
Проведенные эксперименты показали, что BPCS и ABCDE одинаково устойчивы к большинству атак на системы ЦВЗ: их робастность зависит от применяемых контрмер против действий злоумышленников. Но при этом, как было показано в данном разделе, ABCDE обладает большей емкостью внедрения и вносит меньше искажений в изображения, чем BPCS.

Основным недостатком ABCDE является вычислительная сложность операции внедрения данных. Наилучшим решением данной проблемы может быть следующее:

– установить постоянное значение величины k, определяющей размер сегмента, для наименее значащих плоскостей,

– внедрять дополнительный блок в качестве заголовка для каждого сегмента (k блоков потока).

Реализация данного подхода позволила существенно сократить временные затраты на проведение операции внедрения данных (рисунок 1) и не оказала заметного отрицательного воздействия на операцию извлечения данных (рисунок 2).



Библиотека БГУИР

Рисунок 1 – График зависимости времени внедрения от числа плоскостей

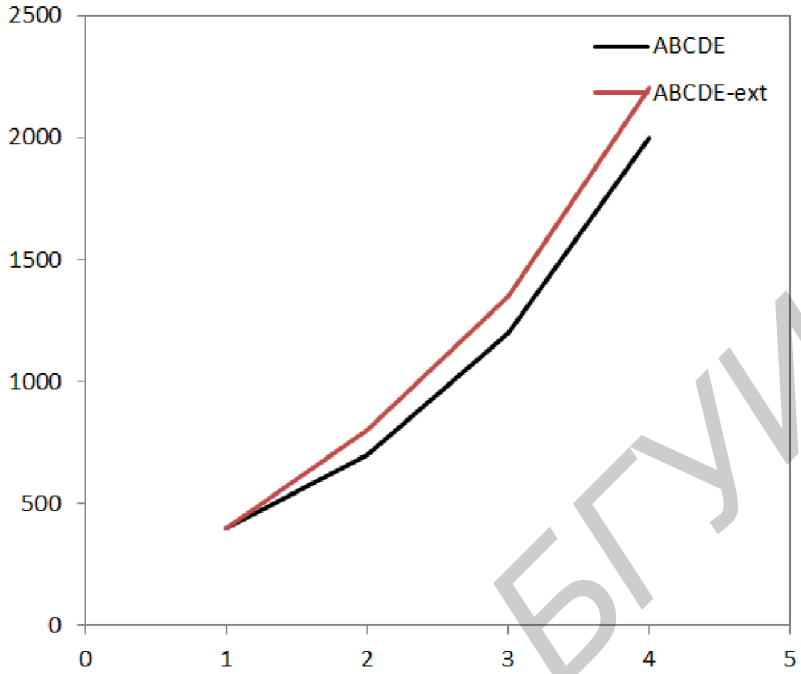


Рисунок 2 – График зависимости времени извлечения от числа плоскостей

ЗАКЛЮЧЕНИЕ

Для достижения поставленной цели исследования было проанализировано развитие стеганографии, проведено сравнение ее с криптографией, а также исследованы приоритетные направления развития данной области науки. С учетом приведенной общей характеристики стеганографии было выбрано одно из наиболее популярных ее направлений – графическая стеганография. Анализ литературных источников в диссертации был сконцентрирован на рассмотрении цифровых водяных знаков, так как именно эта область нацелена на защиту авторских прав.

В работе были рассмотрены методы наиболее популярной группы внедрения водяных знаков – группы изменений младшего значащего бита:

– LSB

Наиболее простой в реализации алгоритм, обладающий рядом недостатков:

5) скрытое сообщение легко разрушить;

6) не обеспечена секретность встраивания информации (для преодоления данного недостатка можно встраивать скрытое сообщение не во все пикселы

Библиотека БГУИР

изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известному только законному пользователю, но пропускная способность при этом значительно уменьшается).

– BPCS

Более сложный алгоритм сокрытия данных, состоящий в последовательном выполнении следующих шагов:

7) разбиение на битовые плоскости,

8) разбиение на блоки,

9) вычисление меры сложности каждого блока (метрика длины черно-белой границы),

10) вычисление меры сложности секретного сообщения,

11) замена сложного блока изображения на блок сообщения.

Однако вне зависимости от выбранного варианта реализации алгоритма BPCS в контейнер с высокой долей вероятности будут внесены заметные искажения, которые можно обойти с помощью алгоритма ABCDE. Он и был выбран в качестве основы для реализации программного средства.

– ABCDE

Данный метод скрытия базируется на тех же принципах, что и BPCS, но между ними имеются существенные различия:

12) для вычисления мер сложности блоков используют метрику длины черно-белой границы и метрику неравномерности длин серий,

13) использование М-кодирования в процессе внедрения сообщений в блок, что оказывает значительное влияние на структуру внедряемой служебной информации.

В экспериментальной части диссертации были проанализированы результаты внедрения сообщения в графический файл, показавшие высокие значения емкости внедрения у разработанного протокола (до 48% контейнера может быть заменено без существенной деградации качества контейнера). Кроме того, было проведено сравнение BPCS и ABCDE, которое показало:

14) одинаково устойчивы к большинству атак на системы ЦВЗ;

15) ABCDE обладает большей емкостью внедрения и вносит меньше искажений в изображения, чем BPCS.

Основным же недостатком ABCDE, который был выявлен в ходе проведения экспериментов, является вычислительная сложность операции внедрения данных. В качестве мер по решению данной проблемы было предложено:

16) установить постоянное значение величины k для наименее значащих плоскостей,

Библиотека БГУИР

17) внедрять дополнительный блок в качестве заголовка для каждого сегмента (k блоков потока).

Предложенное решение позволило существенным образом сократить временные затраты на проведение операции внедрения данных и не оказало заметного отрицательного воздействия на операцию извлечения данных.

Таким образом, в результате исследования был разработан протокол защиты графических образов, который может быть успешно применен для доказательства авторства в случае отсутствия специфических атак против стегокодера и встроенного сообщения со стороны злоумышленника.

Дальнейшая разработка может быть направлена на решение следующих задач:

18) поддержка внедрения водяного знака в графические форматы, использующие сжатие с потерями;

19) разработка алгоритма автоматического подбора пороговых значений мер сложности для изображений;

20) разработка алгоритма подбора оптимального значения размеров блока и числа бит для внедрения в один блок для каждой битовой плоскости;

21) разработка алгоритма интеллектуального подбора размера водяного знака в зависимости от свойств контейнера (к примеру, для больших контейнеров водяной знак может быть увеличен за счет бит помехоустойчивого кодирования).

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик, В.Н. Ярмолик // Приоритетные направления развития науки и образования: материалы III Международной научно-практической конференции – Чебоксары: Интерактив плюс, 2014 – с. 170-171.

2. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик, А.А. Сушков // Наука, образование, общество: тенденции и перспективы. Сборник научных трудов по материалам Международной научно-практической конференции, часть 3: тезисы доклада – Москва: АР-Консалт, 2014 – с. 68-71.

3. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик // Материалы Международной научной конференции «Информационные технологии и системы»: тезисы доклада – Минск, 2014 – с. 132-133.

Библиотека БГУИР