**СОДЕРЖАНИЕ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 2 |
| Изм. | Лист | № докум | Подпись | Дата |

Введение3

1 Стеганография и методы её реализации 4

1.1 Принципы построения видео стегосистемы 4

1.2 Атаки на видео стегосистемы и противодействия им 6

1.3 Обоснованный выбор стеганографического метода скрытия данных 9

2 Реализация стеганографического метода скрытия данных в видео 12

2.1 Алгоритм скрытия информации в видео-контейнере 12

2.2 Программная реализация

3 Оценка стеганостойкости реализованной системы

3.1 Определение степени пригодности контейнера для стеганографической модификации

3.2 Моделирование атак и оценка стойкости системы

Заключение

Список литературы

Приложение

Полный листинг программной реализации

**ВВЕДЕНИЕ**

Цель работы: программная реализация и скрытие информации на основе дискретных преобразований в видеофайле при помощи вейвлет-преобразования.

Стеганография — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения).

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок или письмо. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография — сам факт наличия каких-либо скрытых посланий от обличения.

Задачей данной курсовой работы является изучение принципов построения защищенных стеганографических систем, атак направленных на стеганографические системы и противодействие им. Определение перспектив дальнейшего изучения и развития в сфере стеганографического сокрытия информации и применения полученных знаний на практике.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 3 |
| Изм. | Лист | № докум | Подпись | Дата |

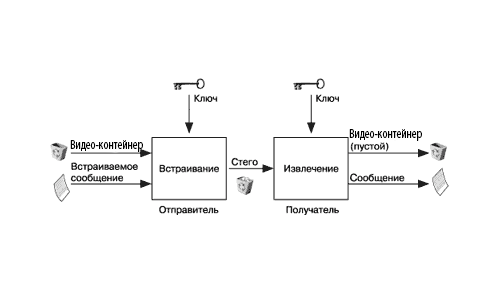
33

**ГЛАВА 1. СТЕГАНОГРАФИЯ И МЕТОДЫ ЕЁ РЕАЛИЗАЦИИ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 4 |
| Изм. | Лист | № докум | Подпись | Дата |

**1.1 Принципы построения видео стегосистемы**

Стеганографическая видеосистема — объединение методов и средств, используемых для создания скрытого видео канала для передачи информации.



В видео стегосистеме в качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п. В общем же случае, для обозначения скрываемой ин­формации, целесообразно использовать слово «сообщение», так как сообщением мо­жет быть как текст или изображение, так и, например, аудио данные. В современной компьютерной стеганографии существует два основных типа файлов: сообщение — файл, который предназначен для скрытия, и контейнер — файл, который может быть использован для скрытия в нем сообщения.

При построении стеганографической видеосистемы должны учитываться следующие положения:

* стегосистема должна иметь приемлемую вычислительную сложность реализации;
* должна обеспечиваться необходимая пропускная способность;
* методы скрытия должны обеспечивать аутентичность и целостность секретной информации для авторизованного лица;
* потенциальный нарушитель имеет полное представление о стегосистеме и делали ее реализации; единственное, что ему неизвестно, – это ключ, с помощью которого только его обладатель может установить факт наличия и содержание скрытого сообщения;
* если факт существования скрытого сообщения становится известным нарушителю, это не должно позволить последнему извлечь его до тех пор, пока ключ сохраняется в тайне;
* нарушитель должен быть лишен любых технических и других преимуществ в распознании или, по крайней мере, раскрытии содержания секретных сообщений.

Сообщение, которое необходимо передать отправителю, с помощью специального программного обеспечения встраивается в видео-контейнер. Данные контейнера должны быть достаточно шумными, чтобы небольшое изменение в их беспорядочности не могло быть заметным. Биты видео-контейнера, хотя и являются шумом с точки зрения точности измерений, могут иметь некоторые специальные статистические характеристики. Предполагается, что кодирование тайного сообщения должно воспроизводить характеристики шума видео-контейнера. Выбор видео-контейнера оказывает существенное влияние на надежность всей видео стегосистемы и возможность обнаружения факта передачи скрытого сообщения.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 5 |
| Изм. | Лист | № докум | Подпись | Дата |

**1.2 Атаки на стегосистемы и противодействия им**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 6 |
| Изм. | Лист | № докум | Подпись | Дата |

Основной задачей стегоанализа является определение факта наличия скрытого сообщения в предположительном видео-контейнере. Решить эту задачу возможно путем изучения статистических свойств сигнала. Например, распределение младших битов сигналов имеет, как правило, шумовой характер. Они несут наименьшее количество информации о сигнале и могут использоваться для внедрения скрытого сообщения. При этом, возможно, изменится их статистика, что и послужит для атакующего признаком наличия скрытого канала.

Пассивный нарушитель может лишь обнаружить факт наличия стегоканала и читать сообщения. Сможет ли он прочесть сообщение после его обнаружения зависит от стойкости системы шифрования, и этот вопрос, как правило, не рассматривается в стеганографии. Если у нарушителя имеется возможность выявить факт наличия скрытого канала передачи сообщений, то стегосистема обычно считается нестойкой. Осуществление обнаружения стегоканала является наиболее трудоемкой задачей, а защита от обнаружения считается основной задачей стеганографии, по определению.

Действия злоумышленного нарушителя наиболее опасны. Он способен не только разрушать, но и создавать ложные стего. Для осуществления той или иной угрозы нарушитель применяет атаки. Наиболее простая атака — субъективная. Нарушитель внимательно рассматривает видео, пытаясь определить «на глаз», имеется ли в нем скрытое сообщение. Ясно, что подобная атака может быть проведена лишь против совершенно незащищенных стегосистем. Тем не менее, она, наверное, наиболее распространена на практике, по крайней мере, на начальном этапе вскрытия стегосистемы. Первичный анализ также может включать в себя следующие мероприятия:

1. Первичная сортировка стего по внешним признакам.
2. Выделение стего с известным алгоритмом встраивания
3. Определение использованных стегоалгоритмов.
4. Проверка достаточности объема материала для стегоанализа.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 7 |
| Изм. | Лист | № докум | Подпись | Дата |

1. Проверка возможности проведения анализа по частным случаям.
2. Аналитическая разработка стегоматериалов. Разработка методов вскрытия стегосистемы.
3. Выделение стего с известными алгоритмами встраивания, но неизвестными ключами.

Можно выделить следующие типы атак на видео стегосистемы:

* Атака на основе известного заполненного видео-контейнера. В этом случае у нарушителя есть одно или несколько стеганографических файлов. В последнем случае предполагается, что встраивание скрытой информации осуществлялось отправителем одним и тем же способом. Задача нарушителя может состоять в обнаружении факта наличия видео стеганографического канала, а также в его извлечении или определения ключа. Зная ключ, нарушитель получит возможность анализа других видео стеганографических сообщений.
* Атака на основе известного встроенного сообщения. Задачей анализа является получение ключа. Если соответствующий скрытому сообщению заполненный видео-контейнер неизвестен, то задача крайне трудно решаема.
* Атака на основе выбранного скрытого сообщения. В этом случае нарушитель имеет возможность предлагать отправителю для передачи свои сообщения и анализировать получающиеся стеганографических видеофайлов.
* Адаптивная атака на основе выбранного скрытого сообщения. Эта атака является частным случаем предыдущей. В данном случае нарушитель имеет возможность выбирать сообщения для навязывания отправителю адаптивно, в зависимости от результатов анализа предыдущих стеганографических видеофайлов.

|  |
| --- |
|  |

* Атака на основе выбранного пустого видео-контейнера. В этом случае нарушитель способен заставить отправителя пользоваться предложенным им видео-контейнером. Например, предложенный видео-контейнер может иметь большие однородные, и тогда будет трудно обеспечить секретность внедрения.
* Атака на основе известной математической модели видео-контейнера или его части. При этом атакующий пытается определить отличие подозрительного сообщения от известной ему модели. Например допустим, что биты внутри отсчета изображения коррелированы. Тогда отсутствие такой корреляции может служить сигналом об имеющемся скрытом сообщении. Задача внедряющего сообщение заключается в том, чтобы не нарушить статистики видео-контейнера.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 8 |
| Изм. | Лист | № докум | Подпись | Дата |

В робастной стегосистеме необходим правильный выбор параметров псевдослучайной последовательности. Известно, что при этом системы с расширением спектра могут быть весьма робастными по отношению к атакам типа добавления шума, сжатия и т. п. Так считается, что ЦВЗ должен обнаруживаться при достаточно сильной низкочастотной фильтрации. Следовательно, база сигнала должна быть велика, что снижает пропускную способность стегоканала. Кроме того, используемая в качестве ключа ПСП должна быть криптографически безопасной.

Различные методы противодействия предлагались для решения проблемы прав собственности. Первый способ заключается в построении необратимого алгоритма ЦВЗ. ЦВЗ должен быть адаптивным к сигналу и встраиваться при помощи однонаправленной функции, например, хэш-функции.

Второй способ решения проблемы прав собственности заключается во встраивании в ЦВЗ некоторой временной отметки, предоставляемой третьей, доверенной стороной. В случае возникновения конфликта лицо, имеющее на изображении более раннюю временную отметку, считается настоящим собственником.

**1.3 Обоснованный выбор стеганографического метода скрытия данных**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 9 |
| Изм. | Лист | № докум | Подпись | Дата |

В данной курсовой работе для скрытия данных в видео-контейнере используется вейвлет-преобразование, а именно один из первых и наиболее простых вейвлетов – вейвлет Хаара.

Вейвлет-преобразование — интегральное преобразование, которое представляет собой свертку вейвлет-функции с сигналом. Вейвлет-преобразование переводит сигнал из временного представления в частотно-временное.

Способ преобразования функции в форму, которая или делает некоторые величины исходного сигнала более поддающимися изучению, или позволяет сжать исходный набор данных. Вейвлетное преобразование сигналов является обобщением спектрального анализа. Вейвлеты — это обобщённое название математических функций определенной формы, которые локальны во времени и по частоте и в которых все функции получаются из одной базовой, изменяя её (сдвигая, растягивая).

Вейвлет-преобразование широко используется для анализа сигналов. Помимо этого, оно находит большое применение в области сжатия данных. В дискретном вейвлет-преобразовании наиболее значимая информация в сигнале содержится при высоких амплитудах, а менее полезная — при низких. Сжатие данных может быть получено за счет отбрасывания низких амплитуд. Вейвлет-преобразование позволяет получить высокое соотношение сжатия в сочетании с хорошим качеством восстановленного сигнала. Вейвлет-преобразование было выбрано для стандартов сжатия изображений JPEG2000 и ICER. Однако, при малых сжатиях вейвлет-преобразование уступает по качеству в сравнении с оконным Фурье-преобразованием, которое лежит в основе стандарта JPEG.

Выбор конкретного вида и типа вейвлетов во многом зависит от анализируемых сигналов и задач анализа. Для получения оптимальных алгоритмов преобразования разработаны определенные критерии, но их еще нельзя считать окончательными, так как они являются внутренними по отношению к самим алгоритмам преобразования и, как правило, не учитывают внешних критериев, связанных с сигналами и целями их преобразований. Отсюда следует, что при практическом использовании вейвлетов необходимо уделять достаточное внимание проверке их работоспособности и эффективности для поставленных целей по сравнению с известными методами обработки и анализа.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 10 |
| Изм. | Лист | № докум | Подпись | Дата |

**Достоинства:**

* Вейвлетные преобразования обладают всеми достоинствами преобразований Фурье.
* Вейвлетные базисы могут быть хорошо локализованными как по частоте, так и по времени. При выделении в сигналах хорошо локализованных разномасштабных процессов можно рассматривать только те масштабные уровни разложения, которые представляют интерес.
* Базисные вейвлеты могут реализоваться функциями различной гладкости.

**Недостатки:**

* Можно выделить один недостаток ― это относительная сложность преобразования.

Вейвлет Хаара — один из первых и наиболее простых вейвлетов. Он основан на ортогональной системе функций. Вейвлеты Хаара ортогональны, обладают компактным носителем, хорошо локализованы в пространстве, но не являются гладкими.

Преобразование Хаара используется для сжатия входных сигналов, компрессии изображений, в основном цветных и черно-белых с плавными переходами. Идеален для картинок типа рентгеновских снимков. Данный вид архивации известен довольно давно и напрямую исходит из идеи использования когерентности областей. Степень сжатия задается и варьируется в пределах 5-100. При попытке задать больший коэффициент на резких границах, особенно проходящих по диагонали, проявляется «лестничный эффект» — ступеньки разной яркости размером в несколько

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 11 |
| Изм. | Лист | № докум | Подпись | Дата |

Преобразование Хаара для одномерного сигнала.

Пусть имеется одномерный дискретный входной сигнал ***{\displaystyle S}S***. Каждой паре соседних элементов ставятся в соответствие два числа: {\displaystyle a\_{i}={\frac {S\_{2i}+S\_{2i+1}}{2}}}  и {\displaystyle b\_{i}={\frac {S\_{2i}-S\_{2i+1}}{2}}} . Повторяя данную операцию для каждого элемента исходного сигнала, на выходе получают два сигнала, один из которых является огрубленной версией входного сигнала — {\displaystyle a\_{i}}, а второй содержит детализирующую информацию, необходимую для восстановления

исходного сигнала. Аналогично, преобразование Хаара может быть применено к полученному сигналу{\displaystyle a\_{i}}  и т.д.

Преобразование Хаара для двумерного сигнала.

Двумерное преобразование Хаара — это не что иное, как композиция одномерных преобразований Хаара. Пусть двумерный входной сигнал представляется матрицей {\displaystyle S}. После применения одномерного преобразования Хаара к каждой строке матрицы {\displaystyle S} получаются две новые матрицы, строки которых содержат аппроксимированную и детализирующую часть строк исходной матрицы. Аналогично к каждому столбцу полученных матриц применяют одномерное преобразование Хаара и на выходе получают четыре матрицы, одна из которых является аппроксимирующей составляющей исходного сигнала, а три оставшиеся содержат детализирующую информацию — вертикальную, горизонтальную и диагональную.

**ГЛАВА 2. Реализация стеганографического метода скрытия данных в видео**

**2.1 Алгоритм скрытия информации в видео-контейнере**

Шифрование информации в видео можно разделить на следующие этапы:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 12 |
| Изм. | Лист | № докум | Подпись | Дата |

2)RGB->YCrCb

3)Вейплет преобразование

4)Шифрование

5)Собрать

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  | 9 |
| Изм. | Лист | № докум | Подпись | Дата |

9

|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  |  |
| Изм. | Лист | № докум | Подпись | Дата |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | Лист |
|  |  |  |  |  |  |
| Изм. | Лист | № докум | Подпись | Дата |