

Библиотека
Профессионала

Грибунин В. Г., Оков И. Н., Туринцев И. В.

Цифровая стеганография



Оглавление

Введение	3
1. Введение в цифровую стеганографию	6
1.1. Цифровая стеганография.	
Предмет, терминология, области применения	6
1.2. Встраивание сообщений в незначащие элементы контейнера.....	16
1.3. Математическая модель стегосистемы	18
1.4. Стеганографические протоколы.....	22
1.4.1. <i>Стеганография с открытым ключом</i>	22
1.4.2. <i>Обнаружение ЦВЗ с нулевым знанием</i>	25
1.5. Некоторые практические вопросы встраивания данных	29
2. Атаки на стегосистемы и противодействия им	31
2.1. Атаки против систем скрытной передачи сообщений	31
2.2. Атаки на системы цифровых водяных знаков	34
2.2.1. Классификация атак на стегосистемы ЦВЗ	34
2.2.2 Атаки, направленные на удаление ЦВЗ	36
2.2.3. Геометрические атаки	39
2.2.4. Криптографические атаки	40
2.2.5. Атаки против используемого протокола	41
2.3. Методы противодействия атакам на системы ЦВЗ	44
2.4. Статистический стегоанализ и противодействие	46
3. Пропускная способность	
каналов передачи скрываемой информации	47
3.1. Понятие скрытой пропускной способности	47
3.2. Информационное скрывание	
при активном противодействии нарушителя	49
3.2.1. <i>Формулировка задачи информационного</i>	
<i>скрывания при активном противодействии нарушителя</i>	49
3.2.2 <i>Скрывающее преобразование</i>	57
3.2.3. <i>Атакующее воздействие</i>	58
3.3. Скрытая пропускная способность	
стегоканала при активном противодействии нарушителя	59
3.3.1. <i>Основная теорема информационного скрывания</i>	
<i>при активном противодействии нарушителя</i>	59
3.3.2 <i>Свойства скрытой пропускной способности стегоканала</i>	62

3.4. Двоичная стегосистема передачи скрываемых сообщений.....	66
3.5. Теоретико-игровая формулировка информационно-скрывающего противоборства	70
3.6. Стегосистемы с бесконечными алфавитами	75
3.6.1. <i>Использование контейнера как ключа стегосистемы</i>	77
3.6.2. <i>Слепая стегосистема с бесконечным алфавитом</i>	79
3.7. Построение декодера стегосистемы.....	84
3.8. Анализ случая малых искажений стего	85
3.9. Атакующее воздействие со знанием сообщения	89
3.10. Скрывающие преобразования и атакующие воздействия с памятью	91
3.11. Стегосистемы идентификационных номеров	94
3.12. Скрытая пропускная способность стегоканала при пассивном нарушителе	100
4. Оценки стойкости стеганографических систем и условия их достижения	110
4.1. Понятие стеганографической стойкости	110
4.2. Стойкость стегосистем к обнаружению факта передачи скрываемых сообщений.....	116
4.3. Стойкость недетерминированных стегосистем	123
4.4. Практические оценки стойкости стегосистем.....	130
4.4.1. <i>Постановка задачи практической оценки стегостойкости</i>	130
4.4.2. <i>Визуальная атака на стегосистемы</i>	131
4.4.3. <i>Статистические атаки на стегосистемы с изображениями-контейнерами</i>	134
4.4.4. <i>Статистические атаки на стегосистемы с аудиоконтейнерами</i>	138
4.4.5. <i>Направления повышения защищенности стегосистем от статистических атак</i>	141
4.5. Теоретико-сложностный подход к оценке стойкости стеганографических систем	144
4.6. Имитостойкость системы передачи скрываемых сообщений	147
5. Скрытие данных в неподвижных изображениях	154
5.1. Человеческое зрение и алгоритмы сжатия изображений.....	155
5.1.1. <i>Какие свойства зрения нужно учитывать при построении стегоалгоритмов</i>	155

5.1.2	Принципы сжатия изображений	157
5.2.	Скрытие данных в пространственной области	162
5.3.	Скрытие данных в области преобразования	171
5.3.1.	Выбор преобразования для скрытия данных	171
5.3.2	Скрытие данных в коэффициентах дискретного косинусного преобразования	175
6.	Обзор стегаалгоритмов встраивания информации в изображения	183
6.1.	Аддитивные алгоритмы	183
6.1.1.	Обзор алгоритмов на основе линейного встраивания данных ..	183
6.1.2	Обзор алгоритмов на основе слияния ЦВЗ и контейнера	194
6.2.	Стеганографические методы на основе квантования	196
6.2.1.	Принципы встраивания информации с использованием квантования. Дизеризованные квантователи	196
6.2.2	Обзор алгоритмов встраивания ЦВЗ с использованием скалярного квантования	200
6.2.3.	Встраивание ЦВЗ с использованием векторного квантования	202
6.3.	Стегаалгоритмы, использующие фрактальное преобразование	203
7.	Скрытие данных в аудиосигналах	207
7.1.	Методы кодирования с расширением спектра	207
7.2.	Внедрение информации модификацией фазы аудиосигнала	213
7.3.	Встраивание информации за счет изменения времени задержки эхо-сигнала	215
7.4.	Методы маскирования ЦВЗ	220
8.	Скрытие данных в видеопоследовательностях	225
8.1.	Краткое описание стандарта MPEG и возможности внедрения данных	225
8.2.	Методы встраивания информации на уровне коэффициентов	231
8.3.	Методы встраивания информации на уровне битовой плоскости	233
8.4.	Метод встраивания информации за счет энергетической разности между коэффициентами	237
Заключение		246
Список литературы		247