Д.В. Решетников
Научный руководитель: доцент кафедры ФПМ, к.т.н. А.В. Астафьев
Муромский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264 г. Муром Владимирской обл., ул. Орловская, 23
E-mail:
student.reshetnikov@mail.ru

Обзор и анализ стойкости алгоритмов стеганографии

Согласитесь, мало кто из нас хотел, чтобы его секретная информация или личные данные стали кому-то известны без его ведома, но в наше время есть множество способов, благодаря которым можно узнать любую информацию, которая нас заинтересует. А как же быть с той, которую мы хотим оставить в секрете от посторонних глаз? Вот тут нам на помощь приходит такая наука как стеганография. Основная суть её заключается не только в скрытии самих данных, но еще и в их передачи. Мы прячем передаваемую информацию в какую-нибудь обыкновенную картинку, факт передачи которой не вызвал бы никаких подозрений. Исходя из этого, разработка новых и совершенствование уже существующих алгоритмов стеганографии является актуальной научно-технической задачей.

Целью исследования является обзор и анализ стойкости алгоритмов стеганографии.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор стойкости алгоритмов стеганографии.
2. Анализ стойкости алгоритмов стеганографии к различного рода атакам.
3. Сделать выводы о проделанной работе.

Обзор стойкости алгоритмов стеганографии. Под стойкостью алгоритмов стеганографии понимается способность противостоять атакам (изменению скрытого сообщения). В качестве атак рассмотрим сжатие изображения, устойчивость к фильтрации, устойчивость к геометрическим преобразованием и устойчивость к средствам статистического стегоанализа. Выбор алгоритмов сжатия обусловлен их широким использованием для обработки изображений в системах мультимедиа. Рассмотрим 6 алгоритмов стеганографии.

Таблица 1 – Алгоритмы стеганографии.

Название алгоритма	Тип стегосистемы	Цифровой водяной знак	Область преобразования
Wang	Закрытая	Числовая последовательность	Вейвлет-преобразования
Barni	Закрытая	Числовая последовательность	Вейвлет-преобразования
Cox	Закрытая	Числовая последовательность	Блоки ДКП n × n
Koch	Открытая	Текстовая строка	Блоки ДКП 8 × 8
Pitas	Открытая	Текстовая строка	Пространственная
Bruyndonckx	Открытая	Текстовая строка	Пространственная

Анализ стойкости алгоритмов стеганографии к различного рода атакам. В результате анализа были выявлены следующие достоинства и недостатки данных алгоритмов по следующим критериям, приведенных в таблице:

Таблица 2 - Результаты анализа стойкости алгоритмов.

Название алгоритма	Однозначность восстановления	Устойчивость к фильтрации	Устойчивость к геометрическим преобразованиям	Устойчивость к сжатию	Устойчивость к средствам статистического стегоанализа
Wang	+	+	-	+	-
Barni	-	+	-	+	+
Cox	+	-	+	+	-
Koch	+	-	-	-	-
Pitas	+	-	-	+	+
Bruyndonckx	+	-	-	-	+

Вывод о проделанной работе. Благодаря проделанному анализу мы видим, что у каждого алгоритма есть свои недостатки. Именно поэтому создание стойкого алгоритма, который мог бы справляться с различными преобразованиями является актуальной задачей.

Литература

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006. — 288 с

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. - М.: Солон-Пресс, 2002. - 272 с

3. Миано Дж. Форматы и алгоритмы сжатия изображений в действии. М.: Триумф, 2003. 336 с.