АЛГОРИТМ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Д.т.н. А.А. Кобозева, А.Д. Шовкун

Одесский национальный политехнический университет
Украина, г.Одесса
alla_kobozeva@ukr.net

Один из наиболее эффективных технических средств защиты мультимедийной информации заключается во встраивании в защищаемый объект некоторых меток – цифровых водяных знаков (ЦВЗ) [1]. В отличие от обычных водяных знаков ЦВЗ могут быть видимыми и (как правило) невидимыми. ЦВЗ могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию. Наиболее подходящими объектами защиты при помощи ЦВЗ являются неподвижные изображения, файлы аудио и видеоданных. Для простоты изложения далее в качестве информационных контентов, в которые происходит погружение ЦВЗ, рассматриваются цифровые изображения, называемые контейнерами. Контейнер после погружения в него ЦВЗ будем называть стеганосообщением.

ЦВЗ могут быть трех типов: робастные, хрупкие и полухрупкие (под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стеганосообщение). В настоящей работе рассматриваются ЦВЗ последнего типа. Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. Вообще говоря, все ЦВЗ могут быть отнесены к этому типу. Однако полухрупкие ЦВЗ специально проектируются так, чтобы быть неустойчивыми по отношению к определенного рода операциям [1,2].

Чаще всего ЦВЗ используются для защита цифровых изображений от модификации и подделки (аутентификация изображений).

Целью настоящей работы является разработка нового стеганографического алгоритма для встраивания полухрупких ЦВЗ,

позволяющего решать не только задачу аутентификации изображения-контейнера, но и задачу скрытой передачи информации.

Разрабатываемый метод основывается на алгоритме, предложенном в [2], - алгоритме встраивания ЦВЗ и защиты изображения от модификаций на основе псевдоквантования, осуществляющий встраивание одного пикселя (бита) ЦВЗ в один пиксель изображения-контейнера, что дает возможность максимизировать объём скрытно передаваемой информации (ЦВЗ), но делает данный метод непригодным для проверки подлинности изображения.

Предлагаемый в настоящей работе алгоритм после предварительного стандартного разбиения матрицы F изображения-контейнера на 8*8-блоки осуществляет встраивание одного бита ЦВЗ в блок матрицы, рассматривая формально процесс погружения ЦВЗ как процесс возмущения матрицы контейнера [3]:

$$\overline{F} \square F \square \square F ,$$

где $\overline{F}$ матрица ЦИ после погружения ЦВЗ, $\square F$ - матрица возмущения при стеганопреобразовании контейнера.

Разработанный алгоритм позволяет одновременно осуществлять скрытую передачу информации и защиту изображения-контейнера от модификации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

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

2. Глумов Н.И. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации / Н.И.Глумов, В.А.Митекин. - Компьютерная оптика. – 2011. - №2, т.35. – С.262-267.

3. Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. - К.: Изд.ГУИКТ, 2009. – 251 с.