

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ СТЕГАНОГРАФИЧЕСКОГО СОКРЫТИЯ ИНФОРМАЦИИ МЕТОДОМ LSB

Цель – создание программного средства для сокрытия текстовой информации в изображении посредством алгоритма внедрения данных least significant bit (LSB). Задачи: анализ метода внедрения информации в изображения, изучение алгоритма LSB, создание ПС для внедрения текстовой информации в изображение на основе данного метода.

Для создания скрытой передачи данных необходимо построить стегосистему согласно следующим принципам:

- потенциальный злоумышленник обладает знаниями о деталях реализации системы, кроме ключа, с помощью которого можно обнаружить наличие скрытой информации и ее содержание;
- пока потенциальный злоумышленник не располагает ключом, обнаружение наличия внедренного сообщения никаким образом не влияет на его извлечение и на извлечение подобных сообщений в других данных;
- потенциальный злоумышленник не должен иметь технических, программных или иных преимуществ в обнаружении и расшифровке содержания внедренной информации.

На рисунке 1 схематически показана обобщенная стеганографическая система [1].

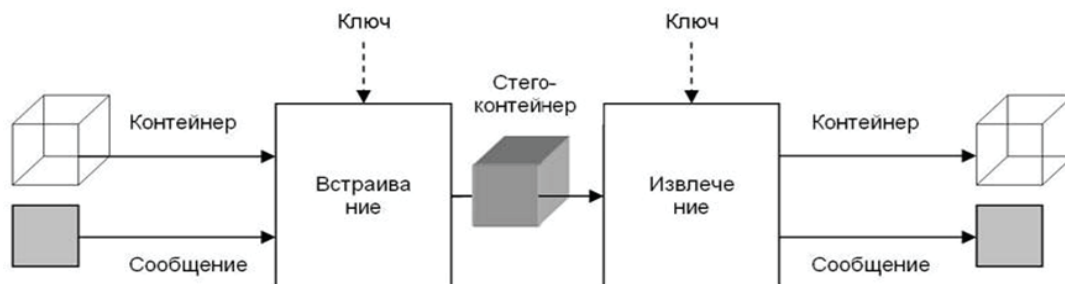


Рисунок 1 – Стеганографическая система

В рамках данного исследования был разработан алгоритм стеганографического метода. Алгоритм включает в себя выбор изображения, модификацию пикселей и сохранение результата. Кроме того, на основе данного алгоритма было разработано приложение, с помощью которого можно встраивать секретную информацию методом замены наименьшего значащего бита.

Приложение реализовано на основе метода замены наименее значащих битов. Данный метод основан на принципе замены бит избыточной и малозначимой информации изображения на биты внедряемого сообщения. Зачастую длина бит внедряемой информации меньше количества бит изображения, поэтому после внедрения появляются две области с различными статистическими свойствами, что легко распознается статистическими тестами. Поэтому внедряемую информацию дополняют информационным мусором – случайными битами, чтобы ее битовая длина была равна количеству пикселей изображения, используемому для внедрения. Простота реализации метода и высокая полезная емкость контейнера являются несомненными достоинствами метода, однако, при любом искажении контейнера встроенная информация также искажается. Чтобы определить полезную емкость контейнера при использовании метода замены наименее значащего бита, необходимо воспользоваться формулой (1):

$$Q = H \times W \times V \times D, \quad (1)$$

где Q – это емкость контейнера, измеряемая в битах, H – это высота изображения в пикселях, W – это ширина изображения в пикселях, V – это число компонент цвета, D – это количество наименее значащих бит в каждой компоненте.

Для приложения также разработан графический интерфейс. Форма даёт доступ к основным функциям программного средства.

Для сокрытия информации в изображении-контейнере необходимо выполнить следующие шаги: выбрать вкладку «Hide information»; выбрать путь к изображению-контейнеру, в котором необходимо сокрыть информацию; ввести текст, который необходимо скрыть; если необходимо защитить информацию с помощью криптографического алгоритма, то выбрать пункт «Use a cryptographic algorithm for more reliable information protection» и ввести секретный ключ; нажать кнопку «Hide information in the image and save».

Для извлечения информации из изображения-контейнера необходимо выполнить следующие шаги: выбрать вкладку «Get information»; ввести путь к изображению-контейнеру, из которого необходимо извлечь информацию; если сокрытая в изображении-контейнере информация зашифрована, то выбрать пункт «Use a cryptographic algorithm for more reliable information protection» и ввести секретный ключ; нажать кнопку «Extract data from image».

В результате, разработанное приложение представляет собой программное средство, которое предоставляет возможность скрывать или извлекать информацию в/из изображение с использованием алгоритма LSB.