УДК [004.056+003.26] (075.8)

Студ. Е. В. Сергиенко
Науч. рук. проф. П. П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

# ПРИЛОЖЕНИЕ ДЛЯ РЕАЛИЗАЦИИ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ С ИСПОЛЬЗОВАНИЕМ КОДА ХЭММИНГА

Стеганография – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи [1]. В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования.

Существуют следующие направления стеганографии: цифровая, компьютерная и сетевая.

Цифровая стеганография – направление стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов.

Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы.

Сетевая стеганография использует для сокрытия данных элементы сетевых протоколов [2].

Актуальность использования кода Хэмминга для стеганографического преобразования заключается в том, что он позволяет обнаруживать и исправлять ошибки, которые могут возникнуть в процессе хранения или передачи секретного сообщения. Используя код Хэмминга, стеганографическая система способна восстанавливать скрытое сообщения, даже если контейнер, в котором передавалось сообщение, подвергся воздействию шума или другим формам помех.

Основная техника избыточного кодирования – добавление при записи (передаче) в полезные данные избыточной информации (контрольных символов или битов четности), а при чтении – использование такой избыточной информации для обнаружения и исправления ошибки [3]. Число ошибок, которое можно исправить, ограничено и зависит от конкретного применяемого кода. В нашем исследовании применяется код Хемминга. Он позволяет исправлять одиночную ошибку и находить двойную. В контексте стеганографии код Хэмминга можно использовать для сокрытия секретного сообщения в изображении.

В рамках исследования разработано специальное приложение, реализующее стеганографическое преобразование с использованием кода Хэмминга. Исходное сообщение представляется в двоичном виде

и делится на блоки длиной 4, 8, 16 битов. Эти блоки соответствуют информационным словам. Выбор кода – 7,4; 12,8 или 21,16 – выбирается из меню. Одно из окон приложения представлено на рис. 1.

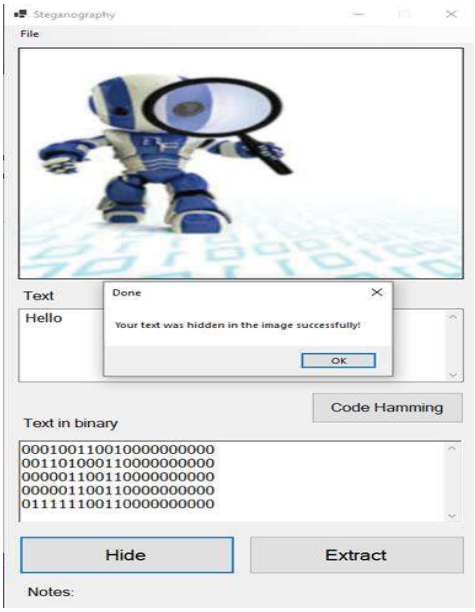


**Рисунок 1 – Интерфейс приложения**

Как видно из представленного скриншота, в данном приложении можно также выбрать изображение-контейнер, текст для осаждения в контейнер, просмотреть, как этот текст будет выглядеть в коде Хемминга, а также разместить информацию в контейнер или извлечь эту информацию из него.

## ЛИТЕРАТУРА

1. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 220 с.

2. Урбанович, П. П. Компьютерные сети и сетевые технологии: учеб. пособие для студ. технических спец. / П. П. Урбанович, Д. М. Романенко. – Минск: БГТУ, 2022. – 608 с.

3. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 1. Кодирование информации: учеб.-метод. пособие для студентов учреждений высшего образования / П. П. Урбанович, Д. В. Шиман, Н. П. Шутько. – Минск: БГТУ, 2019. – 116 с.