УДК 003.26+004.9

П.П. Урбанович, Е.В. Сергеенко
Белорусский государственный технологический университет
Минск, Беларусь

СИМУЛЯТОР СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИЗОБРАЖЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИЗБЫТОЧНО КОДА

Аннотация. *Проанализированы особенности использования избыточного кодирования информации совместно со стеганографией. Приведено описание разработанного симулятора для анализа эффективности применения кода Хемминга, а также статистические результаты, свидетельствующие о корректирующих способностях кода при модификации 1-2 младших битов на цветовой канал для каждого пиксела изображения.*

P.P. Urbanovich, E.V. Sergeenko
Belarusian State Technological University
Minsk, Belarus

SIMULATOR OF STEGANOGRAPHIC IMAGE TRANSFORMATION USING REDUNDENT CODE

Abstract. *The features of using redundant information coding in conjunction with steganography are analyzed. A description of the developed simulator for analyzing the effectiveness of using the Hamming code is given, as well as statistical results indicating the corrective abilities of the code when modifying 1-2 low-order bits per color channel for each image pixel.*

Как известно, стеганография в общем понимании – это наука о скрытом хранении или о скрытой передаче информации [1]. Важным свойством любой стеганографической системы является устойчивость стеганоконтейнера к различным модификациям. Интуитивно понятно, что чем меньше изменений вносит процесс внедрения тайного сообщения, тем меньше вероятность того, что такие изменения контейнера будут обнаружены. Существует концепция «эффективности внедрения», которая рассматривается как среднее количество битов сообщения, внедренных с использованием изменения одного бита контейнера [2].

Важность проблемы обеспечения высокой эффективности встраивания для стеганографии и актуальность разработки и использования для этих целей так называемых покрывающих кодов (covering codes) впервые предложены Крэндаллом (Crandall) [3], который показал, что линейные коды могут заметно повысить эффективность встраивания.

Как вариант реализации идеи Крэндалла, в [4] проанализированы некоторые особенности использования избыточных корректирующих кодов в стеганографических приложениях. Приведено формальное описание модели стеганосистемы, в которой код используется для коррекции извлекаемого из стеганоконтейнера сообщения. Предложена конструкция линейного кода для коррекции одиночных и двойных парных (смежных) ошибок. А в [5] рассмотрены прикладные особенности совместного использования методов помехоустойчивого кодирования данных и стеганографии: стеганографические преобразования основаны на цветовых моделях RGB и HSL, а также на использовании метода наименее значащих битов (LSB). Комбинация двух видов преобразования позволяет, тайно передавать или хранить информацию, а также повышает, ее защищенность при конвертациях стеганоконтейнера.

В настоящей статье описывается структура, особенности и результаты использования приложения, в котором реализовано стеганографическое преобразование с использованием избыточного кода Хемминга.

Проект реализован на основе паттерна MVVM (Model-View-ViewModel), который позволяет отделить логику приложения от визуальной части (представления). Основная логика приложения разделена на два основных класса: класс, обслуживающий стеганографические операции, и класс для работы с кодом Хемминга.

Структура первого класса состоит из методов для осаждения данных в изображение и их извлечения (методы *EmbedBits* и *ExtractBitsAndSymbolsInBlock* соответственно), а также методов, предназначенных для генерации шума, т. е. имитации ошибок. Второй из упомянутых классов состоит из методов, реализующих кодирование и декодировани блоков осаждаемого сообщения: *CodeHamming* и *DecodeHamming* соответственно.

Пример генерации шума, представленного псевдослучайным изменением цветовых координат фрагмента контейнера размером 50x50 показан на рис. 1.

На рис. 2 показан фрагмент сообщения приложения о характере и результатах наложения шума на изображение-контейнер.

Для оценки эффективности использования кода Хемминга, задачей которого было выявление и исправление внесенных ошибок, был проведен тест. Его сущность. В изображение с размерами 75x112 (максимальное число бит, которое можно разместить в контейнере – 50 400, т. е. предполагалось, что можно модифицировать при осаждение максимально по 2 младших бита на цветовой канал, формирующий цвет пиксела).

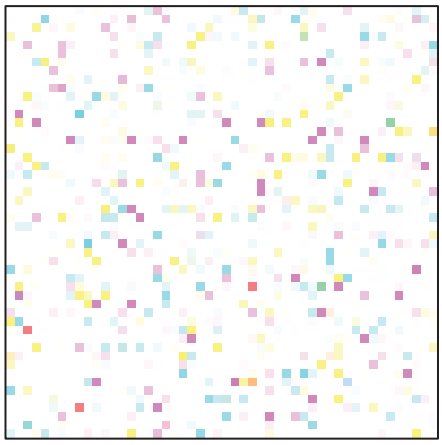


Рис. 1 - Цветовое представление работы генератора в виде 100 ошибок

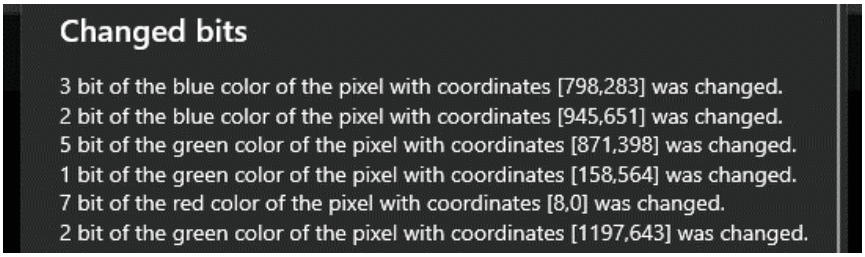
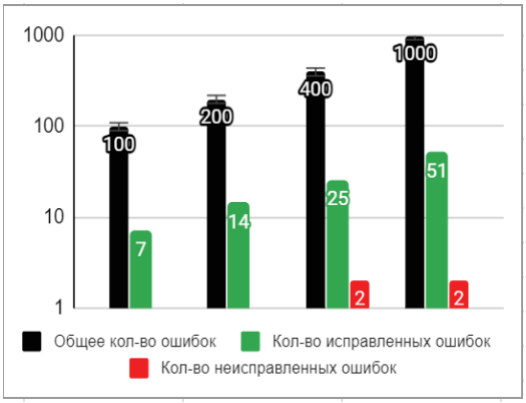


Рис. 2 - Информация приложения о внесенных ошибках

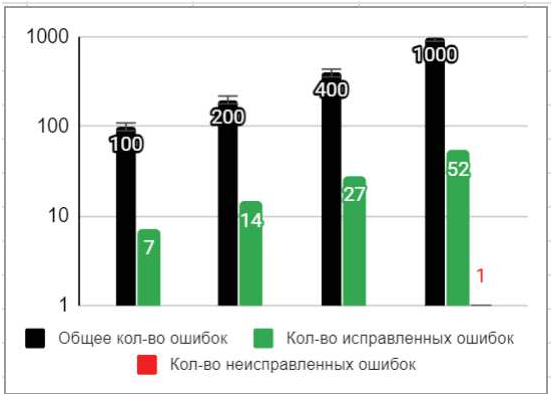
В указанный фрагмент изображения-контейнера размещались данные, объем которых составлял 25%, 50% и 100% от максимального размера сообщения. При этом можно было варьировать длиной формируемого кодового слова (n), которая, как известно, равна сумме кодируемых (k) и проверочных (r) символов. При обработке стеганоконтейнера (что соответствует режиму извлечения осажденного сообщения с коррекцией обнаруженных ошибок) собиралась и накапливалась статистика о выявленных и невыявленных кодом ошибках.

Результаты эксперимента приведены в виде гистограмм на рис. 3–5. На этих гистограммах черный цвет соответствует данным без применения кода. При кодировании основное информационное слово состояло из двух байтов (k=16). При этом в одном случае это слово дополнялось 5 битами (r=5; код – (21,16)), во втором – делилось на 2 части по 8 битов (код – (12,8)), к каждой из которых присоединялись по 4 бита, что соответствует коду с минимальным кодовым расстоянием d=3, для которого должно выполняться условие:

$r \geq \log_2 k+1$.

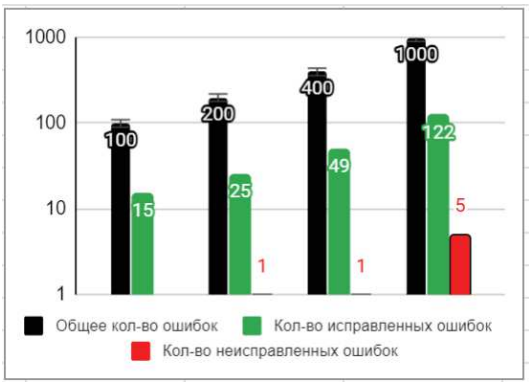


а)

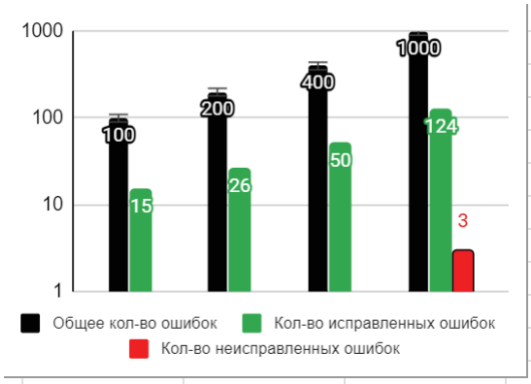


б)

Рис. 3 - Эффективность использования кода при 25-процентном заполнении контейнера и при использовании кодов (21,16) – а) и (12,8) – б)

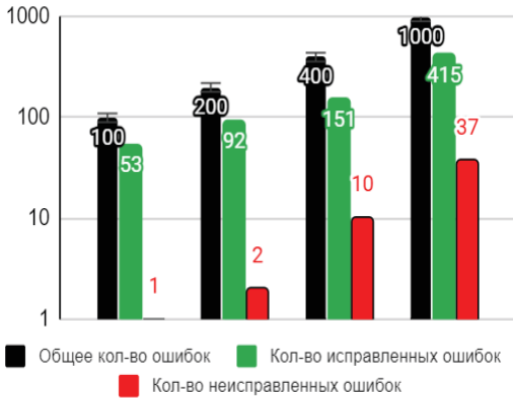


а)

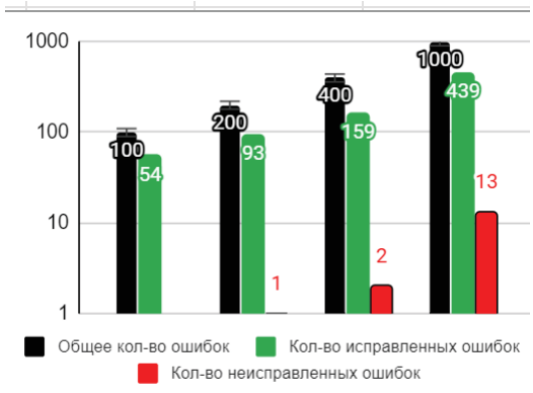


б)

Рис. 4 - Эффективность использования кода при 50-процентном заполнении контейнера и при использовании кодов (21,16) – а) и (12,8) – б)



а)



б)

Рис. 5 - Эффективность использования кода при 100-процентном заполнении контейнера и при использовании кодов (21,16) – а) и (12,8) – б)

Код Хемминга, удовлетворяющий приведенным параметрам, позволяет обнаружить и скорректировать 1 ошибку в кодовом слове. Необходимо отметить, что избыточные символы сократили пропускную

способность контейнера, означающую максимально возможное количество размещаемой информации.

Например, при 100% заполнения контейнера без использования кода объем такой информации составил 3148 символов, а при использовании кода (21, 16) этот объем сократился на 23,8% и на 33,3% – кода (12, 8).

Из анализа и сравнения приведенных данных следует, что использование кода позволяет существенно повысить надежность преобразования. Вместе с тем, практическое уменьшение в 2 раза длины кодируемого слова (до 1 байта) не гарантирует обнаружение и коррекцию всех ошибок.

Список использованных источников

1. Урбанович, П.П. Использование скрытых каналов для передачи информации на основе стенографических методов в стеке протоколов TCP/IP / П.П. Урбанович, И.В. Калоша, Н.П. Шутько // Импортозамещение, научно-техническая и экономическая безопасность: сборник статей V Международной научно-технической конференции "Минские научные чтения-2022", Минск, 07-09 декабря 2022 г. : в 3 т. Т. 2. – Минск: БГТУ, 2022. С. 393–398.

2. Bierbrauer, J., Fridrich, J. Constructing Good Covering Codes for Applications in Steganography. In: Shi, Y.Q. (eds) Transactions on Data Hiding and Multimedia Security III. Lecture Notes in Computer Science, v. 4920. – Springer, Berlin, Heidelberg, 2008. DOI:10.1007/978-3-540-69019-1_1.

3. Crandall, R. Some Notes on Steganography, Posted on Steganography. Mailing List, 1998.

4. Урбанович, П. П. Коррекция одиночных и двойных парных ошибок в стенографических каналах передачи информации /

П.П. Урбанович // Информационные системы и технологии: материалы международного научного конгресса по информатике : в 3-х ч., Минск, 27–28 октября 2022 г. – Ч. 1. – С. 113–119.

5. Урбанович, П.П. Особенности использования методов избыточного кодирования в стеганографических приложениях / П. П. Урбанович [и др.] // Информационные технологии и системы 2022 (ИТС 2022) = Information Technologies and Systems 2022 (ITS 2022): материалы Международной научной конференции, Минск, 23 ноября 2022 / Белорусский гос. ун–т информ. и радиоэл.– Минск: БГУИР, 2022. – С. 173–174.