УДК 003.26+004.56

МОДИФИКАЦИЯ МЕТОДА LSB ДЛЯ МНОГОКЛЮЧЕВОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

Берников В.О., Урбанович П.П.
БГТУ, г. Минск, Республика Беларусь; vladbernikovronaldo@gmail.com

Реферат. В докладе кратко описываются модификация стеганографического метода LSB [1] и разработанное программное средство для осаждения и обратного извлечения тайного сообщения при использовании данного метода на базе многоключевой модели стеганографической системы. Многоключевая модель информационной системы оперирует различными методами стеганографии, криптографии, помехоусточивого кодирования или иными преобразованиями для повышения стеганостойкости системы в целом. Программное средство может использоваться в научных исследованиях, а также в учебном процессе.

Задача повышения стеганографической стойкости документов-контейнеров текстового или иного типа приобретает все большую актуальность в связи с возрастающей ролью правовых аспектов создания, размещения и использования электронного контента. Одно из эффективных средств решения задачи повышения стеганографической стойкости документов-контейнеров тестового типа – применение эффективных методов стеганографии. При этом необходимо обеспечить требуемый уровень защищенности стеганографической системы перед несанкционированным использованием осажденной в контейнер информации. Использование многоключевой модели информационной системы обеспечивает эффективное решение поставленной задачи.

Формально многоключевую стеганосистему можно представить следующим образом:

$$X = \{M, C, K, S, f, \mu\} \quad (1),$$

где: M – множество сообщений, C – множество контейнеров, K – множество ключей, S – множество секретных сообщений, f – функция осаждения информации, μ – функция извлечения информации [2, 5].

Для анализа эффективности некоторых решений нами разработано специализированное программное средство, которое использует описанную выше модель информационной системы. Контейнером для внедрения стегосообщений являются электронные документы формата *.doc или *.docx.

Для того, чтобы внедрить тайное сообщение в соответствующий контейнер, электронный документ был представлен в формате *xml* (использована соответствующая библиотека *Aspose.Words* на языке C#). Документ сначала разбивается на объекты, которые называются параграфами. Из параграфов, в свою очередь, извлекаются *Run*-ы, то есть слова с одинаковым форматированием. Далее извлекаются все узлы (буквы) из этих *Run*-ов и только после этого возможно осаждение секретных битов стегосообщения.

Как известно, LSB (Least Significant Bit, наименьший значащий бит) – стеганографический метод, который заключается в замене младших значащих битов в контейнере на биты скрываемого сообщения.

Опишем модификацию метода LSB, которая была использована в качестве ключа для осаждения секретной информации по цвету в электронный документ Microsoft Word. В данном методе есть возможность использования псевдорандомизации (отдельного ключа многоключевой модели информационной системы) секретных бит по всему электронному документу. На каждый символ документа можно скрыть один бит секретной информации. После получения всех узлов объектов *Run*, возможно внедрение секретных битов в наш документ.

Далее в текущий узел помещаем единичный секретный бит с цветом #0459ED в 16-ой системе счисления (это синий цвет). В противном случае, внедряется нулевой секретный бит с 16-ым значением #ED0459, который будет соответствовать розовому цвету. Если пользователь не выберет подсветку внедренных секретных бит, то данный метод

автоматически получит текущий цвет слов электронного документа, а цвет секретных символов в документе изменится на 16-ые значения #000001 и #000002 относительно своего исходного цвета для единичного и нулевого секретных битов соответственно [3]. При этом факт передачи скрытой информации будет не заметен человеческому глазу. Демонстрация работы данного метода представлена на рисунке 1.

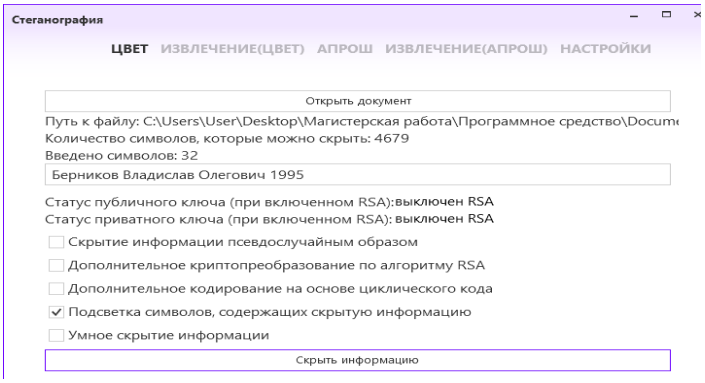

Рисунок 1 – Диалоговое окно для осаждения информации на основе цвета

Выбирается документ, куда будет помещена секретная информация. Производится автоматический подсчет символов, которые можно скрыть в выбранном электронном документе. После этого вводится непосредственно наше секретное сообщение. В данном примере не будем использовать псевдослучайный разброс внедряемых битов, выбрав лишь подсветку символов, содержащих секретную информацию, наглядно убедившись в правильной работе данного стеганографического метода. Убедимся, что информация успешно была осаждена в стеганоконтейнере (рисунок 2).

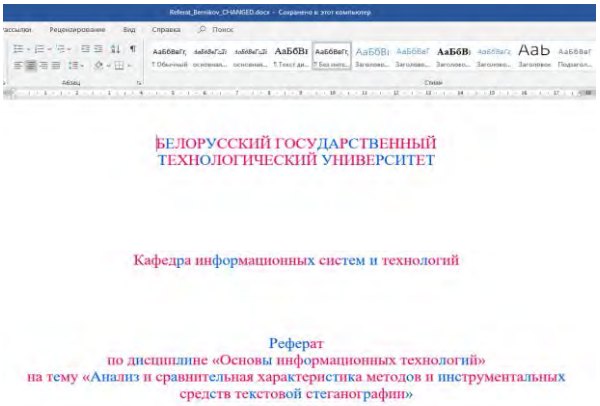

Рисунок 2 – Стеганоконтейнер после осаждения на основе цвета

Как видно из рисунка, секретная информация была успешно осаждена в начало электронного документа. Синий цвет показывает, что были осаждены единичные биты секретного сообщения, а розовый – что нулевые. Далее покажем контейнер после осаждения секретной информации при отключенной опции подсветки скрытых символов (рисунок 3).

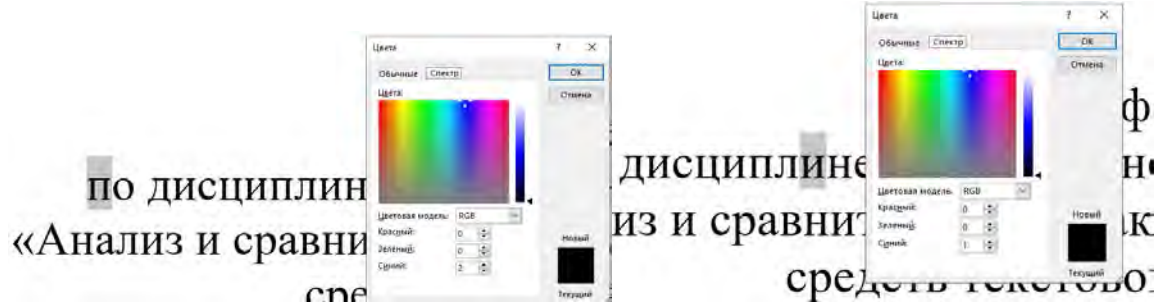

Рисунок 3 – Осаждение стегосообщения в контейнере без опции подсветки символов

Для проверки корректной работы модификации метода LSB была использована

аддитивная цветовая модель RGB непосредственно в самом электронном документе. На рисунке видно, что в букву «п» был внедрен нулевой бит, а в букву «и» соответственно был осажден единичный бит. Отметим, что другие символы, в которые не были внедрены секретные биты тайного сообщения в цветовой модели RGB принимают значения (0; 0; 0) для красного, зеленого и синего цветов соответственно.

Далее продемонстрируем процесс извлечения стегосообщения из электронного документа (рисунок 4). Сначала выбирается документ, в который уже предварительно была спрятана информация. Электронный документ разбивается на параграфы, затем на *Run*-ы и после этого извлекаются нужные узлы со значением цветов, которые были указаны при сокрытии секретной информации [4].

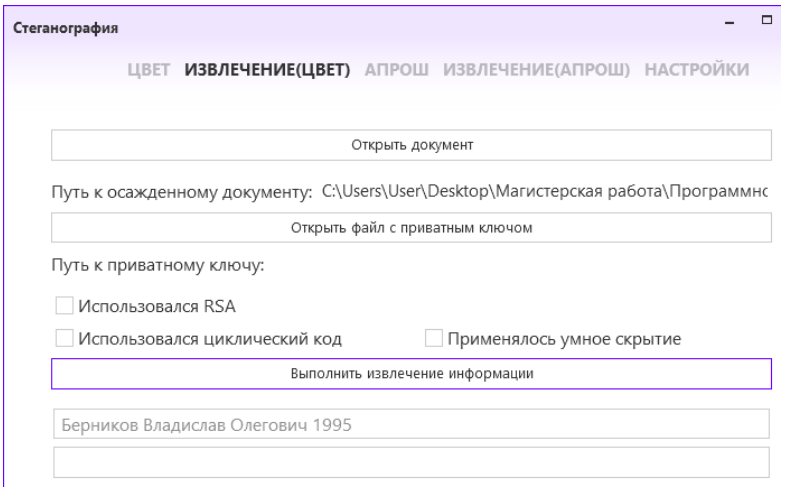

Рисунок 4 – Диалоговое окно для извлечения информации на основе цвета

Как видно из рисунка, стегосообщение успешно было извлечено из электронного документа. Отметим, что совместно с описанной модификацией метода LSB можно использовать и другие компоненты (ключи) многоключевой модели информационной системы такие как криптографический ключ, ключ для псевдорандомизации бит по всему документу, ключ для хеширования стегосообшения, а также ключ для помехоусточивого кодирования, если учитывать возникновение возможных ошибок при передачи и хранении информации.

Описанное программное средство реализовано на основе модели информационной системы, которая подразумевает применение практически неограниченного числа ключей. Мы представили процесс внедрения и извлечения стегосообщения при использовании контейнера текстового типа формата DOCX и DOC на основе модификации метода LSB. Разработанное средство используется также в учебном процессе при изучении студентами дисциплин «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации».

Список литературы:

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Pavel Urbanovich, Nadzeya Shutko. Theoretical Model of a Multi-Key Steganography System, in: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Computer Science Vol. 2, Ed. A. Zapała. – Wydawnictwo KUL, Lublin, 2016, Part II, Chapter 11. – P. 181-202.

3. Берников, В.О. Разработка стеганографических методов на основе многоключевой модели информационной системы/ В.О. Берников // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях. – Гомель: ГГУ им. Ф. Скорины. – 2018. – С. 192-193.

4. Берников, В.О. Анализ стеганографической стойкости текстового документа-

контейнера в многоключевой стеганосистеме // 69-я НТК студентов и магистрантов: сб. науч. работ: в 4-х ч. 17-22 апреля 2018 г. – Минск: БГТУ, 2018. – Ч. 4. – С.14-17.

5. Берников, В. О. Математическое моделирование стеганографической стойкости многоключевой системы / В. О. Берников, П. П. Урбанович // Информационные технологии : материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4-15 февраля 2019 г. / отв. за изд. И. В. Войтов; УО БГТУ. – Минск : БГТУ, 2019. – С. 31-33.