УДК 004.056.55

РЕАЛИЗАЦИЯ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА В АЛЬТЕРНАТИВНЫХ ПОТОКАХ ФАЙЛОВОЙ СИСТЕМЫ NTFS

М. В. Колмаков, Е. А. Блинова
Белорусский государственный технологический университет, Минск

Одним из решений проблемы скрытой передачи информации является применение цифровых стеганографических методов. В настоящее время актуальна задача поиска новых типов контейнеров, пригодных для стеганографического встраивания информации, и методов их использования. В качестве контейнера скрытых сообщений предлагается использовать альтернативные потоки данных, доступные в файловой системе NTFS (New Technology File System). Передача данных в альтернативных потоках без потерь затруднительна, для решения этой проблемы предусмотрена архивация данных в специальные форматы.

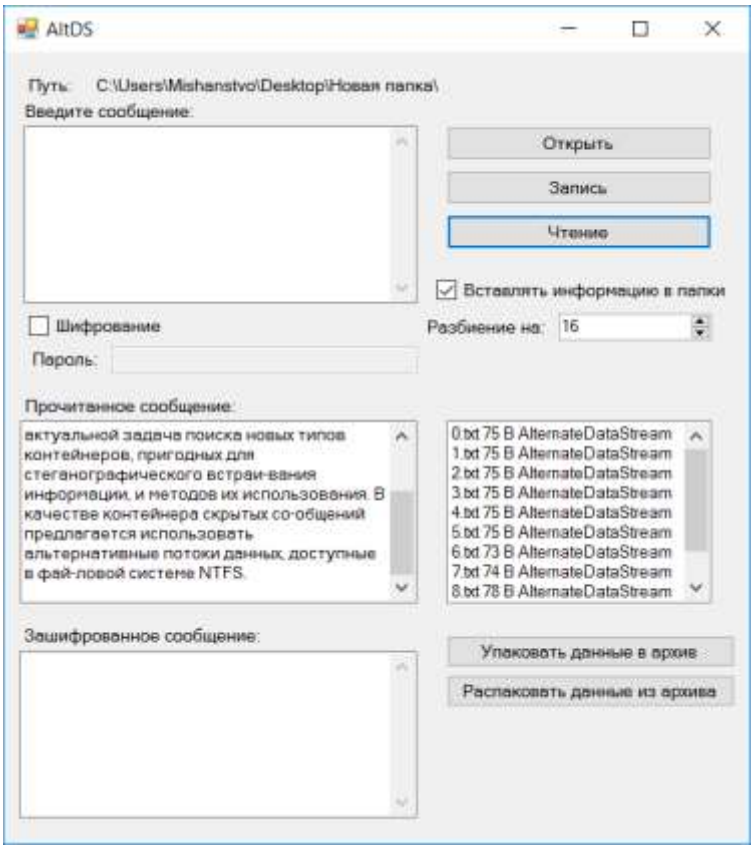
Стеганография – это наука, изучающая способы скрытой передачи информации путем скрытия самого факта передачи. С изобретением цифровых способов реализации алгоритмов, применяемых в стеганографии, ее развитие вышло на существенно новый уровень. Зачастую стеганографические методы применяются в комплексе с криптографическими, т. е. в стеганографические контейнеры осаждаются уже зашифрованные данные.

NTFS – стандартная файловая система для семейства операционных систем (ОС) Windows компании Microsoft. NTFS поддерживает хранение метаданных и разграничение прав доступа к данным для различных пользователей и групп. В файловой системе NTFS файл, кроме основных данных, также может быть связан с одним или несколькими дополнительными (альтернативными) потоками данных, причем произвольного размера. В альтернативных потоках могут храниться такие атрибуты, как сведения об авторе, названии и иконке файла, а также подробная информация о происхождении загруженных файлов. ОС Windows позволяют получать доступ к альтернативным потокам данных, однако большинство программ их игнорируют.

Авторами разработано программное средство и выполнена адаптация стеганографического метода на основе альтернативных потоков в файловой системе NTFS. В качестве стеганоконтейнера может выступать папка в ОС на основе файловой системы NTFS, содержащая любое количество файлов. Данные будут разбиваться на части и записываться в альтернативные потоки к файлам [1]. Для разработки программного средства выбран язык программирования C# с использованием Win-API-функций. Для работы с альтернативными потоками была выбрана библиотека Trinet.Core.IO.Ntfs, так

как стандартные средства в C# не поддерживают работу с альтернативными потоками. Дополнительно данные могут быть зашифрованы, для расшифрования потребуется пароль. Кроме того, вставка сообщения в альтернативные потоки может осуществляться с разбиением на отдельные блоки и при последующем извлечении информация будет объединена в одно сообщение в правильной последовательности [2].

На рисунке изображено основное окно программного средства AltDS. При работе пользователь первоначально выбирает папку с файлами, куда будет выполнено осаждение информации. Далее пользователь выбирает, на сколько частей разбивать секретное сообщение, их должно быть не более чем количество файлов в папке. Имеется возможность использовать папки как контейнеры. Преимуществом папок является то, что при вставке скрытых данных их размер никак не меняется. При выборе директории, в которую необходимо вставить скрытую информацию, она проверяется на наличие файлов и папок. Если окажется, что директория пуста, то будет ошибка, так как нечего осаждать информацией. В программе отображается размер каждого потока и указывается, сколько было использовано потоков.



Главное окно программы

Пользователь может ввести любое сообщение, которое он хочет внедрить в электронный файл-контейнер, длина сообщения не ограничена. Есть

возможность дополнительного выбора предварительного криптопреобразования сообщения с последующим хешированием зашифрованного сообщения. После всех операций программа создает альтернативные потоки к выбранным файлам и записывает в них части сообщения.

При считывании сообщения идет проверка на наличие альтернативных потоков, и при наличии в них данных секретная информация может быть извлечена. Если она была предварительно зашифрована, то при извлечении из контейнера нужно ввести пароль.

Стоит отметить, что при переносе файлов в другие файловые системы, отличные от NTFS, скрытая информация полностью теряется. Чтобы переносить данные без потерь, их нужно упаковать в специальный архив, который поддерживает потоки файловой системы NTFS. Для архивации используются архивы Windows Imaging Format (wim), это файл-ориентированный формат образа диска. Формат был разработан компанией Microsoft для развертывания последних релизов ОС семейства Windows. Затем архив .wim упаковывается в .7z – свободный формат сжатия данных, поддерживающий несколько различных алгоритмов сжатия и шифрования данных, так как .wim не поддерживает сжатие. Извлечение данных происходит в обратном порядке: сначала извлекается архив .7z, после этого .wim, программное средство делает это все автоматически.

Проведен анализ целостности файлов с осажденной информацией после переноса их между различными файловыми системами. Разработано программное средство и выполнена адаптация стеганографического метода на основе альтернативных потоков в файловой системе NTFS. В качестве стеганоконтейнера может выступать папка в ОС на основе файловой системы NTFS, содержащая любое количество файлов и папок.

Список литературы

1. Github [Electronic resource] – 2018. – Mode of access: https://github.com/mis-hanstvo/AltDS_Steganography. – Date of access: 01.02.2019.

2. Колмаков, М. В. Особенности применения стеганографических методов в альтернативных потоках файловой системы NTFS / М. В. Колмаков, Е. А. Блинова // Материалы 69 науч.-техн. конф. учащихся, студентов и магистрантов. – Минск, 2018. – С. 9–13.