

*Кротенко К.В.
студент 4 курса*

*факультет «Прикладная информатика»
Пермский государственный аграрно-технологический университет
научный руководитель: Глотина И.М., к.э.н.
доцент
Россия, г. Пермь*

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ СКРЫТИЯ И ИЗВЛЕЧЕНИЯ ИНФОРМАЦИИ В ГРАФИЧЕСКИХ ФАЙЛАХ

Аннотация: в данной статье рассмотрены аспекты защиты информации. Определены понятия шифрования, стеганографии, криптографии. Представлены каналы и сферы утечки информации за последние года. Сформированы конкретные требования к стеганографическим методам. Подробно описан один из методов скрытия и извлечения текста в графических файлах, представлен подробный алгоритм, а также интерфейс реализации в виде программного приложения.

Ключевые слова: информационная безопасность, целостность данных, криптография, стеганография, методы стеганографии.

*Krotenko K.V.
student*

*4 course, faculty "Applied Informatics"
Perm State Agrarian and Technological University
Russia, Perm
Scientific supervisor: Glotina I.M.*

Candidate of Economic Sciences, Associate Professor

DEVELOPMENT OF THE PROGRAM FOR HIDDEN AND RECOVERY OF INFORMATION IN GRAPHIC FILES

Annotation: aspects of information protection are considered in this article. The concepts of encryption, steganography, cryptography are defined. The channels and areas of information leakage for the last years are presented. Specific requirements for steganography methods have been formed. One of the methods of hiding and extracting text in graphic files is described in detail, a detailed algorithm is presented, as well as an implementation interface in the form of a software application.

Keywords: information security, data integrity, cryptography, steganography, steganography methods.

Современные технологии развиваются с огромной скоростью, причем во всех сферах жизни. Еще 30 лет назад было невозможно представить, что будут существовать персональные компьютеры, что каждый сможет

выходить в глобальную сеть Интернет, а мысль о смартфонах казалась нелепой.

Сейчас трудно представить жизнь человека без этих вещей. С помощью современных достижений отрасли производства выходят на новые уровни, в больницах стало возможно спасение большего количества людей, даже самый мелкий бизнес может быть не только автоматизирован, но и полностью существовать в виртуальной среде. И это малая часть того, что дал нам век высоких технологий.

Информационные ресурсы выходят на первый план, заменяя материальные аспекты.

Но у всего есть и обратная сторона.

Мошенники тоже развиваются и изучают всевозможные способы и методы получения прибыли. В течение последних нескольких лет наблюдается рост количества краж конфиденциальной информации. Утечка информации может осуществляться через совершенно разные каналы: оборудование, мобильные устройства, съемные носители, браузеры или облачные хранилища, электронную почту. Неосторожное распространение персональных данных также может привести к несанкционированному доступу или краже в разных сферах: банки, медицина, торговля, промышленность и транспорт, госорганы, образование, муниципальные учреждения. В последствие данные «жертвы» могут использоваться, к примеру, для шантажа, подделки финансовых бумаг или махинаций в сфере недвижимости.

В связи с этим, информационная безопасность в 21 веке набирает все большую актуальность.

Методы защиты от мошенников развиваются также стремительно. Один из таких методов – криптография.

Криптография – наука, изучающая методы обеспечения целостности данных, цель которой – шифрование информации, причем таким образом, чтобы третье лицо не смогло эту информацию распознать.

Шифрование – преобразование информации с целью защиты от нарушителей.

Для разработки программы использован криптографический метод – стеганография [1].

Стеганография – такой способ шифрования, который отвечает за сокрытие самого факта хранения (передачи) данных.

Стеганография является наиболее надежным криптографическим методом, так как третье лицо может и не узнать о факте сокрытия (передачи) данных.

Как происходит преобразование данных стеганографическим методом?

Секретное сообщение помещается в контейнер – данные различного вида. Контейнером могут выступать: аудиофайл, текстовый и графический

файл, так и в видеофайл, HTML-документ. Важным моментом является то, что при шифровании используются индивидуальные свойства каждого из вида контейнеров.

Если файл содержит секретную информацию, то он является заполненным контейнером, в случае отсутствия такой информации – пустым контейнером.

В связи с вышеперечисленными аспектами, можно определить четкие требования, предъявляемые к стеганографическим методам:

- даже если злоумышленник знает о методе шифровании информации, он не должен обнаружить саму информацию;
- контейнером могут служить данные различного вида;
- пустой контейнер не должен отличаться от заполненного для злоумышленника [2].

Что же представляет собой шифрование и дешифрование информации в графических файлах?

При шифровании информация из текстового файла помещается в картинку.

При дешифровании происходит обратный процесс – из картинки достается текст, который был зашифрован.

Алгоритм программы основан на свойствах файлов формата BMP.

Цвета изображения состоят из смешивания 3 цветов: красный, синий, зеленый. Эти цвета – основа RGB-кодировки (red, green, blue).

В программе шифруется текст в изображение. Каждый символ текста в двоичной кодировке занимает 8 позиций (или 8 бит, или 1 байт). Для того, чтобы поместить один такой символ в изображение, нужно использовать 3 пикселя (рисунок 1).

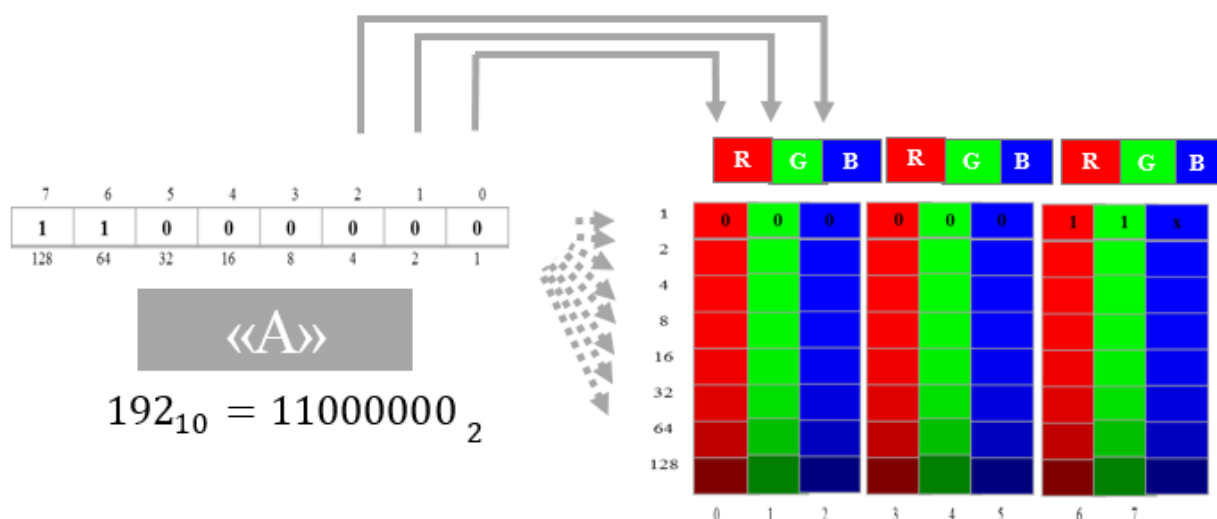


Рисунок 1 – Алгоритм шифрования

Для примера используется заглавная русскоязычная буква «А». Ее код в двоичной системе – 11000000. Он записывается в обратной порядке и нумеруется с нуля. Один компонент цвета равен одному биту, так что таких

компонентов нужно 8. Один пиксель состоит из трёх цветов, так что понадобится 3 пикселя. Хотя и понадобится 8 цветов, а в 3 пикселях их 9, один компонент цвета останется пустым, в программировании он использоваться не будет. В результате двоичный код символа преобразуется двоичный код цвета.

Стоит учитывать и глубину цвета, его разрядность. Если использовать самый незначительный по весу разряд (1 бит), то преобразование изображения совершенно не будет заметно. Использование более значимых по весу разрядов будет более значительным, и к 128 биту человек сможет четко увидеть искажения.

Количество скрываемых символов ограничено размером изображения. Так, к примеру, изображение размеров 2000 на 3000 пикселей содержит в себе 6000000 пикселей (6 мегапикселей). 1 символ занимает 3 пикселя, а значит 600000 нужно разделить на 3, и в итоге получится 2 миллиона символов, которые можно скрыть в заданном изображении.

Интерфейс программы представлен на рисунке 2.

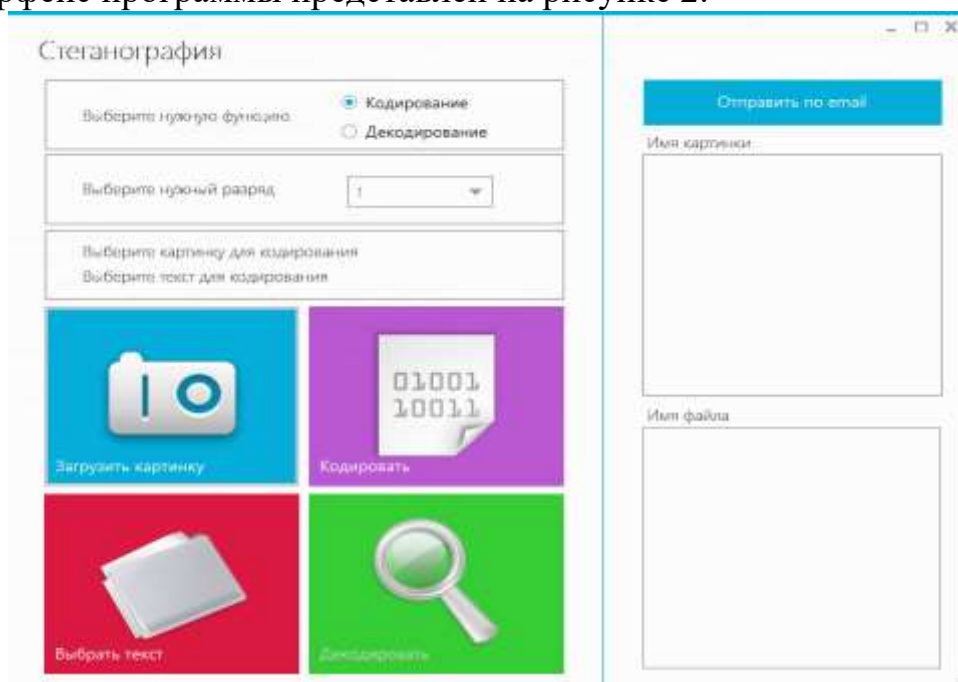


Рисунок 2 – Интерфейс программы

Функции программы включают в себя:

- кодирование текста, его скрытие в изображении;
- декодирование текста, его получение из изображения;
- определение максимально возможного количества символов, которые можно скрыть в изображении;
- определение количества символов в выбранном текстовом файле;
- передача изображения со скрытым текстом по email.

Какого же практического применения программы?

Можно использовать шифрование в личных интересах, если нужно

вести какую-либо тайную переписку в социальных сетях или по электронной почте.

Если есть необходимость в шифровании своих персональных данных, таких как: логинов, паролей, банковских счетов и прочих. К примеру, при регистрации на различных порталах, желательно использование логинов и паролей, которые не будут повторяться с теми, что вы использовали ранее.

Еще одно применение – борьба со злоумышленниками, которая может принести заработок. Изучение методов стеганографии поможет в дальнейшем определить свою профессию, предотвращать действия хакеров и, при соответствующей реализации, монетизировать представленный в работе проект.

Таким образом, используя современные технологии, человек не должен забывать, что угроза безопасности информации становится все актуальнее. Существует множество способов борьбы со злоумышленниками, и стеганография является одним из надежных методов для шифрования информации.

Использованные источники:

1. Глотина И.М. Актуальные вопросы информационной безопасности [Текст]: монография / И.М. Глотина, В.Г. Климов, М-во с.-х. РФ, ФГБОУ ВПО Пермская ГСХА. – Пермь: Изд-во ФГБОУ ВПО Пермская ГСХА, 2013. – 360 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – М.: МК-Пресс, 2006. – 288 стр.
3. Хабрахабр. ИТ портал. [Электронный ресурс]. – Режим доступа: <https://habrahabr.ru> (дата обращения: 10.02.2018).