УДК 004.421+004.421 DOI: 10.18698/2541-8009-2020-02-582

РЕАЛИЗАЦИЯ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА LSB В СРЕДЕ MATLAB APP DESIGNER

А.Ю. Яковлев

andrey.67.rus@yandex.ru
SPIN-код: 6420-6870

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Описан стеганографический алгоритм LSB и его реализация в приложении с графическим интерфейсом среды MATLAB App Designer. Рассмотрена компьютерная и цифровая стеганография и реализован алгоритм, который позволяет спрятать полезную информацию в изображение. Данное приложение позволяет пользователям тайно обмениваться текстовыми сообщениями, используя изображения определенных форматов. В данных форматах изображений используются алгоритмы сжатия без потерь. В программе предусмотрены алгоритмы, позволяющие затруднить стегоанализ файлов статистическими методами. Также реализован алгоритм электронной цифровой подписи RSA, позволяющий подтвердить авторство пользователя и проверить целостность сообщения.

Ключевые слова

Стеганография, MATLAB, App Designer, алгоритм LSB, обработка изображений, стегоанализ, графический пользовательский интерфейс, RGB-модель изображения.

Поступила в редакцию 13.02.2020

В век информационных технологий проблема защиты информации актуальна как никогда ранее. Нас окружает огромное количество информации, которую необходимо обрабатывать, например, защищать и скрывать. Иногда пользователь оказывается в условиях, когда в канал связи вторгается злоумышленник. Злоумышленник может действовать по-разному, к примеру, просто читать сообщения. В такой ситуации пользователь вынужден преодолевать эту трудность, как вариант, путем сокрытия информации от противника. Здесь на помощь приходит стеганография, которая позволяет спрятать полезные данные так, чтобы факт передачи этих данных остался в тайне. Так же стеганография позволяет создавать «водяные знаки» в файлах, что будет препятствовать нарушению авторского права.

Стеганография — способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения). В отличие от криптографии, которая шифрует сообщение, стеганография позволяет скрыть сам факт передачи сообщения. При этом передаваемое сообщение не подвергается шифрованию. Приведем здесь необходимые понятия и термины:

1) сообщение — общее название передаваемой скрытой информации;

2) контейнер — любая информация, используемая для сокрытия тайного сообщения.

В данном случае сообщение — это текст, который один пользователь хочет отправить другому, оставляя в тайне факт передачи. Контейнер — изображение формата PNG, для которого предусмотрен алгоритм сжатия без потерь Deflate. Важно не допустить потерь при сжатии и отправке изображения. Такой формат позволяет с точностью до бита восстановить закодированные данные после их передачи. Формат PNG позиционируется, прежде всего, для использования в Интернете и редактирования графики. Таким образом, пользователь может скрыть сообщение в контейнер формата PNG и передать его другому пользователю по сети без ущерба целостности информации. Конечно, мы можем использовать и другие форматы изображений, в которых предусмотрены алгоритмы сжатия без потерь.

Описание алгоритма LSB. LSB (Least Significant Bit) — суть этого метода заключается в замене последних значащих битов в контейнере (в данной работе в изображении) на биты скрываемого сообщения. Разница между пустым и заполненным контейнером не должна быть заметна для глаз.

В среде MATLAB изображение представляется при помощи RGB-модели. Изображение кодируется тремя каналами: R — красный, G — зеленый, B — синий. Цвет пикселя кодируется числом от 0 до 255 по каждому каналу включительно. Например, черный цвет будет кодироваться следующей тройкой чисел — (0, 0, 0), желтый — (255, 255, 0) и т. д. Далее выбираем канал, в который мы поместим сообщение. Выберем красный канал. Получаем число, которое кодирует цвет пикселя по красному каналу, переводим его в двоичную систему счисления. Заменяем два младших бита на два бита полезной информации и переводим обратно в десятичную систему счисления. После чего заменяем в изображении код старого цвета кодом полученного (с полезной информацией). Например, возьмем фисташковый цвет (190, 245, 116), красный канал характеризуется числом 190 — рис. 1. Переведем его в двоичную систему счисления: $190_{10} = 1011\ 1110_2$. Допустим, что часть полезной информации представлена как 11_2, заменяем два младших бита числа двумя битами полезной информации и получаем $1011\ 1111_2 = 191_{10}$. Таким образом, мы получили пиксель другого цвета #bff574 (191, 245, 116) — рис. 2. Человеческий глаз не способен заметить разницу, а значит, факт передачи и сокрытия информации останется в тайне.

Рис. 1. Фисташковый (190, 245, 116)

Рис. 2. #bff574 (191, 245, 116)

Необходимо внимательно выбирать контейнер среди изображений. Изображение должно быть цветным, без явного преобладания одного цвета и однотонной заливки. Пиксели выбираются не подряд, а с некоторыми пропусками, для усложнения стегоанализа. Также можно использовать алгоритмы шифрования для при-

дания сообщению свойств случайного набора данных, однако это уже второй рубеж защиты. Вместо шифрования мы используем электронную цифровую подпись алгоритмом RSA. При выборе контейнера стоит придерживаться следующих правил:

1) следует использовать два бита контейнера для хранения сообщения и не заполнять контейнер полностью. Желательно, чтобы сообщение составляло не более 10 % объема контейнера;

2) большое количество мелких и разноцветных деталей на изображении позволит повысить надежность сокрытия;

3) использовать изображения из свободного доступа не рекомендуется, так как банальное сравнение исходного и полученного изображения позволит сразу найти сообщение.

Описание программы. Программа состоит из двух частей: первая — сокрытие сообщения в изображении, вторая — получение сообщения и анализ целостности файла. Анализ целостности файла происходит с помощью электронной цифровой подписи (ЭЦП) алгоритмом RSA. Это криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. В приложении предусмотрены два режима работы, которые меняются с помощью переключателя. Для наглядности показывается изображение до преобразования и после (рис. 3).

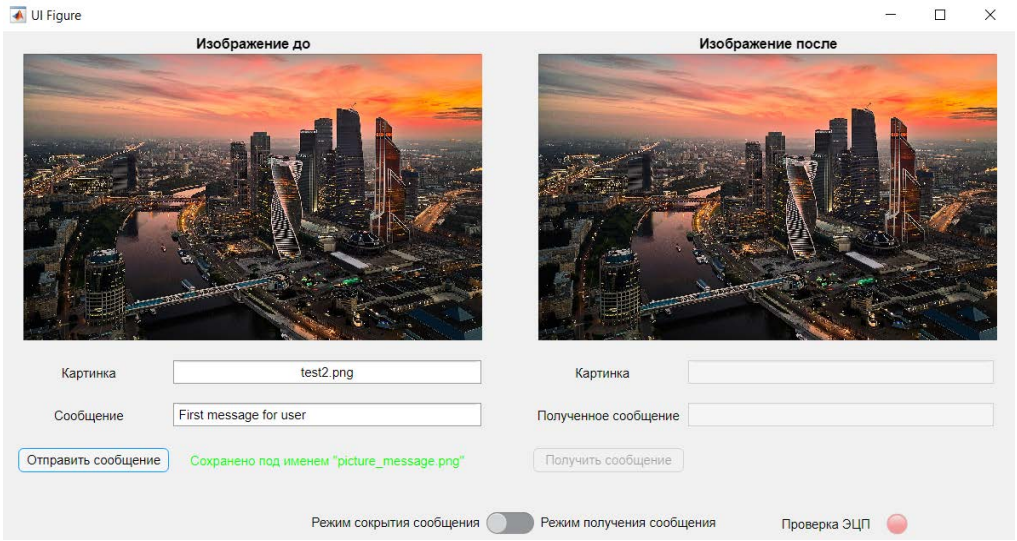

Рис. 3. Режим сокрытия сообщения

В первом режиме пользователь вводит в поле название изображения, которое будет являться контейнером. Далее он пишет сообщение в соответствующее поле и нажимает кнопку «Отправить сообщение». Приложение прячет текст в контейнер и сохраняет новое изображение в папку с программой. Определенный пиксель содержит информацию о длине сообщения. Затем пользователь может передать изображение другому пользователю любым способом по сети, так как файл формата PNG сжимается без потерь. В алгоритме программы предусмотрено ±1 кодирование изображения, что затрудняет стегоанализ ста-

тистическими методами, например, атака Хи-квадрат и RS-метод. Кодирование ±1 заключается в изменении не только двух последних битов в пикселе, а еще и в прибавлении к значению всего байта либо −1, либо +1. При этом учитываем, что к 0 мы только прибавляем 1, а от 255 только отнимаем 1. Таким образом мы вносим изменения в два младших бита всего изображения, что позволяет обойти автоматические средства детектирования и поиска.

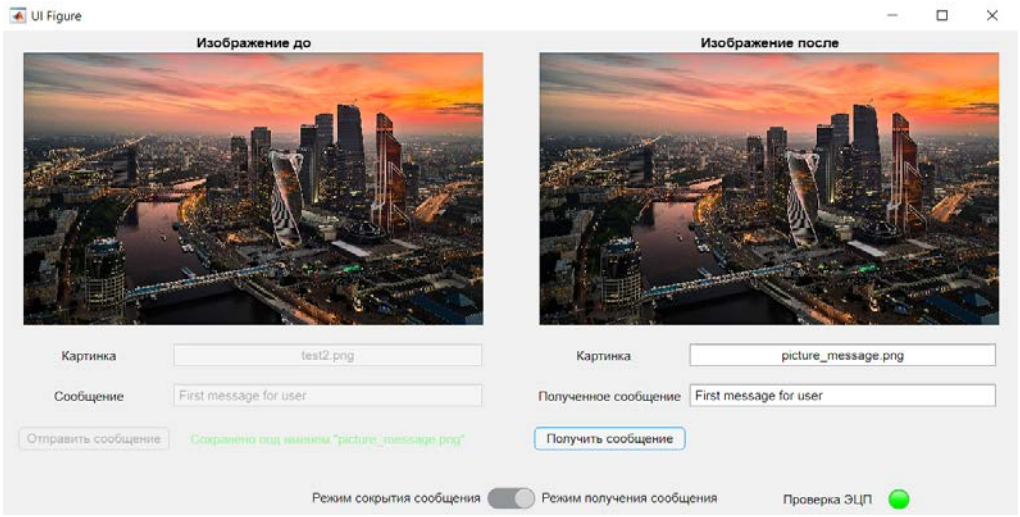

Рис. 4. Режим получения сообщения

В режиме получения сообщения пользователь извлекает сообщение из контейнера. Вводит название файла в соответствующее поле, нажимает кнопку «Получить сообщение», после чего информация из файла показывается в поле «Полученное сообщение», а индикатор «Проверка ЭЦП» показывает, что файл не менялся при передаче, и становится зеленым (рис. 4).

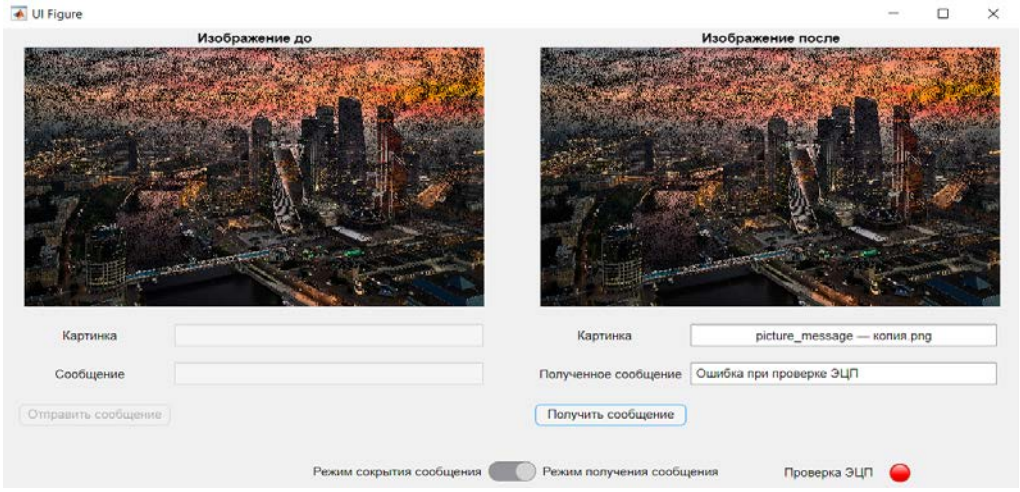

Рис. 5. Проверка работы ЭЦП

Представим, что файл был поврежден в процессе передачи и изменим его. В таком случае алгоритм ЭЦП RSA позволяет сделать вывод о нарушенной целостности файла и индикатор «Проверка ЭЦП» станет красным (рис. 5).

Заключение. Рассмотрен стеганографический алгоритм LSB в среде MATLAB App Designer. Выявлены сильные и слабые стороны алгоритма, указаны правила подбора изображения (контейнера). В алгоритм внедрены средства, позволяющие обойти средства автоматического поиска, основанные на статистических методах. Описана программа, позволяющая пользователям обмениваться информацией, пересылая друг другу изображения. Каждый из них записывает и получает сообщения с помощью данного приложения.

Литература

[1] Аграновский А.В., Балакин А.В., Грибунин В.Г. и др. Стеганография, цифровые водяные знаки и стегоанализ. М., Вузовская книга, 2009.
[2] Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М., Солон-Пресс, 2002.
[3] Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии. М., Горячая линия Телеком, 2013.
[4] Завьялов С.В., Ветров Ю.В. Стеганографические методы защиты информации. СПб., Изд-во СПбПУ, 2012.
[5] Грибунин В.Г., ред. Стеганографические системы. Критерии и методическое обеспечение. Саров, ФГУП «РФЯЦ-ВНИИЭФ», 2016.
[6] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев, МК-Пресс, 2006.
[7] Мао В. Современная криптография, Теория и практика. М., Вильямс, 2005.
[8] Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М., Научный мир, 2004.
[9] Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М., Горячая линия-Телеком, 2011.
[10] Габидуллин Э.М., Пилипчук Н.И. Лекции по теории информации. М., МФТИ, 2007.

Яковлев Андрей Юрьевич — студент кафедры «Системы автоматического управления», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Кваша Владимир Сергеевич, кандидат технических наук, старший преподаватель кафедры «Космические войска, противоракетная оборона», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Яковлев А.Ю. Реализация стеганографического алгоритма LSB в среде MATLAB App Designer. *Политехнический молодежный журнал*, 2020, № 02(43). http://dx.doi.org/10.18698/2541-8009-2020-02-582

LSB STEGANOGRAPHIC ALGORITHM IMPLEMENTATION IN MATLAB APP DESIGNER

A.Yu. Yakovlev
andrey.67.rus@yandex.ru
SPIN-code: 6420-6870

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The LSB steganographic algorithm and its implementation in a GUI application with MATLAB App Designer are described. Computer and digital steganography are considered and an algorithm is implemented that allows one to hide useful information in an image. This application allows users to secretly exchange text messages using images of certain formats. These image formats use lossless compression algorithms. The program provides algorithms that make it difficult to steganalize files by statistical methods. An RSA electronic digital signature algorithm is also implemented, which allows you to confirm the authorship of the user and verify the integrity of the message.

Keywords

Steganography, MATLAB, App Designer, LSB algorithm, image processing, stegoanalysis, graphical user interface, RGB image model

Received 13.02.2020

References

[1] Agranovskiy A.V., Balakin A.V., Gribunin V.G., et al. Steganografiya, tsifrovye vodyanye znaki i stegoanaliz [Stenography, digital watermarks and stegoanalysis]. Moscow, Vuzovskaya kniga Publ., 2009 (in Russ.).

[2] Gribunin V.G., Okov I.N., Turintsev I.V. Tsifrovaya steganografiya [Digital stenography]. Moscow, Solon-Press Publ., 2002 (in Russ.).

[3] Ryabko B.Ya., Fionov A.N. Osnovy sovremennoy kriptografii i steganografii [Basics of modern cryptography and stenography]. Moscow, Goryachaya liniya Telekom Publ., 2013 (in Russ.).

[4] Zav'yalov S.V., Vetrov Yu.V. Steganograficheskie metody zashchity informatsii [Stenographical methods of information protection]. Sankt-Petersburg., Izd-vo SPbPU Publ., 2012 (in Russ.).

[5] Gribunin V.G., ed. Steganograficheskie sistemy. Kriterii i metodicheskoe obespechenie [Stenographical systems. Criteria and methodological support]. Sarov, FGUP "RFYaTs-VNIIEF" Publ., 2016 (in Russ.).

[6] Konakhovich G.F., Puzyrenko A.Yu. Komp'yuternaya steganografiya. Teoriya i praktika [Computer stenography. Theory and practice]. Kiev, MK-Press Publ., 2006 (in Russ.).

[7] Mao W. Modern cryptography. Upper Saddle River, Pearson Education, 2004. (Russ. ed.: Sovremennaya kriptografiya, Teoriya i praktika. Moscow, Vil'yams Publ., 2005.)

[8] Ryabko B.Ya., Fionov A.N. Osnovy sovremennoy kriptografii dlya spetsialistov v informatsionnykh tekhnologiyakh [Basics of modern cryptography for specialists in information technologies]. Moscow, Nauchnyy mir Publ., 2004 (in Russ.).

[9] Barichev S.G., Goncharov V.V., Serov R.E. Osnovy sovremennoy kriptografii [Fundamentals of modern cryptography]. Moscow, Goryachaya liniya-Telekom Publ., 2011 (in Russ.).
[10] Gabidullin E.M., Pilipchuk N.I. Lektsii po teorii informatsii [Lections on information theory]. Moscow, MFTI Publ., 2007 (in Russ.).

Yakovlev A.Yu. — Student, Department of Automatic Control Systems, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Kvasha V.S., Cand. Sc. (Eng.), Senior Lecturer, Department of Space Forces, Missile Defense, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Yakovlev A.Yu. LSB Steganographic Algorithm Implementation in MATLAB App Designer. *Politekhnicheskiy molodezhnyy zhurnal* [Politechnical student journal], 2020, no. 02(43). http://dx.doi.org/ 10.18698/2541-8009-2020-02-582.html (in Russ.).