УДК 004.021

О МЕТОДАХ СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ

Кривчикова А. С, Черноморец А. А
Белгородский государственный национальный исследовательский университет, Россия
e-mail: 1855159@bsuedu.ru, chernomorets@bsuedu.ru

В данной статье представлен аналитический обзор методов стеганографического внедрения данных в цифровые изображения. Стеганография занимается скрытым обменом информацией, предназначенным для конфиденциальной передачи данных между сторонами, с целью сохранить сам факт передачи в тайне. Основное внимание в статье уделено различным алгоритмам и методам стеганографического скрытия информации, а также их сравнительному анализу.

Ключевые слова: стеганография, встраивание информации, метод наименее значимого бита (LSB), метод псевдослучайной перестановки, метод замены палитры.

ABOUT METHODS OF STEGANOGRAPHIC HIDING OF INFORMATION IN IMAGES

Krivchikova A. S., Chernomorets A. A
Belgorod National Research University, Russia
e-mail: 1855159@bsuedu.ru, chernomorets@bsuedu.ru

This article presents an analytical review of methods of steganographic embedding of data in digital images. Steganography deals with hidden information exchange intended for confidential transmission of data between parties in order to keep the fact of transmission secret. The main attention in the article is paid to various algorithms and methods of steganographic hiding of information, as well as their comparative analysis.

Keywords: steganography, information embedding, least significant bit (LSB) method, pseudorandom permutation method, palette substitution method.

Введение

Цель криптографии заключатся в том, чтобы скрыть содержание сообщений. В то время как стеганография стремиться не только скрыть содержание сообщения, но и скрыть сам факт передачи сообщения. Такие скрытые сообщения могут быть встроены в различные данные, например, в изображение или в видео, что позволяет передавать их, не вызывая подозрений со стороны.

Стеганография играет важную роль в обеспечении безопасности информации: она не является заменой криптографии, а служит ее дополнением, защищая данные от лиц, которым она не предназначена. Использование методов стеганографии для скрытия сообщения уменьшает вероятность выявления факта его передачи. При этом если само сообщение было зашифровано, то оно получает большую защиту. [1]

Методы стеганографии

Один из методов стеганографии является метод наименее значащего бита известный (LSB). Данный метод является одним наиболее распространённым среди методов замены в пространственной области.

Младший значащий бит изображения содержит в себе наименьшее количество информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, младший значащий бит можно рассматривать как шум, в результате чего, появляется возможность встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. В случае изображений в градациях серого объем встроенных данных может составлять 1/8 от общего объема контейнера. [2]

Широкое применение данного метода связано с его простой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации. Метод наименее значащего бита применим к изображениям в форматах без сжатия или со сжатие без потерь. Это связано с тем, что при сжатии с потерями информация, скрытая в менее значащих битах, может быть утеряна.

Следующим рассматриваемым методом является метод псевдослучайной перестановки. Метод псевдослучайных перестановок – это метод стеганографии, при котором биты скрытого сообщения распределяются по изображению случайным образом.

Суть метода псевдослучайной перестановки заключается в том, что генератор псевдослучайных числе генерирует последовательность индексов $j_1, j_2, \ldots, j_N$ и после чего k-й бит сообщения сохраняется в пикселе с индексом j_k.

Пусть N – общее количество бит (самых младших) в контейнере, P^N – перестановка чисел от 1 до N, если есть сообщение для скрытия длинной n бит, то эти биты можно встроить вместо бит контейнера $P^N(1), P^N(2), \ldots, P^N(n)$. При этом функция перестановки должна быть псевдослучайной, то есть, она должна обеспечивать выбор бит контейнера приблизительно случайным образом. В результате биты сообщения будут равномерно распределены по всему битовому пространству контейнера. [3]

Такой подход скрытия информации в контейнере значительно усложняет процесс обнаружения сообщения, особенно в случае, если генератор псевдослучайных чисел работает по сложному алгоритму.

Другим методом для стеганографического скрытия информации является метод замены палитры. Данный метод основан на использовании специфических особенностей формата контейнера и предназначен для скрытия текстовой информации в графических файлах,

которые используют цветовые палитры. К таким файлам относятся, например, BMP, GIF и PCX.

Суть метода замены палитры заключается в том, что искажаются не сами цвета, а их номера. Однако, благодаря, предварительно отсортированной палитре, цвет точки заменяется на схожий, который практически невозможно отличить от исходного цвета из-за их малого различия. [3]

Один из вариантов метода заключается в упорядочивании палитры перед скрытием информации таким образом, чтобы соседние цвета стали более схожими. Например, цвета могут быть упорядочены по расстоянию в RGB-пространстве. После сортировки палитры индексы цветов могут быть изменены без значительного искажения изображения.

Другой вариант метода замены палитры заключается в снижении общего числа цветовых значений путем «размытия» изображения. В данном случае элементы палитры дублируются так, что различие в их цветовых значениях становиться несущественным. В результате каждое цветовое значение размытого изображения соответствует двум элементам палитры, выбор которых осуществляется в зависимости от бита скрываемого сообщения.

Информация, скрытая методом замены палитры, является не заметной для человека, что делает ее труднодоступной для посторонних лиц. Также замена палитры позволяет сохранить качество и исходный вид изображения.

В таблице 1 приведен сравнительный анализ рассмотренных методов.

Таблица 1 - Сравнительный анализ рассмотренных методов

Метод	Преимущества	Недостатки
Метод наименее значащего бита	Простая реализация; Минимальное влияние на качество итогового изображения.	Уязвим для стегоанализа; Зависит от качества исходного изображения; Неприменим для записи в файлы формата с сжатием;
Метод псевдослучайной перестановки	Метод вставляет биты сообщения, изменяя порядок их следования, что усложняет процесс обнаружения и расшифровки информации;	Бит сообщения, вставленный случайным образом в младший бит контейнера, может быть поврежден; При вставке бит сообщения не в последние биты, может появится

	Биты скрываемого сообщения равномерно распределены по всему контейнеру.	дополнительный шум в изображении.
Метод замены палитры	Возможность скрыть конфиденциальную информацию путём перестановки цветов в палитре, поскольку порядок цветов не важен для восстановления общего изображения; Возможность изменения младших бит цветовых индексов без значительного искажения изображения.	Методы, в основе которых лежит порядок формирования палитры, неустойчивы; Добавление нескольких одинаковых цветов в палитру может уменьшить стойкость метода.

Таким образом, по итогам сравнительного анализа рассмотренных методов можно заметить, что среди рассмотренных методов метод псевдослучайной перестановки является наиболее надежным. Это связано с тем, что результаты его применения сложнее обнаружить, а также они обладают хорошей устойчивостью к стегоатакам. Метод замены палитры также эффективен, но может вызвать изменения в качестве итогового изображения. Метод наименее значащего бита является менее надежным по сравнению с другими методами, так как его изменения довольно легко можно обнаружить.

Список литературы:

1. Вилкина К. А., Клебеко Е. Ю., Носкович П. Н. Стеганографические методы защиты информации // Конференция «Компьютерные системы и сети». 2023. [Электронный ресурс]. URL: https://libeldoc.bsuir.by/bitstream/123456789/52777/1/Vilkina_Steganograficheskie.pdf

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2016. 262 с.

3. Коханович Г. Ф., Пузыренко А. Ю. Компьютерная стенография. Теория и практика. – К.: «МК-Пресс», 2006, 288 с.