УДК 004.056.5 + 681.3

Ражков А.Ф., Тимощенко Е.В.

ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА КОХА И ЖАО ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ

МГУ имени А.А.Кулешова, Могилёв, Беларусь

Поскольку увеличивающееся количество данных хранится в компьютерах и передаётся по сетям, не удивительно, что стеганография, целью которой является тайная передача информации, вошла в цифровой век. В компьютерах и сетях стеганографические приложения позволяют кому-нибудь скрыть любой тип бинарного файла в любом другом бинарном файле, однако, благодаря большой популярности социальных сетей, именно графические и звуковые файлы являются сегодня самыми распространенными носителями для транспортировки зашифрованной информации.

С помощью стеганографии, которая скрывает сам факта передачи информации, обычное изображение может хранить не только графическую информацию. Это может быть полезно во многих сферах деятельности человека, но чаще всего используется в области информационной безопасности и защиты информации.

Таким образом, в виду очевидной актуальности и востребованности темы исследования, было решено разработать программное обеспечение, которое будет использовать стеганографические методы сокрытия информации в цифровых изображениях. При этом, кодирование будет производиться с помощью метода сокрытия в частотной области изображения. Стоит отметить, что размер и качество изображения, при встраивании в него информации, остается практически неизменным. Следовательно, можно хранить в открытом доступе или передавать по открытым каналам связи почти любую конфиденциальную информацию.

Метод, который будем использовать при разработке программы для сокрытия информации в изображениях форматов BMP, PNG является одним из наиболее распространенных на сегодня методов скрытия конфиденциальной информации в частотной области изображения. Метод заключается в относительной замене величин коэффициентов дискретно-косинусного преобразования (ДКП) – метод Коха и Жао [1].

Достоинство метода Коха-Жао состоит в устойчивости к большинству известных стеганоатак, в том числе к атаке сжатием, к аффинным преобразованиям, геометрическим атакам.

Среди недостатков метода: низкая пропускная способность; слабая приспособленность некоторых блоков 8×8 к встраиванию данных; блоки с резкими перепадами яркости содержат большие абсолютные значения в

ВЧ области, что может привести к очень большим искажениям при встраивании информации; модификация СЧ области, содержащей компоненты монотонных изображений, приведет к внесению видимых искажений.

Недостаток низкой пропускной способности метода было решено исправить путем выбора на начальном этапе размерности блоков не только 8×8 пикселей, но и 4×4, 2×2.

При разработке ПО было решено использовать среду .NET, позволяющую применять принципы объектно-ориентированного программирования и язык C# использовался как средство разработки и реализации программ.

Скрытая передача секретного изображения происходит по открытому каналу, где вначале пользователь использует программу для встраивания информации, чтобы скрыть информацию, а другой пользователь, получатель изображения, использует программу для извлечения скрытой информации [2].

Кроме непосредственного сокрытия информации дополнительно в программу решено было ввести такие функции, как «Сравнение изображений» для сравнения двух изображений на наличие пикселей, отличающихся друг у друга, и «Очистка изображения» для внедрения в изображения заведомо случайной информации, благодаря которому невозможно будет получить встроенную в изображение информацию.

На изображениях ниже представлен интерфейс разработанного приложения, где рисунок 1, а иллюстрирует главную форму, а рисунок 1, б – изображение процесса сокрытия информации.

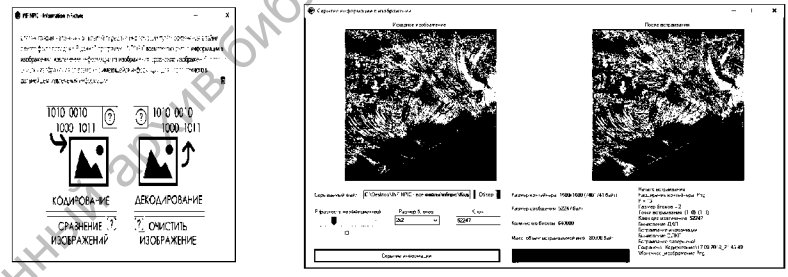

Рисунок 1 – Интерфейс приложения

Приложение отвечает всем требованиям, предъявляемым к стеганографическому программному обеспечению, и может использоваться для сокрытия данных в графических файлах форматов BMP, PNG.

После завершения разработки было проведено тестирование программного средства на ряде фотографий. Результаты тестирования на скрытность встраивания и полезный объем байтов для встраивания являются хорошими.

Литературные источники.

1. Васина Т. С. Обзор современных алгоритмов стеганографии // Электронное научно-техническое издание «Наука и образование», МГТУ им. Н.Е. Баумана, 2012. - с. 1-8.

2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — с. 130-135.

A.F.Razhkov, E.V. Timoshchenko

THE USE OF STEGANOGRAPHIC METHOD, KOCH AND ZHAO TO CONCEAL INFORMATION IN DIGITAL IMAGES

Mogilev state University named A. A. Kuleshov

Summary

The analysis of the existing steganographic methods of hiding data in digital images was carried out in order to use it as the main one in software development. The method of hiding data in the frequency domain was chosen using the improved method of relative replacement of the values of the discrete-cosine transform coefficients (Koch and Zhao method). As a result, an INFINPIC application was developed to hide data in BMP and PNG images.