СТЕГАНОГРАФИЧЕСКИЙ ПРОГРАММНЫЙ МОДУЛЬ

О.Д. Чкоидзе

Актуальность стеганографии заключается в том, что этот метод передачи информации является наиболее скрытным в реалиях новых информационных технологий. Основной задачей стеганографического программного средства является встраивание в цифровое изображение данных, предназначенных для передачи по стегоканалу, таким образом, чтобы исходное изображение было максимально схожим с результирующим. Стеганографическое программное средство должно использовать наиболее эффективные и актуальные стеганографические методы. Такими методами являются: метод наименьшего значащего бита (НЗБ) и метод дискретного косинусного преобразования (ДКП) [1]. Главным преимуществом НЗБ является достаточное количество бит, которое возможно записать в одно цифровое изображение, однако этот метод весьма неустойчив при сжатии изображения. ДКП в свою очередь достаточно устойчив к сжатию, но доступное количество бит для записи в разы меньше по сравнению с НЗБ. Важным элементом любого стеганографического программного средства является шифрование. В связи с возможной частичной потерей данных, алгоритмы симметричного шифрования наиболее применимы для задач стеганографии. Потеря данных обычно связана с особенностью сжатия некоторых форматов цифровых изображений.

Необходимо отметить, что при использовании вышеперечисленных стеганографических методов, возникает проблема извлечения встроенных данных, так как в случае разработанного программного средства, они могут быть распределены по нескольким цветовым каналам цифрового изображения и иметь разный размер. Поэтому, обязательной процедурой будет протоколирование процесса извлечения данных. Для этого был разработан отдельный алгоритм, отвечающий за определение размера и количества сегментов данных в каждом цветовом канале.

Литература

1. Global Journal of Computer Science and Technology. An Analysis of LSB & DCT based Steganography [Электронный ресурс]. – Режим доступа: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.178.7157&rep=rep1&type=pdf – Дата доступа: 30.04.2022.