

## ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ

Галлямова Миляуша Равильевна<sup>1</sup>, Ильченко Лидия Михайловна<sup>2</sup>  
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики «ИТМО»,  
Россия, Санкт-Петербург, Кронверкский просп., 49,  
emails: [Miljausha-18@mail.ru](mailto:Miljausha-18@mail.ru)<sup>1</sup>, [Lidiya9510@yandex.ru](mailto:Lidiya9510@yandex.ru)<sup>2</sup>

**Аннотация:** В статье рассматривается метод защиты информации с использованием методов цифровой стеганографии. Стеганография - это навык общения секретных данных путем встраивания его в мультимедийные носители как изображение, аудио, видео. Конечная цель здесь - замаскировать само существование встроенных данных.

**Ключевые слова:** стеганография, наименее значимый бит, цифровой водяной знак (ЦВЗ), несанкционированный доступ (НСД).

## METHOD OF PROTECTING INFORMATION AS DIGITAL STEGANOGRAPHY

Gallyamova Milyausha<sup>1</sup>, Ilchenko Lidiya<sup>2</sup>  
Saint Petersburg National research University of information technologies, mechanics and optics  
"ITMO",  
Russia, St. Petersburg, Kronverskiy avn. 49,  
emails: [Miljausha-18@mail.ru](mailto:Miljausha-18@mail.ru)<sup>1</sup>, [Lidiya9510@yandex.ru](mailto:Lidiya9510@yandex.ru)<sup>2</sup>

**Abstract:** This article discusses a method of protecting information as digital steganography. Steganography is the skill of communicating secret data by embedding it into multimedia carriers like image, audio, videos. The ultimate goal here is to mask the very existence of the embedded data.

**Keywords:** steganography, least significant bit (LSB), digital watermark (DWM), unauthorized access.

**Введение.** В современном мире информация является одним из важнейших аспектов жизни. В связи с этим, многие эксперты в области компьютерной безопасности, а также многие обычные пользователи компьютеров связаны с информационной безопасностью. В этой статье рассматривается метод защиты информации с использованием методов цифровой стеганографии.

Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Данные объекты являются мультимедиа файлами (изображения, видео, аудио, текст) с внесенными искажениями. Сегодня стеганография позволяет не только успешно решать основную задачу – скрытно передавать информацию, но и целый ряд других актуальнейших задач, в том числе встраивание скрытой информации с целью защиты авторских прав на интеллектуальную собственность, представленную в цифровом виде [Error: Reference source not found].

Эта скрываемая информация называется цифровым водяным знаком (ЦВЗ), который представляет собой специальную метку, содержащую информацию, однозначно подтверждающую авторство или права на коммерческое использование защищаемого объекта. Она незаметно внедряется в изображение или другой сигнал с целью тем или иным образом контролировать его использование. ЦВЗ активно используются при размещении уникальных фотографий, видео, аудио в электронном виде в сети Интернет. Первые работы по встраиванию водяных знаков были сделаны в 90-х годах 20 века.

**Типы ЦВЗ.** Как правило, различают три разных типа ЦВЗ: робастные, хрупкие и полухрупкие. Под робастностью понимается устойчивость ЦВЗ к различного рода воздействиям на стегоконтейнер. Такие ЦВЗ применяются для защиты авторских прав на интеллектуальную собственность, выставляемую в публичных компьютерных сетях. Хрупкие ЦВЗ разрушаются при незначительной модификации заполненного контейнера. Они применяются для аутентификации сигналов. Полухрупкие ЦВЗ устойчивы по отношению к одним воздействиям и неустойчивы по отношению к другим. ЦВЗ называют незаметным, если исходный и помеченный сигналы по определённым критериям восприятия неотличимы. Обычно легко сделать надёжный или незаметный ЦВЗ. Но, как правило, тяжело сделать ЦВЗ незаметным и надёжным одновременно. ЦВЗ могут представляться в виде битовой последовательности, изображения или последовательности с плавающей точкой.

**Области применения ЦВЗ.** Встраивание ЦВЗ в медиафайлы может быть использовано для следующих целей:

1. Встраивание информации с целью ее скрытой передачи.
2. Встраивание ЦВЗ с целью защиты авторских прав на интеллектуальную собственность, представленную в цифровом формате.
3. Маркирование идентификационными номерами для отслеживания путей распространения нелегальных копий продукта, используя технику уникальной подписи для каждой легальной копии.
4. Встраивание с целью защиты от копирования медиафайла.
5. Мониторинг широкоэмитерных каналов.
6. Встраивание с целью проверки целостности переданных данных.
7. Встраивание с целью индексации частей файла.
8. Встраивание ЦВЗ для подписи медицинских снимков или нанесения легенды (картография) на карту.

**Методы и алгоритмы цифровой стеганографии.** Методы, использующие для скрытия данных частотную область, являются более стойкими к различным возможным внешним воздействиям на изображение-контейнер. В этой группе используются достаточно разнообразные трансформации:

- дискретное косинус-преобразование (ДКП);
- вейвлет-преобразование (ДВП);
- дискретное преобразование Фурье (ДПФ);
- преобразование Карунена-Лоева (ПКЛ);
- сингулярное разложение.

**Заключение.** Цифровая стеганография - динамичная и быстро развивающаяся наука, которая использует методы и достижения криптографии, цифровой обработки сигналов, теории коммуникации и информации. Наряду с обычным пользователем также заинтересованы крупные компании, работающие в области мультимедиа, стремясь защитить свой контент от незаконного использования. Это не привлекает внимания, в отличие от чистой криптографии. Анализ тенденций в цифровой стеганографии показывает, что в ближайшие несколько лет интерес к разработке своих методов будет расти все больше и больше.

## СПИСОК ЛИТЕРАТУРЫ

- 1 Грибунин В.Г., Оконов И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002- 272 с.
- 2 Хорошко В.О., Азаров О.Д., Шелест М.Э., Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов.- Винница: ВДТУ, 2003.-143 с.
- 3 Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика И: "МК-Пресс" 2006. с. 283.

- 4     Marks, W.B., Dobelle, W.H.  
     & MacNichol, E.F. Visualpigments of single primate cones. *Science* (1964) 143:1181—1183.