УДК 004:056-53

ИСПОЛЬЗОВАНИЕ МЕТОДА LSB ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ В BMP ФАЙЛАХ

Стрельцова А.С., студентка 4 курса факультета математики, информационных и авиационных технологий
Научный руководитель – Иванцов А.М., кандидат технических наук, доцент
ФГБОУ ВО УлГУ

Ключевые слова: *защита информации, стеганография, метод наименьшего значащего бита.*

Работа описывает реализацию одного из методов стеганографии для скрытие конфиденциальной информации в файлах bmp формата от потенциального нарушителя. Стеганография является эффективным программно-техническим методом сокрытия данных и защиты их от несанкционированного доступа. Эффективное использование стеганографии совместно с другими методами защиты информации обеспечит многоуровневую безопасность.

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. В данной работе предлагается использование метода стеганографии для решения данной проблемы. Актуальность работы заключается в том, что нередко возникает необходимость передать конфиденциальное сообщение небольшого объёма, при этом использование сложных криптографических систем по ряду причин затруднительно. Одной из таких причин является невозможность использования надёжных компьютерных продуктов, которые, как правило, являются коммерческими и для обычного пользователя компьютера недоступны.

Стеганография является наукой, разрабатывающей приемы обмена информацией таким образом, что скрывается сам факт существования секретной связи. При обработке данных стеганографическими методами происходит скрытие передаваемой информации в других объектах таким образом, чтобы постороннее лицо даже не догадывалось о существовании скрытого секретного сообщения [1].

Скрываемая информация называется стеганограммой или просто стего. Данные, среди которых она прячется, играют роль информационного контейнера.

Нарушитель имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному нарушителя, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения; если нарушитель каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне.

Большинство методов компьютерной стеганографии базируется на двух принципах:

- первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением), могут быть до определенной степени видоизменены без потери функциональности;

- второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в таких исходных файлах [2].

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначимых фрагментов среды и замена существующей в них информации на информацию, которую предполагается скрыть[2].

Метод замены наименее значащего бита (НЗБ, LSB – Least Significant Bit) наиболее распространен среди методов замены в пространственной области [1]. Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, LSB – это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. При этом, для изображения в градациях серого (каждый пиксель изображения кодируется одним байтом) объем встроенных данных может составлять 1/8 от общего объема контейнера. Например, в изображение размером 512x512 можно встроить ~ 32 кБайт информации.

Для встраивания будет использоваться информация о цвете каждого пикселя изображения. Цвет пикселя определяется объединением трех основных цветовых составляющих: красной, зеленой и синей (сокращенно, RGB). Каждой из них соответствует свое значение интенсивности, которое может изменяться от 0 до 255. Следовательно, за

каждый из цветовых каналов отвечает 8 битов (1 байт), а глубина цвета изображения в целом – 24 бита (3 байта).

При реализации данного метола в качестве контейнера используется bmp-файл, так как он не привязан к конкретной аппаратной платформе. Этот файл состоит из четырех частей: заголовка, информационного заголовка, таблицы цветов (палитры) и данных изображения[3]. Будет использоваться информационный заголовок, который начинается с собственной длины и содержит размеры изображения, разрешение, характеристики представления цвета и другие параметры.

Можно сделать вывод, что метод LSB заключается в следующем - заменяются младшие биты в байтах, отвечающих за кодирование цвета., таким образом происходит скрытие конфиденциальной информации в изображении. Допустим, если очередной байт нашего секретного сообщения – 11001011, а байты в изображении –…11101100 01001110 01111100 0101100111…, то кодирование будет выглядеть следующим образом, разобьём байт секретного сообщения на 4 двухбитовые части: 11, 00, 10, 11, и заменим полученными фрагментами младшие биты изображения: …11101111 01001100 01111110 0101100111…. Такая замена в общем случае не заметна. Многие старые устройства вывода, даже не смогут отобразить такие незначительные перемены в изображении. Можно менять не только два младших бита, но и любое их количество. Есть следующая закономерность, чем большее количество бит мы меняем, тем больший объём информации мы можем скрыть, и тем большие помехи в исходном изображении это вызовет для потенциального нарушителя.

Библиографический список:

1. Аграновский, А.В. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.

3. Барсуков, В.С. Стеганографические технологии защиты документов, авторских прав и информации / В.С. Барсуков // Обзор специальной техники. – 2000. – № 2. – С. 31 – 40.

3. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцив. – М.: Солон-Пресс, 2016. – 262 с.

LSB USING METHODS TO HIDE THE INFORMATION IN THE BMP FILE

Streltsova A.S., Ivantsov A.M.

Keywords: *information security, steganography, the method of the least significant bit*

The work describes the implementation of a method of steganography to hide sensitive information in files bmp format from a potential intruder. Steganography is an efficient software and hardware method of concealing data and protect them from unauthorized access. Effective use of steganography in conjunction with other methods of information protection provide a multi-level security.

УДК 004.9

ОНТОЛОГИИ В ИНФОРМАТИКЕ И МЕДИЦИНЕ

Суворова А.А., студентка 1 курса факультета ветеринарной медицины и биотехнологии
Научный руководитель – Видеркер М.А.,
кандидат биологических наук, доцент
ФГБОУ ВО Ульяновская ГСХА

Ключевые слов: *онтология, IDEF5, язык описания онтологий, медицина.*

В работе рассмотрены онтологии, как способ представления знаний, описано их использование в различных областях деятельности человека. Представлены примеры использования онтологий в медицине.

Последние годы онтологии (как метод представления информации) являются объектом пристального внимания в области искусственного интеллекта. На их основе могут формироваться базы знаний для различных интеллектуальных систем, в частности – экспертных [1, 2].

Онтология (в информатике) – это методология детальной формализации некоторой области знаний с помощью концептуальной схемы. Она состоит из экземпляров, понятий, атрибутов, отношений [1].

Согласно стандарту онтологического исследования IDEF5 при построении онтологии должны быть выполнены следующие задачи [2]:

1) создания глоссария;

2) описание правил и ограничений, для формирований новых достоверных утверждений, описывающих систему;

3) построение модели, которая позволит сформировать новые утверждения.