СТЕГАНОГРАФИЧЕСКИЙ АЛГОРИТМ ДОПОЛНИТЕЛЬНОГО СЖАТИЯ БИТ

Трифонов Е.О.
Научный руководитель: д-р техн. наук Ярмолик В.Н.
Белорусский государственный университет информатики и радиоэлектроники, Беларусь
E-mail: naffer@tut.by

Аннотация — Описание идеи и важных моментов стеганографического алгоритма дополнительного сжатия бит. Приведена собранная статистика использования алгоритма.

1. Введение

Задача надежной защиты информации (ЗИ) от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени. Одним из способов решения этой задачи может выступать стеганография, как самостоятельно, так и в совокупности с другими методами ЗИ, например, криптографией. Развитие цифровой стеганографии ведется в двух направлениях: уменьшение влияния секретной информации на контейнер, а также увеличение объема встраиваемой информации.

В докладе представлен алгоритм, призванный увеличивать вместимость контейнера и уменьшить влияние встраиваемых данных на контейнер одновременно, а также статистика его применения. Он является независимым от цифрового стеганографического контейнера и алгоритма упаковки сообщения в этот контейнер.

2. Основная часть

Алгоритмы цифровой стеганографии, как правило, базируются либо на особенностях формата цифрового контейнера, либо на избыточности информации в нем. Так или иначе, в цифровом контейнере, помимо встраиваемой информации, находятся некоторые данные — биты: нули и единицы. Алгоритм дополнительного сжатия бит (ДСБ) базируется как раз на данных, находящихся в контейнере, он использует их для дополнительного сжатия встраиваемой информации.

Алгоритм ДСБ применяется вместе с любым алгоритмом стеганографии. Стеганографический алгоритм определяет области контейнера, в которые может быть записана секретная информация, такие области отмечаются как области для записи, все остальные области контейнера помечаются как области только для чтения. Затем алгоритм ДСБ ищет совпадения последовательностей бит секретной информации и информации, находящейся в контейнере, промаркированной только для чтения, потому как данная информация не будет изменена в ходе встраивания секретного сообщения. Встраиваемая информация делится на два типа последовательностей: исходная и замененная (или указатель).

Исходная последовательность представляется следующим образом:

Флаг	Длина	Последовательность бит

«Флаг» — 1 бит, который указывает, является ли последовательность исходной;

«Длина» — переменное число бит, рассчитываемое на основе длины оставшегося сообщения; указывает, сколько следующих бит являются исходным сообщением;

«Последовательность бит» — число бит последовательности; часть исходного сообщения.

Указатель представляется следующим образом:

Флаг	Номер бита	Длина

«Флаг» — 1 бит, который указывает, является ли последовательность замененной;

«Номер бита» — переменное число бит, рассчитываемое на основе размера контейнера; номер бита в контейнере, с которого нужно начинать читать последовательность;

«Длина» — переменное число бит, рассчитываемое на основе длины оставшегося сообщения; число бит замененной последовательности.

Таким образом, вся встраиваемая последовательность разбивается на последовательности, часть из них исходные, остальные — указатели. Разумно использовать указатель в тех случаях, когда длина указателя меньше длины заменяемой последовательности, таким образом, секретное сообщение «сжимается». Важно, чтобы «сжатое» секретное сообщение было меньше исходного, иначе в использовании алгоритма нет выгоды. Использование алгоритма можно прописать в заголовке встраиваемой информации, это займет всего один бит.

Алгоритм был протестирован на графических стеганографических контейнерах формата *Bitmap Picture*. В качестве секретного сообщения использовались: текс, архив и изображение.

Таблица 1

	Текс	Архив	Изобр.
Средняя длина последов, бит	19,64 … 26,47	17,05 … 21,5	16,76 … 21,64
Макс. длина последов, бит	35 … 52	136 … 766	136 … 364
Кол-во последов.	0 … 7	3 … 8	5 … 12
Сжатие, %	0 … 0,48	6,85 … 10,4	0,72 … 2,46

3. Заключение

Из таблицы 1 видно, что текстовое секретное сообщение для графических стеганографических контейнеров «сжимается» слабо, это объясняется короткими совпадающими последовательностями бит текстового сообщения и графического контейнера. А вот встраивание изображения или архива в изображение происходит намного успешнее.

Описанный алгоритм ДСБ является вспомогательным для любого другого стеганографического алгоритма, и может быть использован для любого цифрового контейнера.

STEGANOGRAPHIC ALGORITHM OF THE ADDITIONAL BIT COMPRESSION

Trifonov E.O.
Scientific adviser: Yarmolik V.N.
Belarusian State University of Informatics and Radioelectronics, Belarus

Abstract — The idea and important spots of the steganographic algorithm of an additional bit compression are described. The results of the algorithm usage are presented.