Двухконтурная защита информации от несанкционированного доступа в стегосистемах

Выверица И.Н., Лавданский А.А., Фауре Э.В.
Кафедра компьютерных систем
Черкасский государственный технологический университет
Черкассы, Украина
e-mail: obi-wan@ua.fm

Аннотация—**Задача защиты информации играет важную роль в современной жизни. Встраивание цифровых водяных знаков – один из направлений цифровой стеганографии, которая применяется для защиты от копирования и несанкционированного использования мультимедийной информации. В работе рассмотрены основные методы встраивания цифровых водяных знаков, а также предложен способ обеспечения двухконтурной защиты информации от несанкционированного доступа в стегосистемах.**

Ключевые слова: стегосистема; контейнер; пиксель; гаммирование

I. Введение

Для передачи конфиденциальной информации используют криптографическую защиту. Криптографическая защита, в свою очередь, обеспечивает скрытие смыслового содержания информации, но не скрывает самого факта передачи. Для скрытия фактов передачи конфиденциальной информации используется стеганографическая защита — создание скрытого сообщения в сравнительно большом массиве открытых данных.

II. Двухконтурная защита информации от несанкционированного доступа в стегосистемах

Стеганографические способы защиты информации обеспечивают создание контейнеров — переносчиков скрываемой информации, в частности, в видео- и аудиофайлах. Все известные методы стеганографической защиты информации [1,2] основаны на устранении некоторой части избыточности сообщения, в объеме не влияющим на качество визуального (слухового) восприятия информации.

В работе производится оценка образованного в цветном неподвижном изображении, контейнера для переноса конфиденциальной информации, который основан на внедрении информации в малозначащие (младшие) разряды пикселов, составляющих видеоизображение. Особенностью образованного контейнера является то, что выбор деформируемых пикселов в младших разрядах производится неким, скрываемым от противника, случайным образом. В силу этого обстоятельства существенным является вопрос об определении допустимого значения числа сбойных пикселей в изображении, при котором искажения, вызванные сбоем в младших разрядах пикселя, незаметны на глаз. Проведенные эксперименты показали, что для цветного изображения размером 320x240 пикселей число сбойных пикселей не должно превышать (1-1,5)%. При таком числе деформированных скрытым сообщением пикселей размер контейнера составляет (768-1152) бит и, следовательно, такой же является длина кадра-носителя сообщения. Скрытый кадр данных должен иметь следующую структуру: преамбула, служебное сообщение, информационную и проверочную часть. Преамбула — это заголовок кадра, который служит для определения начала информационной части сообщения. Управляющее слово переносит некоторую служебную информацию, не относящуюся к самому сообщению. Проверочная часть служит для размещения избыточности, обеспечивающую защиту от ошибок, возникающих при транспортировке изображения по каналам связи с помехой. Для повышения защищенности от несанкционированного доступа часть кадра, следующего за преамбулой, подлежит шифрованию, например методом гаммирования, что образует криптосистему с симметричным ключом. Основной мерой защиты от несанкционированного доступа является выбор повреждаемых пикселов «случайным» образом по закону, не известному противнику. Закон перемещения по координатной сетке, составленной пикселами изображения, держится в секрете и имеет вид случайного стохастического процесса. Для этого на передающей и приемной стороне имеется два генератора стохастической случайной последовательности, один из них формирует случайное число по координате X (0-319), а другой — случайное число по координате Y (0-239), где числа X и Y статистически независимы. Ключ стохастического преобразования, определяющий закон перемещения по координатной сетке, един для отправителя и получателя и держится ими в секрете. Перемещение по координатной сетке является вторым контуром шифрования и определяет его как второй контур криптосистемы с секретным ключом.

Если для хранения ключей второго контура шифрования использовать секретную кодовую книгу (которая хранится у источника сообщения и приемника), ключи могут быть сделаны несимметричными. В этом случае стойкость стегосистемы возрастает. При такой схеме криптозащиты существенным является вопрос

синхронизации пикселей – выбора точки начала отсчета последовательности пикселей. Для обеспечения синхронизации пикселей преамбула представляет модулированный по фазе шумоподобный сигнал (ФМ ШПС) длиной Т бит, где T=T1T2, T1 — двоичная последовательность с «хорошей» автокорреляционной функцией (АКФ), выполняющая роль несущего колебания ФМ ШПС, а T2 — двоичная последовательность с «хорошей» АКФ, выполняющая роль модулирующего колебания ФМ ШПС. На приемной стороне с учетом неточности захвата нулевого пикселя в начале сообщения вместо одного пикселя, номер которого формирует по заданному ключу указатель координат ХУ, выбирается группа из 3х3 пикселей в окрестности указанной точки. Выделение синхропоследовательности (роль которой выполняет преамбула) производится по критерию максимального правдоподобия для каждой из 9 гипотез преамбулы. Процедура синхронизации завершена, если определен вектор максимального правдоподобия. В докладе определены основные качественные показатели стегосистемы, основанные на данном принципе.

[1] Оков И.Н., Ковалев Р.М. Электронные водяные знаки как средство аутентификации передаваемых сообщений // Защита информации. Конфидент. 2001. № 3, с.80-85.

[2] Оков И.Н. О требуемой пропускной способности каналов передачи аутентифицированных сообщений в безусловно стойких системах // Проблемы информационной безопасности. Компьютерные системы. 2000. № 3(7), с.78-64.