Системы телекоммуникации, связи и защиты информации

УДК 004.056: 621.397

А.Г. Власюк, д.-р. техн. наук, **А.А. Мужайло**, **Ю.Г. Савченко**, д.-р. техн. наук
Национальный технический университет Украины «Киевский политехнический институт»,
ул. Политехническая, 16, корпус 12, г. Киев, 03056, Украина

Пути увеличения полезного объема стеганоконтейнера за счет искусственного «зашумления»

На основе существующих подходов к применению стеганографии с различными контейнерами был проведен анализ известных методов, с использованием различных контейнеров. Проведено исследование влияния наличия в исходных контейнерах шумовых составляющих и оценка увеличения пропускной способности канала за счёт искусственного внесения шумовой составляющей в исходное изображение, что увеличивает пропускную способность стеганоканала (разумеется, количество информации, переносимое контейнером, соответственно уменьшится). Приведена общая схема организации стеганоканала путем предварительной коррекции файла контейнера, вычисления побитовой разницы между исходным файлом и его модификацией с вложением скрытой информации. Сформулированы рекомендации по использованию и выбору наиболее рационального метода в зависимости от поставленной задачи. Библ. 4, рис. 2, табл. 3

Ключевые слова: *стеганография; сокрытие информации; стеганоканал; генератор псевдослучайных чисел (ГПСЧ); искусственное зашумление; стеганоанализ; дискретно-косинусное преобразование; дифференциальное встраивание энергии (ДЭВ); метод наименее значимого бита (НЗБ); вейвлет-преобразование.*

Введение

В настоящее время проблема защиты информационных ресурсов становится все более острой в связи с широким использованием электронного документооборота, поскольку передача информации осуществляется, в основном, через незащищенные телекоммуникационные каналы. В то же время применение криптографического шифрования с целью исключения несанкционированного доступа не всегда решает проблему, поскольку привлекает нежелательное внимание к самому факту передачи важной информации. Как альтернативный путь в последнее время используют стеганографические методы, когда факт информационного обмена остается скрытым. Однако пропускная способность такого канала весьма ограничена.

Основные (но не единственные) методы встраивания скрытых сообщений базируются на аналоговой природе исходных файлов, используемых в качестве контейнеров для «транспортировки» скрытого сообщения. Речь, прежде всего, идет об аудио и графических файлах, предназначенных для прослушивания или просмотра. Учитывая несовершенство слуховой и зрительной системы человека с точки зрения разрешающей способности, часть информации, содержащаяся в файлах, может быть без ущерба для восприятия модифицирована или удалена. Именно эта часть, воспринимаемая человеком как шум, является полезной для организации скрытого информационного обмена и определяет потенциальную пропускную способность стеганоканала. Исходя из экспериментальных данных, разрешающая способность слуховой и зрительной системы человека не превышает 0,4…0,8%, т.е. человек различает не более $2^7…2^8$ уровней громкости или оттенков красного, голубого или зеленого цвета на изображении. Это означает, что после некоторого значения дальнейшее увеличение уровней квантования при оцифровке аналоговых сигналов и, соответственно, количество пикселей матрицы цифровой фотокамеры для человека не приводит к заметному ухудшению качества, т.е. незаметно.

Другими словами, если этот уровень превышен при передаче соответствующих файлов по реальному каналу, то имеет место избыточ-

ная и скрытая пропускная способность канала передачи C_γ. В общем случае оценить величину C_γ достаточно сложно, поскольку на нее существенно влияет способ преобразования аналогового сигнала в цифровой. Например, при аналогово-цифровом преобразовании аудио сигнала необходимо учитывать частоту дискретизации и требования к качеству передачи (полосу воспроизводимых частот или полосу пропускания используемого канала передачи). Так, в традиционных сетях многоканальной телефонной связи частота дискретизации f_d = 8кГц, и требуемое качество достигается при 8-битовом кодировании каждого отсчета. Реально без заметного для пользователя ухудшения качества можно уменьшить разрядность каждого отсчета до семи бит, а младший, наименее значащий бит (НЗБ) использовать для скрытого вложения (СВ).

По сути, это и есть основная идея метода НЗБ, который многократно описан в различных литературных источниках [1,2]. С другой стороны, этот «наименее значащий бит» можно интерпретировать как шум канала.

Постановка задачи

С точки зрения конечного пользователя, для которого предназначена информация контейнера, этот «шум» неотличим от шума, создаваемого помехами в канале, или шума, наложенного на первичный аналоговый сигнал при записи от микрофона (шум в помещении) или неравномерности освещения при съемке. Но этот шум независимо от его происхождения или источника для создания стеганоканала является полезным – чем больше такого «шума», тем лучше. Поэтому может быть оправданным искусственное внесение шумовой составляющей, что увеличивает пропускную способность стеганоканала (разумеется, количество информации, переносимое контейнером, соответственно уменьшится).

Необходимо, очевидно, проанализировать источники цифрового шума в файлах, используемых в качестве контейнеров, оценить его уровень и наметить пути целенаправленного искусственного увеличения шумовой составляющей.

Источники шума

Рассмотрим источники шума, которые могут оказаться полезными для увеличения полезного объема контейнера.

Цифровой шум – это дефекты изображения, которые вносятся матрицей цифрового фотоаппарата. Они видны как мелкие элементы изображения в виде светлых, темных или цветных точек, заполняющих целые области. Этот шум заметен на однотонных областях. Различают яркостный и хроматический шум. В первом случае это небольшие участки изображения, которые имеют отличия в яркости, во втором – в цвете. Уровень цифрового шума зависит от модели камеры и может быть снижен при использовании специальных программ шумоподавления.

Не останавливаясь здесь на детальном анализе физических и даже химических факторов, влияющих на уровень шума, отметим, что цифровой шум присутствует практически во всех изображениях, полученных с помощью цифровых фотокамер. Наиболее существенными факторами, влияющими на уровень шума, являются светочувствительность сенсора (матрицы) и экспозиция. Например, на затемненных недоэкспонированных участках изображения, а также на фотографиях, снятых с большой экспозицией при недостаточном освещении, можно увидеть небольшие разноцветные точки прямоугольной или неопределенной формы. На участках, которые хорошо освещены, как правило, шум не проявляется.

Другой важный параметр – экспозиция. Чем больше экспозиция, тем выше уровень шума. Это проявляется при ночной съемке и съемке без вспышки при слабом освещении.

Шумы, возникающие при сканировании изображений

Еще один распространенный вид цифрового шума – это помехи, которые возникают, например при использовании сканеров. Проявляется этот шум при увеличении изображений в виде точек (кластеров). Кроме того, уровень шума зависит, очевидно, от качества подложки (бумаги), на которой отпечатано (нарисовано) изображение. Ясно, что дефекты подложки также будут перенесены в файл при сканировании и эквивалентны шумовой составляющей.

Не нужно также забывать, что определенный уровень шума всегда присутствует в любом электрическом сигнале как результат внешних помех и наводок от посторонних источников электромагнитного излучения. Такой шум становится особенно заметным при передаче аналоговых сигналов по кабелю или через эфир.

Следует также выделить в отдельный класс шум, возникающий при квантовании и оцифровке аналогового сигнала. Такой шум проявляется

в виде «снега», гранулированности или беспорядочно расположенных точек на изображении. Это результат нестабильности работы электроники при изменении температуры.Такой же шум может появиться при излишне большой разрядности АЦП при преобразовании аналогового сигнала (так называемое «дрожание» младшего бита).. Шум наиболее заметен на темных участках изображения, так как при постоянстве абсолютного уровня шумовой составляющей уровень сигнала уменьшается и соответственно уменьшается отношение сигнал\шум. На светлых участках это не проявляется. Именно для минимизации такого шума перед сканированием выполняют калибровку для коррекции базового напряжения светочувствительных элементов. Регулярный шум, который является результатом перекрёстных помех и взаимных наводок, проявляется в виде полос на изображении и не представляет интереса с точки зрения возможности использования в качестве полезного объема для скрытых вложений.

Кроме перечисленных источников и причин возникновения шумовой составляющей любая обработка сигналов электронными приборами сопровождается присутствием так называемого дробового шума. Возникает он как результат флуктуаций вследствие дискретности зарядов, которые создают ток в электронных и полупроводниковых приборах. Поскольку электроны начинают свое движение в случайные моменты времени и эти моменты независимы друг от друга, спектральная плотность дробового шума не зависит от частоты, то эту составляющую можно отнести к белому шуму и описывается она известной формулой Шотки

$$\frac{i^2}{\Delta f} = 2ql,$$

где i^2 - середний квадрат флуктуациитока; Δf – полоса частот, в которой проводится измерение уровня шума; q – элементарный заряд; I – протекающий ток.

Еще одна разновидность шума – тепловой шум. Электрический ток кроме направленного движения электронов содержит составляющую, определяемую их хаотическим (ненаправленным) тепловым движением, что приводит к случайным колебаниям плотности тока и, соответственно, напряжения на входе, например, сенсора.

Дисперсия теплового шума определяется формулой Найквиста

$$U_ш^2 = 4KTRB$$

где K – постоянная Больцмана, $R = 1{,}38 \cdot 10^{-23}$ Дж/К, T – абсолютная температура сопротивления, B – эфективнаяполоса частот, в которой проводят измерения уровнятеплового шума.

Эта формула определяет тепловые шумы активных сопротивлений при любых температурах, за исключением свехнизких. Приведенная формула показывает, что спектральнаяплотность теплового шума, т.е.мощность, отнесенная к одиночному интервалу частоты, не зависит от частоты.Такой шум можно считать «белым» и, по крайней мере, в первом приближении моделировать равномерно распределенными разноцветными точками на изображении.

Перечисленные и некоторые другие разновидности шума являются естественными в том смысле, что шумовая составляющая возникает и присутствует в контейнере независимо от желания пользователя и для обычного (традиционного) информационного обмена является нежелательной. Но для организации скрытого обмена эта составляющая оказывается полезной, поскольку позволяет (по крайней мере, потенциально) увеличить полезную нагрузку контейнера.

Целенаправленное искусственное введение шумовой составляющей

Наиболее простым и очевидным способом увеличения шумовой компоненты (и, тем самым, и пропускной способности стеганоканала) является добавление шумовой э.д.с. еще на электрическом уровне, добавив ее к аналоговому сигналу. То же самое можно реализовать и на акустическом уровне, записывая файл-контейнер от микрофона в зашумленном искусственно помещении (студии). Аналогично для изображений искусственный шум может быть добавлен на уровне освещения (например, съемке при недостаточном освещении и, соответственно, длительной экспозиции либо сканировании изображений, отпечатанных на бумаге невысокого качества).

Шум может быть внесен и путем целенаправленной коррекции или модификации файла-контейнера.

Графические файлы неподвижных изображений

В этом случае шум может быть внесенпрограммно с помощью инструментов программы Photoshop [3].

При кодировании в компьютерной графике изображение понимается компьютером как таблица, которая состоит из маленьких ячеек одного и того же размера, каждой из которых присваивается цветовое значение в зависимости от занимаемой ей площади. Когда обрабатывается изображение, компьютер запоминает идентифицированную таблицу изображения, ячейки в которой несется информация о цвете элементов этого изображения.

Практически все эффекты, применяемые к исходному изображению, увеличивают его битовый объем. Например, и применив к изображению несколько эффектов, связанных с шумами, оценим изменение объема изображений. Исходный размер изображения 2,8 Мб.

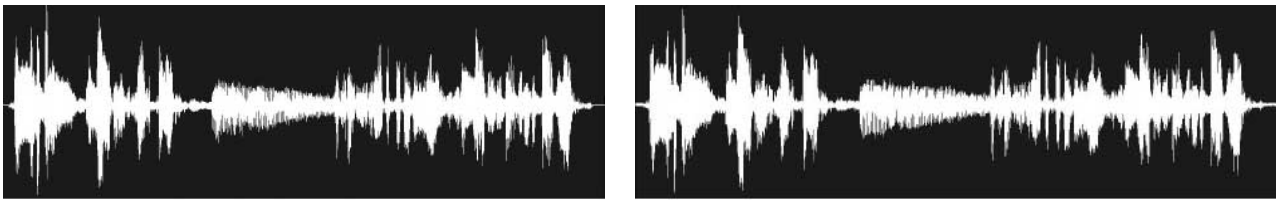
Таблица 1. Зависимость размера картинки от применяемого эффекта

Эффект	Размер (Мб)	Комментарии
+10% Гауссовского шума	4,1 Мб	Вносимое количество мелких деталей существенно увеличивает размер.
+50% Гауссовского шума	5,9 Мб	То же
+100% Гауссовского шума	6,3 Мб	Следует заметить отсутствие линейной зависимости между количеством шума и размером, поскольку пиксели шума всё больше и больше перекрывают друг друга
Уменьшение шума с максимальными значениями резкости и цветового шума	1,4 Мб	Уменьшение размера в 2 раза объясняется уменьшением детализации объекта, а так же снижением количества цветовых тонов
Гауссовского размытие в 1 пиксель	611 Кб	Уменьшение размера объясняется уменьшением детализации объекта
Гауссовское размытие в 5 пикселей	340 Кб	Объясняется тем, что один пиксель принимают на себя значение пяти, и поэтому снижается количество информации

Аудио файлы

Преобразование аналогового звука в цифровой при использовании формата WAV в максимальной степени сохраняет исходный звук с определенной степенью точности, но размер файла оказывается достаточно большим. Например, при частоте дискретизации 44 кГц (16 битов на отсчет, стерео) размер файла будет составлять 44·16·2=1408 кбит в одной секунде звучания или 1408/8=176 кбайт.

Использование формата MP3. Это способ позволяет существенно уменьшить размер файла. Достичь этого можно, если убрать некоторые частоты, вне частотного диапазона слышимости человека.. Аудиостеганография скрывает сообщение в области частот, не воспринимаемых человеческим ухом [4] На слух результат ничуть не отличается от оригинала по качеству звучания.



а) **б)**

Рис. 1. Частотная диаграмма оригинального звукового фрагмента (а) и тот же фрагмент, но со скрытым сообщением (б)

Существует несколько методов аудиостеганографии:

Эхо-методы применяются в цифровой аудиостеганографии и используют неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия. Эхо характеризуется тремя параметрами: начальной амплитудой, степенью затухания,

задержкой. При достижении некоего порога между сигналом и эхом они смешиваются. В этой точке человеческое ухо не может уже отличить эти два сигнала.

Эхо-методы устойчивы к амплитудным и частотным атакам, но неустойчивы к атакам по временным характеристикам.

Фазовое кодирование – также применяется в цифровой аудиостеганографии. Происходит замена исходного звукового элемента на относительную фазу, которая и является секретным сообщением.

Фазовое кодирование является одним из самых эффективных методов скрытия информации.

Метод расширенного спектра заключается в том, что специальная случайная последовательность встраивается в контейнер, затем, используя согласованный фильтр, данная последовательность детектируется. Данный метод позволяет встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу. Метод заимствован из широкополосной связи.

Таблица 2. Зависимость размера аудио-файла от применяемого метода

Эффект	Размер (Мб)	Комментарии
Исходный файл	7,7	Длина аудио-дорожки 3 мин 24 сек
Внесение данных в тэг метаданных	7,9	Тэг ID3v1 не позволит сохранить много данных и жёстко регламентирован, но вот ID3v2.4, как видно из увеличения размера способен хранить большее количество информации
Внесение фазовых изменений	8,3	Размер файла увеличился, но всё зависит от количества изменений
Встраивание специальных случайных последовательностей	8,9	Опять же объём файла напрямую зависит от объёма внесённых последовательностей

Таким образом, самый обычный на первый взгляд (и слух) формата MP3-файл может содержать в себе очень много конфиденциальной информации.

Видеофайлы

Несмотря на то, что существует большое количество видеоформатов, на практике для сокрытия информации используются форматы MPEG-2 и MPEG-4. Рассмотрим три способа внедрения информации в файлы формата MPEG-2

Метод встраивания информации на уровне коэффициентов. Биты скрываемой информации встраиваются в коэффициенты дискретного косинусного преобразования (ДКП). Главной проблемой модификации коэффициентов ДКП в сжатом потоке видео является накопление сдвига или ошибок. Искажения, вызванные изменением коэффициентов ДКП, могут распространяться во временной и пространственной областях. Поэтому для компенсации искажений добавляют специальный сигнал. В силу ограничения на битовую скорость, при внедрении изменяются только 10-20% коэффициентов ДКП. При использовании данного метода скрываемая информация сохраняется при фильтровании, зашумлении (аддитивным шумом) и дискретизации.

Метод встраивания информации на уровне битовой плоскости. Этот метод отличается высокой пропускной способностью и небольшой вычислительной сложностью. Но есть и существенный недостаток: информация, встроенная таким образом, может быть легко удалена. При повторном наложении последовательности бит качество видео ухудшится, а скрываемая информация будет уничтожена.

Метод встраивания информации за счёт энергетической разницы между коэффициентами. В основе этого метода лежит дифференциальное встраивание энергии (ДЭВ). Сложность алгоритма ДЭВ незначительно выше сложности метода встраивания на уровне битовой плоскости и значительно ниже сложности метода, основанного на корреляции с компенсацией ошибок предсказания. Метод ДЭВ может быть применён не только к видеоданным MPEG, но и к другим алгоритмам сжатия видео. Информация встраивается путём удаления нескольких коэффициентов ДКП, и это имеет свои преимущества. Во-вторых, в сжатый поток видеоданных не надо ничего добавлять, можно обойтись без повторного сжатия восстановленного потока видео. Во-вторых, удаление высокочастотных коэффициентов будет уменьшать размер стегообраза потока сжатых видеоданных по сравнению с исходным потоком. Алгоритм ДЭВ вносит

в видео несколько меньше искажений, чем метод встраивания информации на уровне битовой плоскости. Для удаления скрытой информации требуется проведение более сложных вычислительных операций, чем встраивание новой произвольной битовой последовательности.

Таблица 3. Зависимость размера видео-файла от применяемого метода

Эффект	Размер (Мб)	Комментарии
Исходный файл	45,5	
Встраивание в ДКП	47,2	Только 10-20% коэффициентов ДКП используются, тем не менее, информация сохраняется при дискретизации, зашумлении и фильтровании
Встраивание на уровне битовой плоскости	48,9	Высокая пропускная способность, но небольшая надёжность.
Метод ДЭВ	46,75	Более низкий объём файла достигается за счёт удаления «лишних» коэффициентов ДКП

В заключение следует отметить, что кроме метода НЗБ могут быть использованы и другие подходы, которые не предполагают первичной аналоговой природы файла контейнера и несовершенства слуховой или зрительной системы человека. Для пояснения зададим себе вопрос: так ли уж необходима визуальная (слуховая) неотличимость заполненного и пустого контейнера? Представим, что в качестве контейнера используется файл записанного музыкального произведения. Даже если изменить оркестровку исполнения, вряд ли для рядового слушателя, который впервые прослушивает файл, это покажется необычным и подозрительным. В то же время изменением оркестровки можно существенно увеличить объем файла и, соответственно, потенциальные возможности увеличения полезного объема для скрытого информационного обмена.

Аналогично при изменении исходного изображения путем коррекции яркости, контрастности, цветового баланса и т.п. в значительных границах не вызовет подозрений.

Можно пойти дальше. А если вообще вместо одного файла передавать по каналу другой файл (контейнер)? Например, вместо одной картинки другую, вместо одной песни другую, или вместо одного текста другой? А битовую разницу между ними использовать для вложения СВ? Как бы там ни было, такая идея имеет право на существование, хотя ее реализация может оказаться достаточно сложной прежде всего из-за необходимости применения специальных приемов при загрузке СВ и для его маскировки.

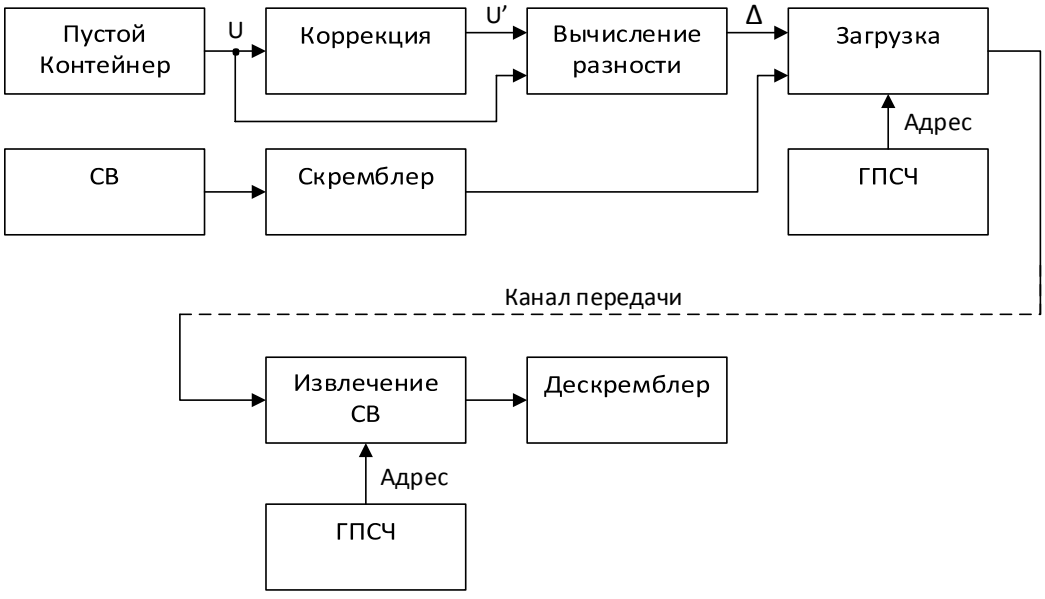


Рис. 2. Общая схема организации стеганоканала

В общем случае рассмотренный подход предполагает процедуру создания стеганоканала путем предварительной коррекции файла контейнера, вычисления побитовой разницы между исходным файлом и его модификацией и загрузкой СВ (рис.2). На этой схеме показан также блок формирования адресов загрузки СВ с помощью генератора псевдослучайных чисел (ГПСЧ). Точно такой же генератор должен быть в составе средств (аппаратных или программных) получателя СВ. Кроме того необходима синхронизация генераторов путем обмена стартовыми числами (битовыми комбинациями), например, с помощью протокола Диффи- Хеллмана.

Выводы

Стеганография включает в себя методы сокрытия секретных сообщений внутри контейнера. Как правило, сокрытие информации с использованием электронных носителей требует модификации свойств контейнера, что, в свою очередь, может вызвать его деградацию. Например, в случае компьютерной графики возможна деградация изображения, заметная глазом, что может указывать на специфические методы, использованные для скрытия сообщения, а также может нейтрализовать саму цель стеганографии – скрыть существование сообщения.

Двумя задачами стеганализа являются обнаружение и уничтожение скрытого сообщения. Любой файл может быть обработан с целью уничтожить потенциальное скрытое сообщение, вне зависимости от его наличия, но предварительное обнаружение сэкономит время на этапе уничтожения. В зависимости от наших целей, мы можем выбрать тип контейнера для передачи и метод стеганографии для того, чтобы скрыть её.

Чтобы предельно затруднить анализ злоумышленником файла-контейнера со стеганографической информацией, сам контейнер должен быть равномерно заполнен, а внедряемый объект должен иметь равномерное распределение, близкое к случайности. Проще говоря, данные должны быть как минимум сжаты. Чтобы обеспечить и случайность распределения, и защиту от несанкционированного доступа к информации даже в случае извлечения, к внедряемым данным обычно применяется один из криптоалгоритмов. Данные зашифровываются перед их сокрытием либо непосредственно в процессе сокрытия. Последний подход считается более прогрессивным, так как позволяет удобно скрыть служебную информацию (заголовки, контрольные суммы, флаги). Существует и комбинированный подход, включающий оба метода.

Если взять видео как контейнер, то определённо метод ДЭВ является наиболее удобным и надёжным в использовании. Ведь применение вейвлет-преобразований и преобразований ДКП лучше подходит в случае защиты от активного злоумышленника, так как эти алгоритмы хорошо отделяют существующие детали от второстепенных.

Аудиоконтейнер является тоже достаточно эффективным, а метод фазового кодирования обеспечивает защиту сообщения на достаточном уровне и при этом предполагает достаточно большой объем скрываемого сообщения.

Список использованных источников

1. *В.Г.Грибунин, И.Н.Оков, И.В.Туринцев*, – Цифровая стеганографія. –М., Солон-Пресс, 2002. – 272с
2. *Г.Ф.Кохановіч, А.Ю.Пузыренко*, Компъютерная стеганография, – «МК-Пресс»,Киев, 2006 – 284с.
3. *Г.В.Кугушина, Ю.Г.Савченко*, Использование инструментов программы Photoshop для организации скрытого информационного обмена, ВісникДУІКТ,том 10, №4, 2012, с.24-28
4. *Gary C. Kessler , Null Ciphers*. An Overview of Steganography for the Computer Forensics Examiner, Forenic Science Communications, vol. 4, №5, 2004, p.27

Поступила в редакцию 06 февраля 2015 г.

УДК 004.056: 621.397

А.Г. Власюк, д. – р. техн. наук, **А.А. Мужайло**, **Ю.Г. Савченко**, д. – р. техн. наук
Національний технічний університет України «Київський політехнічний інститут»
вул. Політехнічна, 16, корпус 12, м. Київ, 03056, Україна

Шляхи збільшення корисного об'єму стеганоконтейнера за рахунок штучного «зашумлення»

На основі існуючих підходів до застосування стеганографії з різними контейнерами був здійснений досить докладний аналіз кожного методу, з використанням відповідного контейнера та визначення його слабких і сильних сторін. Проведено дослідження щодо впливу наявності в початкових контейнерах шумових складових і оцінка збільшення пропускної здатності каналу за рахунок штучного внесення шумової складової у вихідне зображення. Наведено загальну схему організації стеганоканалу шляхом попередньої корекції файлу контейнера, обчислення побітовіої різниці між вихідним файлом та його модифікацією з вкладенням прихованої інформації. Зроблено висновки та рекомендації щодо використання і вибору найбільш оптимального методу залежно від поставленої задачі. Бібл. 4, рис. 2, табл. 3.

Ключові слова: *стеганографія; приховування інформації; стеганоканал; генератор псевдовипадкових чисел (ГПСЧ); штучне зашумлення; стеганоаналіз; дискретно-косинусне перетворення; диференціальне вбудовування енергії (ДВЕ); метод найменш значимого біта (НЗБ); вейвлет -перетворення.*

UDC 004.056: 621.397

A.G. Vlasyuk, Dr.Sc., **A.A. Muzhaylo**, **Y.G. Savchenko**, Dr.Sc.
National Technical University of Ukraine "Kyiv Polytechnic Institute"
Polytechnichna str, 16, building 12, Kiev, 03056, Ukraine

The ways to increase the useful volume of steganocontainer by adding artificial noises

On the basis of the existing approaches to the use of steganography with different containers fairly detailed analysis of each method, using the appropriate container to determine its strengths and weaknesses was done. An investigation on the impact of the availability of noise components in the primary containers and evaluation of the channel capacity increasing by adding an artificial noise component in the original image. General scheme of the steganochannel organization with the use of preliminary containter file correction were shown, the calculation of the bit-difference between source file and its modification with the embedding of hidden information is compleded. Conclusions and recommendations regarding the use and selection of the most appropriate method depending on the task are gived. References 4, figures 2, tables 3.

Keywords: *steganography; information hiding; steganochannel; pseudorandom number generator (PRNG); artificial noise pollution; steganalysis; discrete cosine transformation; the differential energy incorporation (DEI); the method of least-significant bit (LSB); the wavelet transformation.*

References

1. *V.G.Gribunin, I.N.Okov, I.V.Turintsev* (2002), «Digital steganography». M. Solon Press, P. 272. (Rus)
2. *G.F.Kohanovich, A.Y. Puzyrenko* (2006), «Computersteganography». MK-Press, Kiev, P. 284. (Rus)
3. *G.V.Kugushina, Y.G.Savchenko* (2012), «Using tools in Photoshop to organize a secret information exchange», News of DUIKT, vol. 10, No 4, pp. 24-28. (Rus)
4. *Gary C. Kessler, Null Ciphers* (2004), «An Overview of Steganography for the Computer Forensics Examiner». Forenic Science Communications, Vol. 4, No 5, P. 27.