УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСТИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056

САВОСТЬЯНЧИК
Вадим Вячеславович

ИССЛЕДОВАНИЕ МЕТОДОВ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ И СТЕГАНОФОНИИ ИСПОЛЬЗУЕМЫЕ ДЛЯ ЗАЩИТЫ ВИДЕО- И АУДИОИНФОРМАЦИИ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии проектирования электронных систем

Минск, 2018

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Алефиренко Виктор Михайлович,**
кандидат технических наук, доцент, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **Бондарик Василий Михайлович**
Кандидат технических наук, доцент, декан факультета доуниверситетской подготовки и профессиональной ориентации БГУИР

Защита диссертации состоится «27» января 2018 г. в 10^{00} часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, 1 уч. корп., ауд. 415, тел.: 293-20-80, e-mail: kafpiks@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В настоящее время современное информационное общество все активнее востребует научные исследования и разработки в области стеганографии, что связано с многочисленным применением цифровых форматов мультимедиа. Но вместе с тем существуют проблемы управления ресурсами и соблюдения авторских прав на цифровые файлы. Отсюда возникает актуальная задача сокрытия информации в рамках инфраструктуры сетевого общения интернет-участников в медиа-пространстве.

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации.

В стеганографии, в отличие от криптографии, скрывается сам факт передачи сообщения. Здесь принципиальным является помещение информации в какой-либо нейтральный, не вызывающий подозрений объект, называемый контейнером (чаще всего в компьютерной «тайнописи» им является текстовый, графический, аудио- или видеофайл) и незаметное распределение в нем. Своеобразным шифром автора такого сообщения выступает определение «гнезд», в которые вносится информация, порядок ее внесения, внешняя незаметность изменений контейнера, сохранение различных статистических характеристик контейнера и сам факт, что в этом безобидном файле может быть что-то скрыто. Использование тайнописи, не подкрепленное средствами криптографической защиты, вскоре сочли ненадежным, и с появлением все новых методов шифрования стеганография начала оставаться «в тени» криптографии. До сих пор книг и публикаций, посвященных стеганографии, гораздо меньше, чем различных материалов по криптографии.

Однако в современном мире, где огромную роль играет цифровое представление информации и где возможны самые разнообразные комбинации методов работы с данными на цифровых носителях, у стеганографии появилось много новых областей применения. Развитие вычислительной техники создало предпосылки для исследований и научных предложений в области компьютерной стеганографии. Одна из причин активной работы в направлении этих исследований заключается в том, что во многих странах мира существуют законодательные ограничения на использование средств криптографии. Другая причина – необходимость защиты права собственности на цифровую информацию. На данный момент компьютерная стеганография является полноценным направлением в области защиты информации.

Основные методы компьютерной стеганографии, успевшие стать классическими, основаны на существовании естественной неточности в средствах оцифровки, на незаметности изменений в младших битах отсчетов в файлах-рисунках и файлах-фотографиях, на избыточности аналоговых аудио- и видеосигналов, на специальном форматировании текстовых файлов и вообще на всевозможных особенностях компьютерных форматов данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

На сегодняшний день в сети Интернет имеется большое количество свободно распространяемых программ, позволяющих осуществлять стеганографическое сокрытие данных в различных типах контейнеров. Эти программы очень легко доступны и применять их может любой. Такое развитие в области скрытой передачи данных, а также легкая доступность стеганографического программного обеспечения привела к появлению нового канала несанкционированного распространения информации, который весьма трудно пресечь.

В последние годы на внутренние угрозы стали обращать больше внимания и необходимость использования соответствующих средств защиты стала упоминаться в стандартах и нормативных документах.

Существуют различные решения для защиты сети предприятия или организации от утечки из нее конфиденциальной информации, не обрывающие при этом необходимые для работы предприятия коммуникации. Данный класс решений получил название *DLP (Data Leakage Prevention*). Системы, относящиеся к этому классу, перехватывают весь трафик, выходящий за пределы сети предприятия, и сканируют его на наличие в нем конфиденциальных данных. Кроме того, они сканируют всю информацию, записываемую пользователями сети на съемные носители при помощи их рабочих станций.

Известные представители данного класса – *Websense DSS, SecurlT Zgate* и *Zlock, Дозор Джет, Info Watch Traffic Monitor, Symantec DLP*. На сегодняшний день подобные системы способны отследить конфиденциальную информацию, передаваемую в открытом или слабо скрытом (например, заархивированном) виде. Они также способны пресечь передачу зашифрованных данных, в которых может содержаться конфиденциальная информация. Однако стеганографические программные средства дают внутренним нарушителям, передающим конфиденциальные данные за пределы сети предприятия, способ преодоления этих систем. Этот способ заключается в сокрытии конфиденциальных данных в широко распространенных и не запрещенных к передаче контейнерах, таких как графические изображения или аудиофайлы.

Цель и задачи исследования

Целью диссертации является исследование и выбор программного обеспечения с целью повышения эффективности скрытия информации. Для выполнения поставленной цели в работе были сформулированы **следующие задачи**:

– провести обзор и анализ всех существующих методов и программных средств компьютерной стеганографии и стеганофонии;

– изучить влияние человеческого зрения и слуха на факт скрытия информации;

– выбрать наиболее важные критерии выбора программных средств компьютерной стеганографии и стеганофонии, видов контейнеров и сообщений;

– провести экспериментальное сравнение программных средств по выбранным критериям и на основе полученных результатов выбрать наиболее эффективную программу для скрытия информации.

Область исследования. Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области скрытия графической информации методом компьютерной стеганографии и стеганофонии.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна диссертационной работы заключается в исследовании выбора программного обеспечения с целью эффективного скрытия информации.

Основные положения, выносимые на защиту

1. Параметры, используемые для сравнительного анализа эффективности программных средств стеганографии и стеганофонии, и виды контейнеров для скрытия аудиоинформации;

2. Психофизиологические особенности человеческого зрения и слуха, влияющие на возможность обнаружения (не обнаружения) факта скрытия аудиоинформации в используемых видах стегоконтейнеров.

3. Результаты экспериментальных исследований сравнительного анализа по выбору программного средства для скрытия аудиоинформации.

Теоретическая значимость диссертации заключается в детальном анализе методов и программ компьютерной стеганографии и стеганофонии.

Практическая значимость диссертации состоит в экспериментальном сравнении программных средств и выборе программного средства, обеспечивающего наибольшую эффективность скрытия информации.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на международной научно-практической конференции «Материалы и методы инновационных исследований и разработок» (г. Челябинск, Российская федерация, 2016 г.); в международном электронном научном журнале Общества Науки и Творчества «*Science Time*» (г. Казань, Российская федерация, 2017 г.); в международном электронном научном журнале Общества Науки и Творчества «Научное знание современности» (г. Казань, Российская федерация, 2018 г.);

Опубликование результатов диссертации

Изложенные в диссертации основные положения и выводы опубликованы в 6 печатных работах. В их числе 6 статей в сборниках материалов научных конференций.

Общий объем публикаций по теме диссертационной работы составляет 0,975 авторских листа.

Структура и объем работы. Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений. Общий объем диссертационной работы – 89 страниц. Работа содержит 6 таблиц, 19 рисунков. Библиографический список включает 45 наименований

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность проблемы выбора эффективной программы для скрытия информации. Определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В **первой глав**е рассмотрены основные области использования компьютерной стеганографии и стеганофонии – скрытие путем встраивания сообщений в цифровых данных, которые имеют аналоговою природу, такие как аудио или видео, речь и изображение. В качестве контейнеров возможно ис-

пользование текстовых файлов или исполняемых файлов программ, так, например, наименее значимые биты цифрового изображения или аудиофайла могут быть заменены из текстового файла таким образом, что при просмотре этого файла не обнаружат никакой потери в качестве изображения или звука. Отсюда можно утверждать, что любая информация потенциально может содержать скрытую информацию для определенных лиц.

Рассмотрены основные направления, такие как встраивание цифровых водяных знаков, встраивание информации с целью ее скрытой передачи, встраивание информации с целью ее скрытой передачи, встраивание заголовков. Анализ литературных источников позволяет сделать вывод, что стеганосистемы используются для решения следующих первостепенных задач:

– преодоление систем мониторинга и управления сетевыми ресурсами;

– защита конфиденциальной информации от несанкционированного доступа;

– защита авторского права на интеллектуальную собственность;

– камуфлирование программного обеспечения.

Но как бы ни отличались направления использования стеганографии, выдвигаемые при этом требования во многом остаются неизменными. Каждая из указанных выше задач требует определенного соотношения между устойчивостью встроенного сообщения к внешним влияниям и размером встроенного сообщения. В большинстве современных методов, которые используются для скрытия информации в файлах, имеет место зависимость надежности системы от объема встраиваемых данных, как показано на рисунке 1.

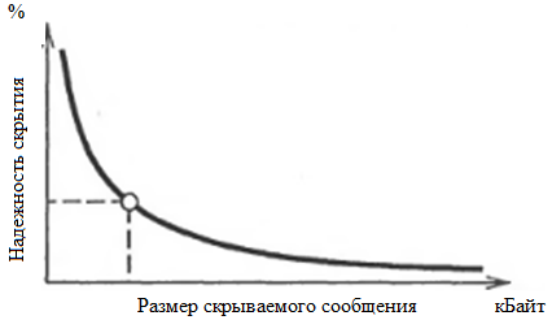

Рисунок 1 – Взаимосвязь между устойчивостью стеганосистемы и объемом скрываемого сообщения при неизменном размере файла-контейнера

На рисунке 1 видно, что увеличение объема встраиваемых данных значительно снижает надежность системы. Таким образом, при ограничении степени ухудшения качеств контейнера, которые способен воспринимать человек, при стеганографической обработке контейнера можно достичь либо высокого объема встраиваемых данных, либо высокой устойчивости к анализу, но не обоих показателей одновременно, т.к. рост одного приводит к снижению другого. Таким образом, благодаря избыточности информации (превышение количества информации, используемой для передачи или хранения

сообщения) существует возможность повысить степень надежности скрытия, жертвуя при этом пропускной способностью, т.е. объемом скрываемых данных.

Важное значение для достижения целей стеганографии имеют протоколы. В стеганографии различают системы с открытым и секретным ключом. В первых для встраивания и извлечения скрытой информации используются разные, не выводимые один из другого ключи – открытый и секретный. В системах с секретным ключом используется один ключ, который заранее известен авторизированным людям до начала скрытого обмена секретными сообщениями.

Свойства системы человеческого зрения (СЧЗ) можно разделить на две группы: низкоуровневые и высокоуровневые. Выделим три наиболее важных низкоуровневых свойства, влияющих на заметность постороннего шума в изображении: чувствительность к изменению яркости изображения, частотная чувствительность и эффект маскирования.

Чувствительность к изменению яркости можно определить следующим образом. Испытуемому показывают некоторую однотонную картинку и после того, как глаз адаптировался к ее освещенности I, «настроился на нее», постепенно изменяют яркость вокруг центрального пятна. Изменение освещенности ΔI продолжают до тех пор, пока оно не будет обнаружено. На рисунке 3 показана зависимость минимального контраста $\frac{\Delta I}{I}$ от яркости I.

Как видно из рисунка 3, для среднего диапазона изменения яркости, контраст примерно постоянен, тогда как для малых и больших яркостей значение порога неразличимости возрастает. Было установлено, что $\Delta I \sim 0.01 - 0.03I$ для средних значений яркости.

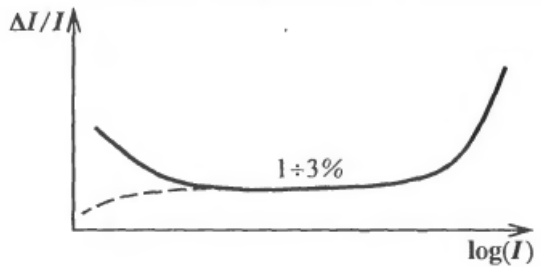

Рисунок 2 – Чувствительность к изменению контраста и порог неразличимости **ΔI**

Исходя из полученных результатов, установлено, что при малых значениях яркости СЧЗ порог неразличимости уменьшается, то есть СЧЗ более чувствительна к шуму в этом диапазоне.

Частотная чувствительность СЧЗ проявляется в том, что человек гораздо более восприимчив к низкочастотному (НЧ), чем к высокочастотному (ВЧ) шуму. Это связано с неравномерностью амплитудно-частотной характеристики системы зрения человека. Экспериментально ее можно определить при помощи того же опыта, что и при яркостной чувствительности. Но в этот

раз в центральном квадрате изменяются пространственные частоты до тех пор, пока изменения не станут заметными.

Аддитивный шум гораздо заметнее на гладких участках изображения, чем на высокочастотных, то есть в последнем случае наблюдается маскирование. Наиболее сильно эффект маскирования проявляется, когда оба сигнала имеют одинаковую ориентацию и местоположение.

Высокоуровневые свойства СЧЗ пока редко учитываются при построении стегоалгоритмов. Их отличием от низкоуровневых является то, что эти свойства проявляются «вторично», обработавший первичную информацию от СЧЗ мозг выдает команды на ее «подстройку» под изображение.

Были рассмотрены основные методы компьютерной стеганографии и стеганофонии и представлена их классификация.

В то же время методы компьютерной стеганографии, основанные на использовании психофизических особенностей человека, невозможно было выявить простым программным анализом и достаточно сложно, а в некоторых случаях и невозможно, обнаружить путём субъективного анализа.

В заключение можно отметить, что методы компьютерной стеганографии, использующие особенности форматов файлов-контейнеров, невозможно выявить путём субъективного анализа (просмотром, прослушиванием), но достаточно легко обнаружить, используя различные программные средства стегоанализа.

Во **второй главе** рассмотрены существующие программные средства стеганофонии и стеганофонии. Для исследования эффективности скрытия графической информации необходимо выбрать ограниченное количество программных средств. Существует достаточно большое число параметров, влияющих на эффективность использования программ компьютерной стеганографии, которые носят как количественный, так и качественный характер. В качестве примера количественных параметров можно привести отношение максимального размера встраиваемого сообщения, не приводящего к искажению изображения, к размеру самого контейнера, количество используемых форматов, а качественных – виды используемых форматов, возможность шифрования информации. Однако, если количественные параметры легко поддаются сравнению, то с качественными параметрами дело обстоит сложнее. Например, одни виды форматов имеют большее распространение (в том числе и в сети Интернет), чем остальные, что является положительным фактором. Однако для некоторых из этих форматов разработан широкий спектр методов и инструментов стеганоанализа. С этой точки зрения эти форматы являются более уязвимыми, а значит и менее эффективными с точки зрения стеганографии.

Проанализировав параметры рассмотренных программных средств компьютерной стеганографии и с учетом вышеизложенного, можно рекомендовать следующие параметры (критерии) их выбора для исследования эффективности скрытия графической информации:

– скрытность или стеганографическая стойкость, которая связана с изменениями (искажениями), вносимыми в исходное изображение при встраивании сообщения;

– размер встраиваемого сообщения, который характеризуется процентным соотношением между объемом встраиваемого сообщения и исходным объемом контейнера;

– устойчивость к модификации заполненного контейнера (сжатию), которая характеризует вероятность восстановления сообщения;

– объем вычислений, необходимый для встраивания сообщения в цифровое изображение;

– количество используемых графических форматов;

– возможность шифрования и их количество.

Анализ параметров существующих программных средств компьютерной стеганографии и стеганофонии, позволил выбрать наиболее важные критерии, по которым в дальнейшем выбирались программные средства для достижения эффективного скрытия информации.

В **третьей главе** рассмотрен выбор контейнера с точки зрения метода внедрения данных, так как именно он определяет биты, которые будут модифицированы на биты сообщения. Учитывался тот факт, что существуют методы анализа, позволяющие обнаружить секретное сообщение, выбор контейнера сделан для метода замены младших бит (*LSB*-метода), на основе которого сделано большинство программ внедрения сообщений. Учитывалось влияние визуального стеганоанализа, как начального этапа анализа контейнера на наличие сообщения. Были рассмотрены принципы выбора видов контейнера, которые представлены ниже:

– отказ от общеизвестных изображений в качестве контейнера, как, например, картины различных художников;

– отказ от использования в качестве контейнера изображений, конвертированных из *JPEG*-формата в формат *BMP*;

– получение изображения при помощи фотоаппарата или сканера, а не при помощи графических редакторов;

– большой размер контейнера;

– зашумленность (разноцветные кубики и есть пресловутый цифровой цветной шум);

– отсутствие плавных переходов и монотонных областей;

– многоцветность;

– большое число перепадов яркости;

– наличие большого числа пикселей, оттенки цветов которых плохо различаются глазом человека (зеленый, желтый).

Известно, что на визуальную скрытность данных влияет цветность изображения, т.е. наличие цветовых областей того или иного цвета. Это объясняется неравномерной чувствительностью человеческого глаза к малым изменениям различных длин волн видимого диапазона. Человеческий глаз

обладает свойством порога цветоразличения при небольших цветовых отличиях, то есть он воспринимает цвет и его «соседний» цвет как один. Величина этого порога неодинакова для разных цветов. Этот эффект представлен на рисунке 3. Таким образом, замена одинакового количества младших бит красной, синей области будет более опасной для обнаружения произведенной замены глазом, чем младших бит желтой или зеленой области за счет разного порога различимости этих цветов.

В результате проведения экспериментальных исследований было выявлено, что:

– файлы одинаковых стегоконтейнеров для различных программ имеют разный размер, что в свою очередь обусловлено различной степенью сжатия исследуемых программ;

– как видно визуально по всем программам зрительные отличия не наблюдались. В тоже время сообщение не должно превышать свой определенный процент размера от контейнера оригинала, так как при превышение своего допустимого предела, при помощи специальных программ, например, *Photoshop*, можно определить, что файл является стегоконтейнером.

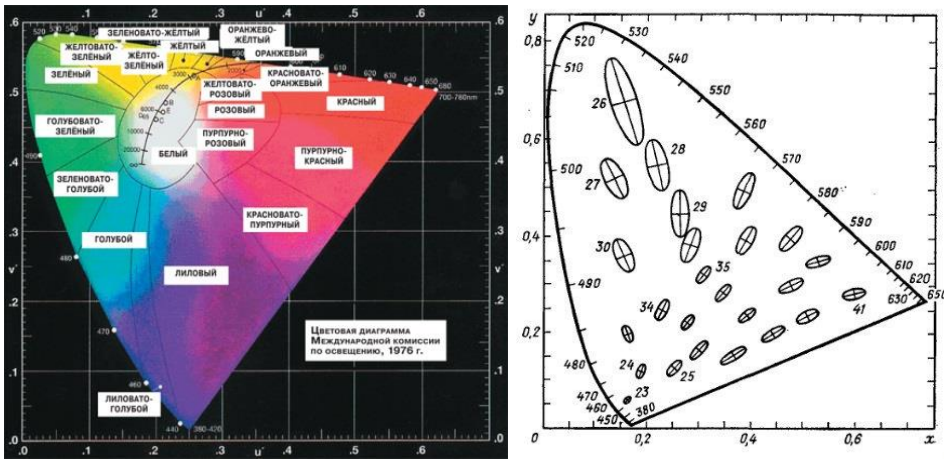

Рисунок 3 – Диаграмма цветностей и пороговые эллипсы

Выбор контейнера, который содержит наибольшие области зеленого, желтого и их смесей с белым цветом, обеспечит наилучшую скрытность данных с точки зрения визуального стеганоанализа. Проанализировав все полученные результаты, сведем их в таблицу 1.

Таблица 1 – Результаты исследований

Параметры (критерии)	Программы стеганографии		
	Masker	*OpenStego*	*DarkCryptTc*
Количество форматов	12	6	12
Количество алгоритмов шифрования	7	1	40
Размер встраивания сообщения для графических/звуковых форматов, %	10/6,5	10/-	10/8

Продолжение таблицы 1

Параметры (критерии)	Программы стеганографии		
	Masker	*OpenStego*	*DarkCryptTC*
Возможность сжатия информации	+	+	+
Стеганографическая стойкость/ скрытность	-	-	+
Возможность скрывать несколько сообщений в одном контейнере	+	+	+

В результате проведения экспериментального сравнения программных средств, установлено, что для эффективного скрытия аудиоинформации подходит программа «*DarkCryptTC*».

ЗАКЛЮЧЕНИЕ

1. Изложены принципы, положенные в основу большинства известных стеганографических и стеганофонических методов, направленных на скрытие конфиденциальных данных в компьютерных файлах графического, звукового и текстового форматов. Для указанных методов проанализированы особенности соответствующих аппаратов человека (зрительного и слухового), сделан акцент на характерные нюансы, позволяющие воспользоваться существующими ограничениями зрительной и слуховой системы человека в стеганографических целях [1, 2].

2. Установлено, что проблемой эффективного скрытия видео- и аудио информации является некачественный подход к выбору программного средства и видов контейнеров, который приводит к значительному ухудшению факта скрываемой информации [3,4]. В результате были определены наиболее важные параметры (критерии), позволяющие выбрать программные средства и виды контейнеров, а также проведен сравнительный анализ выбранных программных средств, с целью определения наиболее эффективной программы для защиты видео- и аудиоинформации. Таким образом были выбраны следующие программы:

– *OpenStego*;

– *Masker*;

– *DarkCryptTC*.

3. Проведено экспериментальное исследование сравнительного анализа выбранных программных средств [5,6]. Показано, что исследуемые программы путем встраивания сообщения в контейнер на выходе имеют разные размеры файла стегоконтейнеров. Это обусловлено наличием в программах разной степенью сжатия. Установлено, что размер встраивания сообщения для графических форматов равен 10% от размера файла контейнера для всех исследуемых программ, а для звуковых форматов у программы *DarkCryptTC* наблюдается лучший показатель в 8%, в отличие от программ Masker и *OpenStego* у которых 6,5% и 6% соответственно. Программа *DarkCryptTC*

превосходит по количеству форматов в 2 раза с программой *OpenStego*, но имеет одинаковое количество с программой *Masker*, а так же по количеству алгоритмов шифрования в 5.71 раз с программой *Masker*, и в 40 раз с программой *OpenStego*. Помимо всего, у программы *DarkCryptTC* имеется стеганографическая стойкость в отличие от других программ, у которых она отсутствует. Таким образом, было определено, что программа *DarkCryptTC* является лучшей для скрытия информации.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в сборниках материалов научных конференций

1. Савостьянчик В.В/ Применение цифровых водяных знаков в стеганографии для защиты мультимедийной информации// Международная научно-практическая конференция// МАТЕРИАЛЫ И МЕТОДЫ ИННОВАЦИОННЫХ ИССЛЕДОВАНИЙ И РАЗРАБОТОК: сборник статей Международной научно-практической конференции (3 декабря 2016 г, г. Челябинск). В 3 ч. Ч.2/ – Уфа: МЦИИ ОМЕГА САЙНС, 2016. – С. 100-101.
2. Савостьянчик В.В/ Воздействие человеческого зрения при построения стегоалгоритмов// Журнал «*Science Time*»: Материалы Международных научно-практических мероприятий Общества Науки и Творчества за октябрь 2017 года. – Казань, 2017.– С.40-42.
3. Савостьянчик В.В/ Влияние активных атак на устойчивость стеганографической системы// Журнал «*Science Time*»: Материалы Международных научно-практических мероприятий Общества Науки и Творчества за октябрь 2017 года. – Казань, 2017.– С.43-47.
4. Савостьянчик В.В., Алефиренко В.М/ Выбор программных средств компьютерной стеганографии для исследования эффективности скрытия графической информации// Журнал «*Science Time*»: Материалы Международных научно-практических мероприятий Общества Науки и Творчества за ноябрь 2017 года. - Казань, 2017.– С. 37-42.
5. 2017.Савостьянчик В.В., Ананич А.Д., Казак А.А., Шкут А.И., Тихновецкий Н.Н/ Составляющие комплексной системы безопасности// Международный электронный научный журнал Общества Науки и Творчества «Научное знание современности», Казань, Российская федерация. 2018 года. – Принято в печать.
6. Савостьянчик В.В., Ананич А.Д., Казак А.А., Шкут А.И., Тихновецкий Н.Н/ Выбор видов контейнеров компьютерной стеганографии для исследования эффективности скрытия графической информации // Международный электронный научный журнал Общества Науки и Творчества «Научное знание современности», Казань, Российская федерация, 2018 года.– Принято в печать.

РЕЗЮМЕ

Савостьянчик Вадим Вячеславович

Исследование методов компьютерной стеганографии и стеганофонии используемые для защиты видео- и аудиоинформации

***Ключевые слова*:** стеганография, стеганофония, сообщение, контейнер, эффективность.

***Цель работы*:** Исследование методов компьютерной стеганографии и стеганофонии с целью выбора программы с наиболее эффективном скрытием информации

***Полученные результаты и их новизна*:** Научная новизна и значимость полученных результатов работы заключается в исследовании выбора программного обеспечения с целью эффективного скрытия информации. Теоретически обоснованы и выбраны критерии, теоретически обоснованы и выбраны виды контейнеров. Практическая значимость заключается в выборе программного средства для наиболее эффективного скрытия информации. Среди множества программных средств позволяющие наиболее эффективно скрывать информацию осуществлен выбор по предложенным критериям и видов контейнеров. Установлено, что размер встраивания сообщения для графических форматов равен 10% от размера файла контейнера для всех исследуемых программ, а для звуковых форматов у программы *DarkCryptTC* наблюдается лучший показатель в 8%, в отличие от программ Masker и *OpenStego* у которых 6,5% и 6% соответственно. Программа *DarkCryptTC* превосходит по количеству форматов в 2 раза с программой OpenStego, но имеет одинаковое количество с программой Masker, а так же по количеству алгоритмов шифрования в 5.71 раз с программой Masker, и в 40 раз с программой *OpenStego*. Помимо всего, у программы *DarkCryptTC* имеется стеганографическая стойкость в отличие от других программ, у которых она отсутствует. Таким образом, было определено, что программа *DarkCryptTC* является лучшей для скрытия информации.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Методы и технические средства обеспечения безопасности».

***Область применения*:** защита графической и аудио информации в компьютерных коммуникациях.

РЭЗЮМЭ

Савасцьянчык Вадзім Вячаслававіча

Даследаванне метадаў кампутарнай стеганографии і стеганофоніі якія выкарыстоўваюцца для абароны відэа- і аудіоінфармациі

Ключавыя словы: сцеганаграфія, сцеганафанія паведамленне, кантэйнер, эфектыўнасць.

Мэта працы: Даследаванне метадаў кампутарнай стеганографии і стеганофонии з мэтай выбару праграмы з найбольш эфектыўным схаванай інфармацыі.

Атрыманыя вынікі і іх навізна: Навуковая навізна і значнасць атрыманых вынікаў працы складаецца ў даследаванні выбару праграмнага забеспячэння дзеля эфектыўнага ўтойвання інфармацыі. Тэарэтычна абгрунтаваны і абраны крытэры, тэарэтычна абгрунтаваны і абраны выгляды кантэйнераў. Практычная значнасць складаецца ў выбары праграмнага сродку для найболей эфектыўнага ўтойвання інфармацыі. Сярод мноства праграмных сродкаў якія дазваляюць найболей эфектыўна хаваць інфармацыю ажыццёўлены выбар па прапанаваных крытэрах і выглядаў кантэйнераў. Устаноўлена, што памер ўбудавання паведамленні для графічных фарматаў роўны 10% ад памеру файла кантэйнера для ўсіх доследных праграм, а для гукавых фарматаў ў праграмы *DarkCryptTC* назіраецца лепшы паказчык у 8%, у адрозненне ад праграм *Masker* і *OpenStego* у якіх 6,5% і 6 % адпаведна. Праграма *DarkCryptTC* пераўзыходзіць па колькасці фарматаў ў 2 разы з праграмай *OpenStego*, але мае аднолькавую колькасць з праграмай *Masker*, а так жа па колькасці алгарытмаў шыфравання ў 5.71 раз з праграмай *Masker*, і ў 40 разоў з праграмай *OpenStego*. Апроч усяго, у праграмы *DarkCryptTC* маецца стеганографическая стойкасць у адрозненне ад іншых праграм, у якіх яна адсутнічае. Такім чынам, было вызначана, што праграма *DarkCryptTC* з'яўляецца лепшай для ўтойвання інфармацыі.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедре праектавання інфармацыйна-камп'ютэрных сістэм ўстановы образования «Беларускі дзяржаўны універсітэт інфарматыкі і радиоэлектроники» ў навучальны курс «Метады і тэхнічныя сродкі забеспячэння бяспекі».

Вобласць ужывання: абарона графічнай і аўдыё інфармацыі ў камп`ютарных камунікацыях.

SUMMARY

Savastsyanchyk Vadzim Vyacheslavovich

Research of methods of a computer steganography and steganophonia used for protection video and audioinformation

***Keywords**: steganografiya, steganophonia, message, container, efficiency.*

***The object of study**: A research of methods of a computer steganografiya and steganophonia for the purpose of the choice of the program with the most effective concealment of information*

***The results and novelty**: The scientific novelty and the significance of the received results of operation consists in a software choice research for the purpose of effective concealment of information. Criteria are theoretically justified and selected, types of containers are theoretically justified and selected. The practical significance consists in a software choice for the most effective concealment of information. Among a set of software allowing to hide most effectively information the choice by the offered criteria and types of containers is realized. It is established that the amount of embedding of the message for graphic formats is equal to 10% of container file size for all studied programs, and for sound formats at the DarkCryptTC program the best indicator in 8% which have unlike the Masker and OpenStego programs 6,5% and 6% respectively is observed. The DarkCryptTC program surpasses in quantity of formats twice with the OpenStego program, but has identical quantity with the Masker program, and also by quantity of algorithms of enciphering at 5.71 time with the Masker program, and by 40 times with the OpenStego program. Besides everything, the DarkCryptTC program has a steganografichesky firmness unlike other programs at which she is absent. Thus, it has been defined that the DarkCryptTC program is the best for concealment of information.*

***Use degree**: results are introduced in educational process on a kakfedra of design of information and computer systems of establishment of an aducation «The Belarusian state university of informatics and radio electronics» in a training course «Methods and technical means of safety».*

***Field of application**: protection graphic and audio of information in computer communications.*