УДК 621.396

Цифровая стеганография: состояние и перспективы

Абазина Е. С., Ерунов А. А.

Постановка задачи: *цифровая стеганография – относительно молодая отрасль знаний, развитие которой принято отсчитывать с 90-х годов прошлого века. Несмотря на это, цифровая стеганография представляет несомненный интерес для специалистов, изучающих вопросы защиты информации, инженеров-проектировщиков средств защиты информации, а также специалистов в области теории информации и цифровой обработки сигналов. Публикации, посвященные способам и методам цифровой стеганографии, за последние пять лет характеризуются разработкой математических моделей мультимедийных контейнеров, применения сигналов с расширенным спектром, помехоустойчивых кодов, привлечением элементов новых математических инструментов.* ***Цель работы:*** *обобщить и уточнить основные понятия и определения цифровой стеганографии, уточнить и систематизировать классификацию ее направлений и методов с учетом перспективных исследований в этой области.* ***Результат****: представлены основные понятия и определения цифровой стеганографии, освещены вопросы неустоявшейся терминологии в этой области. Определены основополагающие публикации в сфере цифровой стеганографии, приведена уточненная классификация ее направлений и методов. Представлены основные направления перспективных исследований в этой области и работы, выполненные в рамках определенных направлений.*

Ключевые слова: *стеганография, скрытые каналы, цифровые водяные знаки, фрактальные широкополосные сигналы, псевдослучайные последовательности, генетические алгоритмы, клеточные автоматы, управление скрытой пропускной способностью, многоканальные стегосистемы.*

Введение

Глобальное распространение и постоянное совершенствование вычислительных и телекоммуникационных систем сопровождается ростом их пропускной способности, интеграцией услуг, применением все новых технологий обработки и хранения информации, а также возрастающей сложностью обеспечения безопасности информации. Решение задач совместного обеспечения конфиденциальности, доступности и целостности информации достигается применением криптографических и стеганографических методов ее защиты.

При этом криптография имеет своей целью сохранение в тайне семантики передаваемых сообщений, стеганография же направлена на сохранение в тайне самого факта передачи такого сообщения.

В настоящее время в стеганографии условно выделяют несколько направлений:

- классическая стеганография, которая включает в себя «некомпьютерные методы» сокрытия сообщений неэлектрической природы;
- компьютерная стеганография предполагает использование свойств форматов данных, обрабатываемых и передаваемых в инфокоммуникационных сетях;

- цифровая стеганография основана на избыточности пересылаемых мультимедийных данных, представленных в цифровом виде, изначально имеющих аналоговую природу (изображения, видео, звук) [1-3].

Далее в статье речь идет о компьютерной и цифровой (преимущественно) стеганографии.

Анализ публикаций, посвященных стеганографии, позволяет выделить работы [1-3], изданные на территории нашей страны, в качестве базовых как по времени их опубликования, количеству цитирований, объему представленного материала, так и по числу проанализированных и систематизированных источников литературы по выбранной проблематике. В данных работах изложены основные подходы, принципы и задачи стеганографии и стегоанализа.

Однако стеганографическая наука не стоит на месте и продолжает бурно развиваться, о чем свидетельствуют многочисленные публикации и защиты диссертаций, конференции, патенты на изобретения и полезные модели, свидетельства о регистрации программ. Число приложений, позволяющих, как осуществлять скрытое встраивание информации, так и проводить анализ на предмет обнаружения таковых вложений, находящихся только в открытом доступе в сети интернет, измеряется десятками.

Таким образом, данная статья призвана дополнить и структурировать устоявшуюся классификацию стеганографических методов, представленную в [1-3], а также осветить направления и тенденции перспективного развития цифровой и компьютерной стеганографии.

Основные понятия и определения стеганографии

На настоящий период времени, к сожалению, в области стеганографии не существует каких-либо нормативных документов, регламентирующих классификацию методов, принципов и терминологии, в связи с чем в различных источниках встречаются различные понятия одного и того же термина, либо же авторы вводят собственный тезаурус. Далее в статье представлены основные термины цифровой стеганографии, определения которых сформулированы в результате обобщения и уточнения понятий, наиболее часто применяемых в публикациях данной области.

Скрытой (стеганографической) передачей информации называют процессы, реализующие методы передачи информации, при которых возможна передача дополнительной информации в структуре данных, представленных в цифровом виде и используемых в качестве контейнера, преимущественно за счет их избыточности.

Под **контейнером** (покрывающим объектом) понимают такие цифровые данные, использование избыточности которых позволяет передавать дополнительную информацию, не обнаруживая факта передачи. Контейнер, не содержащий дополнительной информации, называют **пустым,** в противном случае – **заполненным (или стего).**

Совокупность методик и средств встраивания и извлечения дополнительной информации без обнаружения нарушения целостности контейнера потребителем позволяет говорить о формировании **скрытого (стеганографического) канала** передачи информации.

Стеганографической системой (стегосистемой) называют совокупность средств и методов передачи и приема пустого контейнера, функционирующих взаимосвязано со средствами и методами, используемыми для создания скрытого канала передачи информации.

Скрытность [1-3] **(стеганографическая стойкость)** определяется возможными действиями (атаками) нарушителя в отношении стегосистемы. В зависимости от целей организации стеговложения под скрытностью понимается устойчивость такового к факту обнаружения, либо устойчивость к попытке удаления или разрушения стеговложения, когда факт его существования не является тайной для нарушителя. При этом в первом случае **атаки, предпринимаемые нарушителем**, будут иметь **пассивный характер,** и могут выражаться в проведении следующих мероприятий:

- визуальный контроль с целью субъективной оценки качества видеоданных;
- объективный контроль видеоданных по одному (или нескольким) выбранному параметру оценки качества изображений;
- гистограммная атака.

Во втором случае нарушитель будет проводить геометрические атаки над стего: поворот, масштабирование, сжатие и т.д.

Классификация стеганографических методов

Методы цифровой и компьютерной стеганографии в общем виде могут быть классифицированы по целям использования, по виду выбранного контейнера для встраивания, по структуре контейнера (рис. 1).

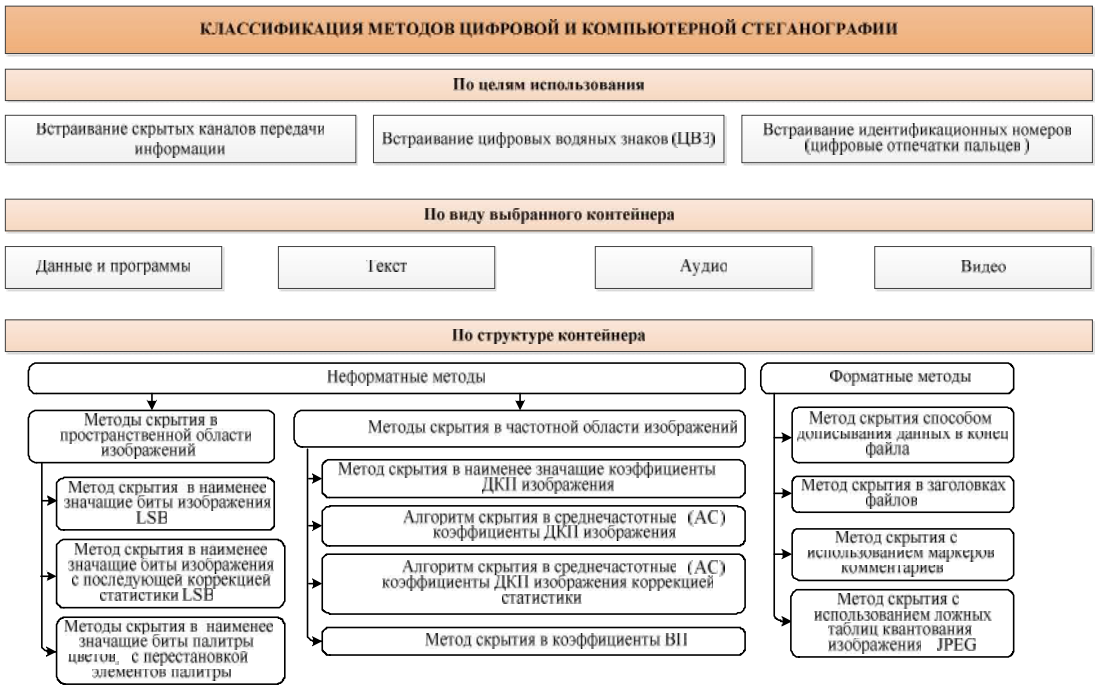

Рис. 1 Классификация методов цифровой и компьютерной стеганографии

По целям использования методов цифровой и компьютерной стеганографии общепризнанными являются три направления:

- встраивание скрытых каналов передачи информации – целью встраивания является сокрытие факта передачи информации;
- встраивание цифровых водяных знаков (ЦВЗ) – цель встраивания состоит в подтверждении подлинности предаваемых данных и в предотвращении несанкционированного доступа к ним;
- встраивание идентификационных номеров (цифровые отпечатки пальцев) – с целью скрытой аннотации и аутентификации передаваемой информации.

Наиболее популярным направлением, получившим развитие в последнее время, является встраивание ЦВЗ. Это во многом определяется необходимостью обеспечения защиты от несанкционированного распространения информации, являющейся интеллектуальной собственностью [4-6]. Организация стеганографических каналов является более актуальным направлением для организаций и ведомств, в которых обеспечение безопасности информации является приоритетным требованием. В связи с тем, что цели, преследуемые при встраивании ЦВЗ и при организации каналов различны, то и основные требования, предъявляемые к разрабатываемым стегометодам имеют ряд отличий. Поскольку ЦВЗ предназначен для защиты от несанкционированного копирования, то знание нарушителем о встраивании ЦВЗ в защищаемый объект не является критичным, в отличие от робастности ЦВЗ, поскольку основной атакой, применяемой в данной ситуации является геометрическая. При этом задача повышения скрытной пропускной способности не стоит, как таковая, в отличие от необходимости обеспечения высокой достоверности приема бит ЦВЗ. При организации скрытого канала же скрытность встраивания является определяющим требованием и основной атакой является визуальная атака и статистический анализ [7-9]. Кроме того, поскольку при организации стегоканалов речь идет о передаче информации, то необходимо обеспечить необходимую скрытую пропускную способность и достоверность приема скрываемых данных не хуже минимальной зависимости от вида передаваемых сообщений. В [1-3] представлена более широкая классификация областей применения стеганографии (рис. 2).

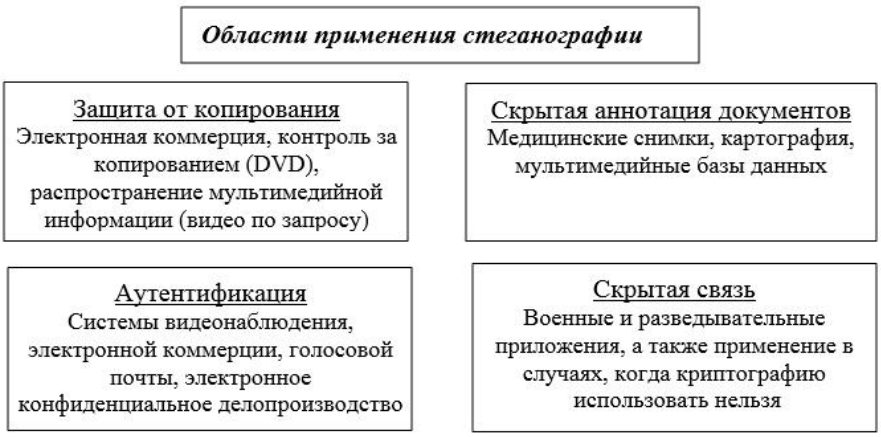

Рис. 2. Классификация областей применения стеганографии

По виду контейнера, выбранного для встраивания стеговложений, стеганографические методы классифицируют [1-3] на методы, подвергающие модификации, данные и программы, текст, аудио и видео. В связи с тем, что организация скрытых вложений возможна преимущественно благодаря избыточности того вида данных, который выбран носителем, то очевидна популярность применения для этой задачи аудио и видеоданных, как наиболее избыточных. Стегометоды организации скрытых каналов используют в качестве контейнера в основном аудио и видеоданные.

В соответствии с тем, какая область в структуре контейнера подлежит модификации, различают форматные и неформатные стегометоды. Применение первых ограничено не высокой стеганографической стойкостью при довольно низкой пропускной способности и более применимо для организации ЦВЗ. Второе направление оказалось более перспективным и базируется на модификации параметров пространства сокрытия файла, характеризующих непосредственно данные самого изображения или звука. В этой области разработаны и хорошо апробированы стойкие к обнаружению стеганографические алгоритмы, обеспечивающие достаточную вместимость контейнеров для вложения скрываемых сообщений или программ. В частности, это и официально признанные алгоритмы стеганографии F5 и OutGess. Поскольку скрытая пропускная способность напрямую зависит от избыточности контейнера, то наиболее применимыми в интересах организации скрытой передачи информации являются подвижные и неподвижные изображения.

Процесс выбора контейнера, встраивание скрываемой информации, представление этих процессов в виде моделей в общем виде описаны в работах [1-3]. Часто используют следующий принцип встраивания данных. Практически любой контейнер в результате обработки может быть представлен последовательностью из N бит. Процесс сокрытия информации начинается с определения бит контейнера, которые можно изменять битами встраиваемой последовательности без внесения заметных искажений. Одним из первых методов встраивания стеговложения основан на замене наименее значащего бита контейнера (НЗБ). Этот метод прост в реализации и позволяет достичь максимума скрытой пропускной способности, однако обладает наименьшей скрытностью и робастностью. Этот способствовало дальнейшему совершенствованию метода НЗБ, а также поиску новых методов и сопровождалось усложнением алгоритмов встраивания и извлечения, а также снижением скрытой пропускной способности. В работах [10-12] отмечено, что встраивание в пространственную область изображений, характеризуется раздвоением пика гистограммы, который является демаскирующим признаком, что определяет целесообразность проведения модификации оцифрованных спектральных составляющих контейнера.

Формализация некоторых известных методов, являющихся основой для разработки новых подходов к организации стеговложений, представлена в [12-13] и сведена в таблицу 1.

Таблица 1 – Наиболее известные подходы к организации скрытых каналов и ЦВЗ в видеоданных

Классификация методов организации скрытых каналов в видеоданных	Правило встраивания $\circ$	Пропускная способность скрытого канала $C_{стег}$	Скрытность U	Достоверность скрываемых данных $p_{ош}$	Число скрытых каналов
1. Направление цифровой стеганографии – встраивание цифровых водяных знаков (ЦВЗ) с целью подтверждения данных					
2. Направление цифровой стеганографии – организация скрытого канала с целью сокрытия факта передачи					
В пространственной области: Наименее значащего бита (К.Ю.Цветков, В.М. Коровин; К.Матсуи, К.Танака, С.Осборн, Дж. Фридрих)	$\circ^1 = I + S$	$C^1_{стег} = \max$	$U^1 = \min$	$p_{ош} = 10^{-3}$, без сжатия	1
В пространственной области: Псевдослучайного интервала (Д.Рамкуман, Дж.Симонс, В.Волошиновский)	$\circ^2 = I + S \mid I_h = 1$	$C^2_{стег} < C^1_{стег}$	$U^2 > U^1$	$p_{ош} = 10^{-3}$, без сжатия	1
В пространственной области: Псевдослучайной перестановки (В.И. Коржик; С.Моллер, А.Фицманн, И.Стиран)	$\circ^3 = I + S \mid h = \ddot{}_i$, $\ddot{}_i - ПСП$	$C^3_{стег} < C^2_{стег}$	$U^3 > U^2$	$p_{ош} = 10^{-3}$, без сжатия	1
В пространственной области: Блочного скрытия (В.О.Хорошко, О.Д.Азаров, К.Ю. Цветков, В.М.Коровин)	$\circ^4 = \left(\frac{I}{D}\right) + S$, D – число блоков	$C^4_{стег} \approx C^3_{стег}$	$U^4 > U^3$	$p_{ош} = 10^{-3}$, без сжатия	1
В частотной области: Наименее значащего бита (В.Г.Грибунин, К.Ю.Цветков, В.М.Коровин; Е.Кох)	$\circ^5 = I^{ДКП} + S$	$C^5_{стег} = \max$	$U^5 > U^1$	$p_{ош} = 10^{-3}$, без сжатия	1
В частотной области: Относительной замены (В.И. Коржик; Е.Кох, Дж. Жао.)	$\circ^6 = \begin{cases} S_0, \left(\frac{I^{ДКП}}{D}\right)_1 - \left(\frac{I^{ДКП}}{D}\right)_2 > P \\ S_1, \left(\frac{I^{ДКП}}{D}\right)_1 - \left(\frac{I^{ДКП}}{D}\right)_2 < P \end{cases}$, P – порог	$C^6_{стег} < C^4_{стег}$	$U^6 \approx U^4$	$p_{ош} = 10^{-3}$, в процессе сжатия	1
В частотной области: Бенгама-Меммона (Д.Бенгам, Н.Меммон, Б-Л Эо, М. Юнг)	$\circ^7 = \begin{cases} S_0, \begin{cases} \left(\frac{I^{ДКП}}{D}\right)_3 < \left(\frac{I^{ДКП}}{D}\right)_1 \\ \left(\frac{I^{ДКП}}{D}\right)_3 < \left(\frac{I^{ДКП}}{D}\right)_2 \end{cases} \\ S_1, \begin{cases} \left(\frac{I^{ДКП}}{D}\right)_3 > \left(\frac{I^{ДКП}}{D}\right)_1 \\ \left(\frac{I^{ДКП}}{D}\right)_3 > \left(\frac{I^{ДКП}}{D}\right)_2 \end{cases} \end{cases}$,	$C^7_{стег} < C^6_{стег}$	$U^7 > U^6$	$p_{ош} = 10^{-3}$, в процессе сжатия	1
В частотной области: Фридрих (Е.А.Небаева; Дж. Фридрих)	$\circ^8 = (I)^{ДКП} + S\left\lvert (I')^{ДКП} < (I)^{ДКП} + 10^2 \sim \right.$, I' – модифицированные видеоданные, $\sim$ – пороговая функция	$C^8_{стег} < C^7_{стег}$	$U^8 \approx U^7$	$p_{ош} = 10^{-3}$, в процессе сжатия	1
В частотной области: Расширения спектра (К.Ю.Цветков, А.Е.Коревых, В.М.Коровин; Дж.-Р. Смит, В.О.Комиски)	$\circ^{10} = (I)^{ДКП} + S \cdot \ddot{}_i$, $\ddot{}_i - ПСП$	$C^8_{стег} < C^{10}_{стег} < C^1_{стег}$	$U^{10} \approx U^9$	$p_{ош} = 10^{-3}$, в процессе сжатия	1
Статистический (И. Патис, В.О.Хорошко, В.Г.Грибунин, М.Е. Шелест)	$\circ^9 = \left[(I)_1^{ДКП}\right]^{\frac{E}{2}} \cup \left[(I)_2^{ДКП}\right]^{\frac{E}{2}}$, E – энергия изображения	$C^9_{стег} < C^8_{стег}$	$U^9 > U^8$	$p_{ош} = 10^{-3}$, в процессе сжатия	1

Развитие методов встраивания как в пространственной, так и в частотной области шло, как правило, по пути усложнения правила встраивания и поиска функций для выбора бит, подлежащих замене, максимально похожим на случайную величину. В работе [1] в качестве альтернативных методов замены указаны следующие.

Встраивание путем инверсии бита: «1» может соответствовать замена 0>1, «0» - замена 1>0.

Встраивание путем вставки бита непосредственно перед модифицируемым битом, при этом значение бита ЦВЗ должно быть противоположно значению бита контейнера.

Встраивание удалением бита, для этого выбирают пары битов «01» или «10» битов, которые соответствуют разным значениям бита ЦВЗ. Затем первый бит пары удаляется.

Встраивание с использованием бита-флага, суть которого состоит в том, что очередной бит контейнера (неизменяемый) является битом ЦВЗ, указывает инверсия предшествующего бита-флага.

Встраивание с применением пороговых бит: используется бит-флаг, но одному биту ЦВЗ соответствует несколько идущих следом за флагом бит (нечетное число). Если среди этих бит больше единиц, то бит ЦВЗ равен «1».

Встраивание с использованием табличных значений. Для определения бита ЦВЗ в предыдущем методе, фактически, использовалась проверка на четность. С тем же успехом можно было бы применять и любое другое отображение множества бит в 1 бит, либо находить его значение по таблице. Возможно использование динамически изменяемой таблицы, когда таблица изменяется на каждом шаге или выбор значения из таблицы осуществляется псевдослучайно. Так как табличные значения (биты контейнера) знает и кодер, и декодер, то их можно не передавать (косвенная динамическая таблица).

Встраивание с применением функции, оценивающей статистику изображение и корреляционные связи между элементами изображения, и последующее применение этой функции для каждого элемента изображения для определения стегопути. При этом в качестве функции может быть использована псевдослучайная последовательность (ПСП).

Другим подходом, отличным от первых двух, является встраивание дополнительной информации за счет энергетической разницы между коэффициентами контейнера, характеризующееся малым изменением статистики изображения.

Отдельной классификационной группировкой среди стегометодов является организация ЦВЗ и стегоканалов с использованием ШПС [7, 10, 14-16], так же именуемые методами с расширением спектра. При этом модификации подлежит все изображение целиком, в отличие от встраивания в частотную и пространственную область, где замене подлежат лишь те элементы и коэффициенты, к которым наименее чувствительна система зрения человека и изменение статистики изображения.

Применение псевдослучайных последовательностей в стеганографических методах

Как правило, для поиска модифицируемых элементов контейнера или для модуляции и кодирования встраиваемых данных в стегометодах используют ПСП, в том числе в методах с применением ШПС. При этом **к ПСП предъявляют следующие основные требования** [17-21].

1. Непредсказуемость появления знаков 1 и 0, благодаря чему спектр сигнала становится более равномерным, а определение алгоритма формирования ПСП по ее участку ограниченной длины – невозможным.

2. Хорошие корреляционные свойства ПСП, которые описываются автокорреляционной и взаимокорреляционной функциями.
3. Наличие большого набора разных ПСП одинаковой длины для построения систем с кодовым разделение каналов.

Чем более хаотична и непредсказуема сгенерированная ПСП, тем ближе ее характеристики к белому шуму. В связи с этим, задача генерации таких ПСП весьма актуальна, в том числе в интересах стеганографии.

На ряду с общеизвестными способами **формирования ПСП, развитие получили и другие подходы,** изложенные ниже и все чаще находящие применение в цифровой и компьютерной стеганографии [17].

1. Использование для генерации ПСП многозначных последовательностей с установлением нелинейных законов их формирования, например, базисных функций Виленкина-Крестенсона, представляющих собой обобщение для дискретно-экспоненциальных функций и функций Уолша. Их применение позволяет получать ПСП значительной структурной скрытности, при этом существует возможность построения ортогональной системы функций с хорошими автокорреляционными и взаимокорреляционными свойствами [12, 14-16, 18, 19].

2. Построение генераторов случайных чисел (ГСЧ), генерирующих приближенные к истинно случайным числовые последовательности [17]. С этой целью в качестве источника случайности ГСЧ используют физические процессы. В этом направлении вопросами повышенного интереса являются вопросы детерминированного хаоса и его использования в системах связи. Современное развитие исследований в области извлечения хаотичности из среды для формирования начального условия для работы ГСЧ характеризуется использованием в качестве источника хаотичности более, чем одной физической среды одновременно. Например, метод [20] заключается в том, что полезный сигнал кодируют в двоичный код, формируют посредством первого генератора исходный детерминированный хаотический сигнал путем модуляции параметров хаотического сигнала полезным цифровым сигналом и передают полученный сигнал по каналу связи принимающей стороне, где его делят на два идентичных сигнала, которыми воздействуют на второй и третий генераторы.

3. Разработка методов повышения качества ГСЧ на основе формализованных моделей дискретных отображений класса «клеточный автомат», которые на основе простых правил, могут порождать сложное поведение [17, 21].

4. Поиск ПСП на основе «естественно» существующих бесконечных числовых последовательностей (иррациональных чисел, которые могут быть оценены, как «непознанные» с точки зрения применения в связи) и конечных последовательностей ограниченного числа объектов (геномные последовательности, так же «непознанные» с точки зрения применения в связи, которые для многих объектов живой природы известны) [17, 22].

5. Формирование фрактальных ПСП, которые совместно с ультракороткими сверхширокополосными сигналами позволяют получить

новый вид сигналов – фрактальные сверхширокополосные сигналы [17]. По мнению авторов, развивающих это направление в работах [23, 24] из-за широкой полосы частот сверхширокополосные сигналы переносят гигантские объемы информации, что определяет их успешное применение в открытых каналах связи для передачи информации на небольшие расстояния (в пределах учреждения), совместно с фрактальным принципом построения возможно обеспечение и информационной безопасности передаваемой таким образом информации.

Новые направления в стеганографии

Анализ открытых публикаций **в области стеганографии** позволяет говорить о формировании новых направлений и тенденций. Как правило, совершенствование стегометодов идет по пути повышения скрытности либо увеличения скрытой пропускной способности [25-28]. Представленные ниже методы ориентированы на организацию стегосистем с новыми возможностями.

1. Выбор в качестве контейнеров цифровых объектов не аналоговой природы: организация стегосистемы в исполняемых файлах, например, сокрытие данных предлагается использовать при помощи замены инвариантных команд или порядка их следования, таким образом, что программа функционирует без изменений [29], использовании аппаратных стегоконтейнеров с LUT-ориентированной архитектурой [30], в кодах, исправляющих ошибки [31].

2. Разработка методов встраивания ЦВЗ и стегоканалов, устойчивых к кодированию источника (сжатию): разработка таких методов, которые бы позволяли с заданной достоверностью идентифицировать ЦВЗ или извлекать скрываемые данные на приемной стороне, встраиваемые до проведения процедур сжатия контейнера на передающей стороне. В работах [8, 9, 13-16, 18, 19, 32, 33] предложено достичь требуемых значений качества встраиваемых данных за счет использования сигнальных конструкций большой избыточности, применяемых для кодирования и модуляции скрываемой информации.

3. Разработка стегометодов, ориентированных на передачу информации по световым волноводам [34].

4. Разработка методов, ориентированных на модификацию аналоговой природы контейнера, а именно встраивание в длину волны. Авторы метода [35-37] исходят из того, что любые вмешательства в пространственное, частотное или энергетическое представление контейнера приводит к скачкообразному изменению длин волн контейнера. Встраиванием в аналоговую природу с учетом этих особенностей позволяют достигать, по мнению авторов, повышения скрытности стеговложений.

5. Создание многоканальных стегосистем и стегосетей, их унификация и стандартизация. Так в работах [8, 9, 13, 18, 19, 32, 33, 38] предложен метод уплотнения скрытого канала в видеоданных, что позволяет формировать многоканальную стегосистему. Авторы достигают заявленный

результат за счет кодового уплотнения скрываемых данных. В работе [39] предложено пространственно-временное разделение стегоканала.

В статье [39] опубликовано предложение формализовать взаимодействие абонентов стеганографической системы связи в виде многоуровневой эталонной модели взаимодействия стеганографических систем – ЭМВСС. Автор надеется, что такая модель позволит обобщить, систематизировать и унифицировать имеющийся опыт в области стеганографии, а в дальнейшем – развивать направление создания единой формализованной модели стегосистемы, как одного из вариантов реализации системы скрытой передачи сообщений, наложенной на телекоммуникационную систему связи.

6. Работы, направленные на совершенствование методов передачи заполненных стегоконтейнеров с целью снижения демаскирующих факторов. Основная идея такого подхода состоит в том, что для уменьшения вероятности перехвата скрытно передаваемых данных следует снижать до минимума время нахождения контейнеров в сети и использовать множество каналов передачи данных, тем самым снижая частоту их демонстрации [40-42].

7. Разработка согласованных методов сжатия изображения и встраивания/извлечения скрываемых данных (стегометодов). Авторы работы [43] предлагают использовать принципы, отличные от общепризнанных, для сжатия видеоданных. При этом, метод сжатия должен быть согласован с метом встраивания стеговложений. Так, для сжатия контейнера и встраивания стего используется фрактальный подход. Метод включает этапы формирования вектора параметров сжатия изображения, ввода скрываемой информации, выделения доменов и ранговых областей, соотнесения ранговых областей и доменов, формирования конечного архива. В способе на этапе выделения доменов и ранговых областей мощность пикселей домена корректируется с учетом значения скрываемых бит информации.

8. Разработка стегометодов, ориентированных на управление сформированными скрытыми каналами. Авторами работ заявляется возможность управления скрытой пропускной способностью, перераспределять ее в зависимости от приоритета абонента и качества обслуживания, предъявляемого к стегоканалу [13, 44-46]. Метод позволяет достичь новых возможностей для потребителей услуг скрытого обмена, а также позволяет говорить о реальной возможности организовать стеганографические сети в перспективе.

9. Разработка генетических алгоритмов в стеганографии [22, 47]. В работе [22] предложен стегометод, предполагающий изменение оцифрованных коэффициентов ДКП изображения битом (или битами) встраиваемой информации. Генетический алгоритм применяется на этапе выбора наиболее подходящего способа изменения коэффициентов ДКП блока изображения при внедрении в него бита дополнительной информации. Формирование исходной популяции хромосом осуществляется псевдослучайным образом в окрестности исходных значений ДКП коэффициентов. Затем авторы проводят оценивание приспособленности хромосом в популяции, по функции которое

приспособленности для хромосомы, которая принимает значение «0» в случае не соблюдения для генов, соответствующих используемым для модификации ДКП коэффициентам. В противном же случае значение функции приспособленности должно определяться на основе вносимых в изображение искажений, вызванных соответствующим данной хромосоме изменением ДКП коэффициентов. Если для хромосомы значение функции приспособленности окажется равным нулю, то ее заменяют на вновь сгенерированную, после чего значение функции для нее пересчитать.

Заключение

Стеганографическая наука является актуальной областью для исследования, как с точки зрения обеспечения безопасности информации, так и с точки зрения защиты персональных данных и авторских прав. Проводимые в настоящее время исследования в области цифровой и компьютерной стеганографии весьма разнообразны и направлены как на совершенствование характеристик стеговложений, так и на возможность создания новых методов, с использованием новых или передовых достижений из различных отраслей знаний, открывающих новые возможности и перспективы для потребителей услуг связи. Несмотря на разнообразие вариантов, которые предлагают авторы в своих работах, основной задачей стеганографии по-прежнему остается поиск компромисса между скрытностью передачи и объемом передаваемой информации. К перспективным и целесообразным направлениям исследований стоит отнести идеи, направленные на поиск решений, позволяющих формировать глобальные системы и сети стеганографической связи, отвечающие, наравне с телекоммуникационными сетями, всем предъявляемым к ним требованиям.

Литература

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. – М.: Солон-Пресс, 2009. – 272 с.

2. Аграновский А. В., Балакин А. В., Грибунин В. Г. , Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ. Монография. – М.: Вузовская книга, 2009. – 220 с.

3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

4. Пономарев К. И., Путилов Г. П. Стеганография: история и современные технологии. – М.: МИЭМ, 2009. – 70 с.

5. Алиев А. Т. Разработка моделей, методов и алгоритмов перспективных средств защиты информации в системах электронного документооборота на базе современных технологий скрытой связи: дис. … канд. техн. наук: 05.13.19. – Ростов-на-Дону: ЮФУ, 2008. – 216 с.

6. Мерзлякова Е. Ю. Построение стеганографических систем для растровых изображений, базирующихся на теоретико-информационных принципах.:дис. … канд. техн. наук: 05.13.19. – Новосибирск: СибГУТИ, 2011. – 161 с.

7. Жгун Т. В. Модель скрытой передачи информации в каналах связи: дис. … канд. ф.-мат. наук: 05.13.18. – В. Новгород: НовГУ, 2003. – 187 с.

8. Абазина Е. С. Метод скрытой передачи информации с кодовым уплотнением в видеоданных // Информация и космос. – 2014. – № 4. – С. 33–38.

9. Цветков К. Ю, Федосеев В. Е., Коровин В. М., Абазина Е. С. Модель кодера скрытых каналов с кодовым уплотнением с использованием сигнальных последовательностей Франка-Уолша, Франка-Крестенсона // Труды НИИР. – 2015. – № 1. – С. 2–11.

10. Небаева К. А. Разработка необнаруживаемых стегосистем для каналов с шумом: дис. … канд. тех. наук: 05.12.13. – СПб.: СПбГУТ, 2014. – 176 с.

11. Коржик В. И., Небаева К. А. Основы стеганографии: учебно-методическое пособие по выполнению практических занятий.– СПб.: СПбГУТ, 2015. – 20 с.

12. Цветков К. Ю, Федосеев В. Е., Абазина Е. С. Применение двумерных нелинейных сигналов Франка-Уолша, Франка-Крестенсона в методе формирования скрытых каналов с кодовым уплотнением в структуре сжимаемых видеоданных // Наукоемкие технологии в космических исследованиях Земли. – 2013. – №. 4. – С. 32–40.

13. Абазина Е. С., Ерунов А. А. Результаты моделирования метода скрытой передачи информации с кодовым уплотнением в видеоданных // Системы управления, связи и безопасности. – 2015. – № 2. – С. 1–25. URL: http://journals.intelgr.com/sccs/archive/2015-02/01-Abazina.pdf (дата обращения: 20.03.2016).

14. Цветков К. Ю. Методы цифровой стеганографии и их приложения в сетях спутниковой связи // Сборник трудов II военно-научной конференции Космических войск. – СПб.: МО РФ, 2004. – Т. 2. – С. 344–349.

15. Цветков К. Ю., Ефимов С. Н., Осташов И. Т. Защита инфокоммуникационных систем и сетей специального назначения: учебное пособие. – СПб.: ВКА имени А.Ф. Можайского, 2010. – 160 с.

16. Коровин В. М. Метод и алгоритмы встраивания широкополосных цифровых водяных знаков в сжатые изображения // Сборник докладов международной научно-практической конференции «Особенности развития космической отрасли России и перспективы ее дальнейшей интеграции в систему международных экономических связей». – СПб.: БГТУ, 2007. – С. 175–178.

17. Сухарев Е. М. Информационная безопасность: методы шифрования. – М.: Радиотехника, 2011. – 208 с.

18. Абазина Е. С. Алгоритмы внедрения двумерных нелинейных кодовых последовательностей в видеопоток // Вопросы радиоэлектроники. Серия Техника телевидения. – 2013. – № 1. – С. 85-93.

19. Абазина Е. С. Применение систем ортогональных сигналов для организации скрытого канала при передаче информации с кодовым уплотнением // Техника средств связи. – 2014. – № 3. – С. 221-224.

20. Москаленко О. И. Фролов Н. С. Короновский А. А. Храмов А. Е.

Способ скрытой передачи информации // Патент РФ № 2509423. 2014. Бюл. № 7.

21. Асосков Г. А., Тихоненко Е. А. Новый генератор случайных чисел на базе двумерного клеточного автомата // Математическое моделирование. – 1996. – Т. 12. – № 8. – С. 77-84.

22. Коваленко М. П. Генетические алгоритмы в стеганографии // Технические науки от теории к практике. – 2012. – № 9. – С. 77–84.

23. Потапов А. А. Фракталы в радиофизике и радиолокации. – М.: Логос, 2002. – 664 с.

24. Шелухин О. И., Тенякшев А. М., Осин А. В Фрактальные процессы в телекоммуникациях. – М.: Радиотехника, 2003. – 480 с.

25. Разинков Е. В., Латыпов Р. Х. Стойкость стегонографических систем // Ученые записки Казанского государственного университета. Физико-математические науки. Книга 2. – 2009. – Т. 151. – С. 126-132.

26. Ремизов А. В., Филиппов М. В. Оценка необнаружимости стеганографических алгоритмов // Наука и образование. – 2012. – № 3. – С. 1-9. – URL: http://technomag.edu.ru/doc/359383.html (дата обращения 17.04.2015).

27. Кувшинов С. С. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии: дис. … канд. тех. наук: 05.13.19. – СПб.: НИУ ИТМО, 2010. – 116 с.

28. Разинков Е. В. Математическое моделирование стеганографических объектов и методы вычисления оптимальных параметров стегосистем: дис. … канд. ф-мат. наук: 05.13.18. – Казань: КГУ, 2012. – 109 с.

29. Нечта И. В. Стеганография в файлах формата PortableExecutable // Вестник СИБГУТИ. – 2009. – № 1. – С. 85–89.

30. Защелкин К. В., Иванова Е. Н. Метод стеганографического скрытия данных в LUT–ориентированных аппаратных контейнерах электротехнические и компьютерные системы. // Электротехнические и компьютерные системы. – 2014. – № 16. – С. 78-84.

31. Слипенчук П. В. Стеганография в кодах, исправляющих ошибки // Вестник МГТУ. – 2013. – № 5. – С. 1-12.

32. Абазина Е. С. Метод кодового уплотнения скрытого канала при передаче видеоданных // Системы управления, связи и безопасности. – 2015. – № 3. – С. 14-42. – URL: http://journals.intelgr.com/sccs/archive/2015-03/02-Abazina.pdf (дата обращения: 20.03.2016).

33. Абазина Е. С. Формирование стеганографического канала с кодовым уплотнением на основе двумерных нелинейных сигналов // Вопросы радиоэлектроники. Серия Техника телевидения. – 2015. – № 2. – С. 108-118.

34. Колесников М. В Метод скрытой передачи данных в оптическом канале видеокамеры // Инженерный вестник. – 2013. – № 2. – С. 501-510.

35. Захаркин С. В., Юрлов А. В., Болбенков А. В., Кирюхин Д. А., Конышев М. Ю., Люлин А. Н. Способ встраивания сжатого сообщения в цифровое изображение // Патент России № 2467486. 2012. Бюл. № 32

36. Захаркин С. В., Иванов И. В., Кирюхин Д. А., Воропаев М. В., Болбенков А. В. Способ встраивания сообщения в цифровое изображение //

Патент России № 2407216. 2010. Бюл. № 35.

37. Двилянский А. А., Кирюхин Д. А., Снаров М. М., Еменка К. Г., Чириков В. Е., Трапашко В. С., Швытов К. В., Чурбанов А. Н., Иванов И. В. Способ встраивания информации в изображение, сжатое фрактальным методом, на основе сформированной библиотеки доменов // Патент России № 2530339. 2014. Бюл. № 28.

38. Алексеев А. П., Макаров М. И. Принципы многоуровневой защиты информации // Инфокоммуникационные технологии. – 2012. – № 2 (10). – С. 88-93.

39. Макаренко С. И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии. // Вопросы кибербезопасности. – 2014. – № 2(3). – С. 24-32.

40. Алексеев А. П., Блатов И. А., Макаров М. И. Оценка вероятности обнаружения мультимедиа контейнеров при пространственно-временном распылении информации // Инфокоммуникационные технологии. – 2013. – Т. 11. – № 3. – С. 91–95.

41. Алексеев А. П., Макаров М. И. Способ скрытой передачи зашифрованной информации по множеству каналов связи, с учетом мощности пикселей домена // Патент России № 2462825. 2012. Бюл. № 27.

42. Макаров М. И. Разработка и исследование методов скрытой распределенной передачи сеансовых данных в телекоммуникационных сетях: дис. … канд. тех. наук: 05.12.13. – Самара: ПГУТИ, 2013. – 144 с.

43. Иванов В. А., Двилянский А. А., Кирюхин Д. А., Снаров М. М., Еменка К. Г., Чириков В. Е., Иванов И. В. Способ встраивания информации в изображение, сжатое фрактальным методом, с учетом мощности пикселей домена // Патент России № 2546558. 2015. Бюл. № 10.

44. Ерунов А. А., Квасов М. Н. Распределение пропускной способности скрытого канала связи, организованного методом цифровой стеганографии // Сборник научных статей Всероссийской научно-практической конференции «Современное состояние и перспективы развития систем связи и радиотехнического обеспечения в управлении авиацией». – Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 4-5.

45. Цветков К. Ю., Федосеев В. Е., Абазина Е. С., Ерунов А. А. Метод скрытой передачи информации с кодовым уплотнением в видеоданных при блочном делении I-кадров // Сборник научных статей Всероссийской научно-практической конференции «Академические Жуковские чтения».– Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 10-13.

46. Цветков К. Ю., Федосеев В. Е., Коровин В. М., Абазина Е. С. Имитационная модель скрытой передачи информации с кодовым уплотнением в структуре сжимаемых видеоданных // Свидетельство о государственной регистрации программы для ЭВМ № 2015615358, 2015.

47. Дрюченко М. А. Статистические и нейросетевые алгоритмы синтеза и анализа стеганографически скрытой информации в аудио- и графических данных: дис. … канд. тех. наук: 05.13.17. – Воронеж: ВГУ, 2010. – 192 с.

References

1. Gribunin V. G., Okov I. N., Turincev I. V. *Tsifrovaia steganografiia* [Digital Steganography]. Moscow, Solon-Press Publ., 2009, 272 p. (in Russian).

2. Agranovskij A. V., Balakin A. V., Gribunin V. G., Sapozhnikov S. A. *Steganografija, cifrovye vodjanye znaki i stegoanaliz. Monografija* [Steganography, Digital Water Marks and Steganoanalysis. Treatise]. Moscow, Vuzovskaja kniga Publ., 2009. 220 p. (in Russian)

3. Konakhovich G. F., Puzirenko A. U. *Komp'iuternaia steganografiia. Teoriia i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press Publ., 2006, 283 p. (in Russian).

4. Ponomarev K. I., Putilov G. P. *Steganografija: istorija i sovremennye tehnologii. Monografija* [Steganography: history and modern technology. Monograph]. Moscow, Moscow Institute of Electronics and Mathematics Publ., 2009, 70 p. (in Russian).

5. Aliev A. T. *Razrabotka modelej, metodov i algoritmov perspektivnyh sredstv zashhity informacii v sistemah jelektronnogo dokumentooborota na baze sovremennyh tehnologij skrytoj svjazi.* Diss. kand. tehn. nauk [The development of models, methods and algorithms of perspective data protection means in electronic document management systems, based on present-day technologies of nondetectable data communication. Ph.D. of Engineering Sciences Tesis]. Rostov-na-Donu, South Federal University Publ., 2008, 216 p. (in Russian).

6. Merzlyakova E. Y. *Postroenie steganograficheskih system dlja rastrovyh izobrazhenij, bazirujushhihsja na teoretiko-informacionnyh principah.* Diss. kand. tehn. nauk [Construction of steganographic systems for raster images based on information-theoretical principles. Ph.D. of Engineering Sciences. Tesis]. Novosibirsk, Sberian Srate University of Telecommunication and Informatics Publ., 2011, 161 p. (in Russian).

7. Zhgun T. V. *Model' skrytoj peredachi informacii v kanalahsvjazi. Dis. … kand.f.-mat. nauk* [The model of hidden information transfer in communication channels. Ph.D. of Physico-mathematical Sciences. Tesis]. Novgorod, Novgorod State University Publ., 2003, 187 p. (in Russian).

8. Abazina E. S. The method of hidden data transmission with code consolidation. *Informatsiia i kosmos*, 2014, no. 4, pp. 33-38 (in Russian).

9. Tsvetkov K. U., Fedoseev V. E., Korovin V. M., Abazina E. S. Model of the coder of the hidden channel with code consolidation with use of signal sequences of Frank-Uolsh, Frank-Krestenson. *Trudi NIIR*, 2014, no. 1, pp. 2-11 (in Russian).

10. Nabieva K. A. *Razrabotka neobnaruzhivaemyh stegosistem dlja kanalov s shumom.* Dis. … kand. teh. nauk [The Development of undetectable stegosystem for channels with noise.Ph.D. of Engineering Sciences.Tesis]. Saint-Petersburg, The Bonch-Bruevich Saint-Petersburg State University of Telecommunication Publ., 2014, 176 p. (in Russian).

11. Korzhik V. I., Nabieva K. A *Osnovy steganografii: uchebno-metodicheskoe posobie po vipolneniyu prakticheskih zanyatij* [Fundamentals of Steganography:a teaching aid for the implementation of practical training]. Saint-Petersburg, The

Bonch-Bruevich Saint-Petersburg State University of Telecommunication Publ., 2015, 20 p. (in Russian).

12. Tsvetkov K. U., Fedoseev V. E., Abazina E. S. Application of two-dimensional nonlinear signals of Frank-Uolsh, Frank-Krestenson into the method of formation of the hidden channel with code consolidation in structure of the compressed video data. *H&ES Research*, 2013, no. 4, pp. 32-40 (in Russian).

13. Abazina E. S., Erunov A. A. Results of the Modelling of the Method of the Hidden Information Transfer with Using of the Code Consolidation in the Video Data. *Systems of Control, Communication and Security*, 2015, no. 2, pp. 1-25. Available at: http://journals.intelgr.com/sccs/archive/2015-02/01-Abazina.pdf (accessed 20 March 2016) (in Russian).

14. Tsvetkov K. U. Metody cifrovoj steganografii i ih prilozhenija v setjah sputnikovoj svjazi [The Methods of digital steganography and their applications in satellite communication networks]. *Sbornik trudov II VNK Kosmicheskih vojsk* [Proceedings 2-ndmilitary scientific conferences of the Space forces.]. Saint-Petersburg, The Russian Federation Ministry of Defense Publ., 2004, no. 2, pp. 344-349 (in Russian).

15. Tsvetkov K. U., Efimov S. N., Ostashov I. T. Zashhita infokommunikacionnyh sistem i setej special'nogo naznachenija: uchebnoe posobie [The protection of the infocommunication systems and networks: Textbook]. Saint-Petersburg, The Mozhaisky Space Military Academy Publ., 2010, 160 p. (in Russian).

16. Korovin V. M. Metod i algoritmy vstraivanija shirokopolosnyh cifrovyh vodjanyh znakov v szhatye izobrazhenija [The method and algorithms of broadband embedding digital watermarks in compressed images. *Sbornik dokladov mezhdunarodnoj nauchno-prakticheskoj konferencii «Osobennosti razvitija kosmicheskoj otrasli Rossii i perspektivy ee dal'nejshej integracii v sistemu mezhdunarodnyh jekonomicheskih svjazej»* [Proceedings of the international scientific-practical conference "Features of development of space industry of Russia and prospects of its further integration into international economic relations]. Saint-Petersburg, The Baltic State Technical university Publ., 2007, pp. 175–178 (in Russian).

17. Sukharev. S. M. *Informacionnaja bezopasnost': metody shifrovanija.* [The Information security: methods of the encryption.] Moscow, Radiotekhnika Publ., 2011, 208 p. (in Russian).

18. Abazina E. S. Algoritmy vnedreniia dvumernykh nelineinykh kodovykh posledovatel'nostei v strukturu szhatykh videodannykh [Algorithms of introduction of two-dimensional nonlinear code sequences in structure of the compressed video data]. *Voprosy radioelektroniki v sfere tekhniki televideniia*, 2013, vol. 1, pp. 85–93. (in Russian).

19. Abazina E. S. Primenenie system ortogonal'nyh signalov dlja organizacii skrytogo kanala pri peredache informacii s kodovym uplotneniem. [The Use of systems of orthogonal signals for the organization of the hidden channel in the transfer of information with code consolidation in structure]. *Tehnika sredstv svjazi*, 2014, no. 3, pp. 221-224 (in Russian).

20. Moskalenko O. I., Frolov N. V. Koronovskiy A. A., Khramov A. E. *Sposob skrytoj peredachi informacii* [The Way of hidden information transfer]. Patent Russia, no. 2509423, 2014.

21. Asoskov G. A., Tihonenko E. A. Novyj generator sluchajnyh chisel na baze dvumernogo kletochnogo avtomata. [A new random number generator on the basis of two-dimensional cellular automaton]. *Mathematical Models and Computer Simulations*, 1996, vol. 12, no. 8, pp. 77-84 (in Russian).

22. Kovalenko M. P. Genetic algorithms in Steganography. *Tekhnicheskie nauki ot teorii k praktike*, 2012, no. 9, pp. 17-20 (in Russian).

23. Potapov A. A. Fraktaly v radiofizike i radiolokacii [Fractals in Radiophysics and radiolocation]. Moscow, Logos Publ., 2002, 664 p. (in Russian).

24. Sheluhin O. I., Tenjakshev A. M., Osin A. V. *Fraktil'nye procesy v telekommunikacijah* [Fractal processes in telecommunication]. Moscow, Radiotekhnika Publ., 2003, 480 p. (in Russian).

25. Razinkov E. V., Latypov R. H. Stojkost' stegonograficheskih system [The resistance steganografic systems]. *Uchenye zapiski Kazanskogo gosudarstvennogo universiteta. Fiz.-mat. Nauki*, 2009, no. 151, pp. 126–132 (in Russian).

26. Remizov A. V., Filippov M. V. Ocenka neobnaruzhimosti steganograficheskih algoritmov [Estimation of undetectable of the steganographic algorithms]. *Nauka i obrazovanie*, 2012, no. 3, pp. 30–38. Available at:http://technomag.edu.ru/doc/359383.html (accessed 17April 2015) (in Russian).

27. Kuvshinov S. S. *Metody i algoritmy sokrytija bol'shih ob#emov dannyh na osnove steganografii. Dis. …kand.tehn. nauk* [Methods and algorithms for hidding large volumes of data based on steganography. Ph.D. of Engineering Sciences. Tesis]. Saint-Petersburg, ITMO University Publ., 2010, 116 p. (in Russian).

28. Razinkov E. V. *Matematicheskoe modelirovanie steganograficheskih ob#ektov i metody vychislenija optimal'nyh parametrov stegosistem* Dis. … kand. f.-mat. nauk [Mathematical modeling of the steganographic objects and the methods of calculation of optimal parameters of stegosystem. Ph.D. of Physico-mathematical Sciences. Tesis]. Kazan, Kazan Federal University Publ., 2012, 109 p. (in Russian).

29. Nechta I. V. Steganography in Portable Executable format files. *Vestnik SIBGUTI*, 2009, no. 2, pp. 85–89 (in Russian).

30. Zashcholkin K. V., Ivanova E. N. Information technology of embedding self-recovery digital watermark in lut-oriented containers, *Elektrotekhnicheskie i kompyuternye sistemy*, 2014, no. 16, pp. 78–84 (in Russian).

31. Slipenchuk P. V. Steganografija v kodah, ispravljajushhih oshibki [Steganography in the correcting errors codes]. *Engineering Bulletin*, 2013, no. 5, pp. 1-12 (in Russian).

32. Abazina E. S., Method of code consolidation of the hidden channel by transfer into video data. *Systems of Control, Communication and Security*, 2015, no 3. pp. 16–42. Available at: http://journals.intelgr.com/sccs/archive/2015-03/02-Abazina.pdf (accessed 20 March 2016) (in Russian).

33. Abazina E. S., Formirovanie steganograficheskogo kanala s kodovym uplotneniem na osnove dvumernyh nelinejnyh signalov [Formation of the

steganographic channel with a code consolidation based on two-dimensional non-linear signals]. *Questions of radio-electronics, the TV equipment series*, 2015, no 2, pp. 108-118 (in Russian).

34. Kolesnikov M. V Metod skrytoj peredachi dannyh v opticheskom kanale video kamery [Method of hidden data transmission in the optical channel of the camera]. *Engineering Bulletin*, 2013, no. 2, pp. 501-510 (in Russian).

35. Zakharkin S. V., Yurlov A. V., Babenko A. V., Kiryukhin D. A., Konyshev M. Y., Lyulin A. N. *Sposob vstraivanija szhatogo soobshhenija v cifrovoe izobrazhenie* [The Way of embedding a compressed message into a digital image]. Patent Russia, no. 2467486, 2012.

36. Zakharkin S. V., Ivanov I. V., Kiryukhin D. A., Voropaev M. V., Bolbenkov A. V. *Sposob vstraivanija soobshhenija v cifrovoei zobrazhenie* [The Way of embedding messages in digital image]. Patent Russia, no. 2407216, 2010.

37. Dvilyanskiy A. A., Kiryhin D. A., Snarov M. M., Emenka K. G., Chirikov V. E., Trapashko V. S., Shvytov K. V., Churbanov A. N., Ivanov I. V. *Sposob vstraivanija informacii v izobrazhenie, szhatoe fraktal'nym metodom, na osnove sformirovannoj biblioteki domenov* [The Way of embedding information in an image that is compressed fractal method, based on a formed library of domains]. Patent Russia, no. 2530339, 2014.

38. Alekseev A. P., Makarov M. I. Principles of multilevel protection of the information. *Infokommunikacionnye tehnologii*, 2012, vol. 10, no. 2, pp. 88-93 (in Russian).

39. Makarenko S. I. The steganographic system interconnection basic reference model and the justification of new areas of steganography theory's development. *Voprosy kiberbezopasnosti*, 2014, vol. 3, no. 2, pp. 24-32 (in Russian).

40. Alekseev A. P., Blatov I. A., Makarov M. I. Probability assessment of multimedia containers detection during space-time information diffusion. *Infokommunikacionnye tehnologii*, 2013, vol. 11, no. 3, pp. 91-95 (in Russian).

41. Alekseev A. P., Makarov M. I. *Sposob skrytoj peredachi zashifrovannoj informacii po mnozhestvu kanalov svjazi, s uchetom moshhnosti pikselej domena* [The way of secure communication of encrypted information across multiple communication channels, taking into account the capacity of the pixel domain]. Patent Russia, no. 2462825, 2012.

42. Makarov M. I. *Razrabotka i issledovanie metodov skrytoj raspredelennoj peredachi seansovyh dannyhv telekommunikacionnyh setjah. Dis. …kand. tehn. nauk* [Development and study of distributed methods of hidden data transmission session in telecommunication networks. Ph.D. of Engineering Sciences. Tesis]. Samara, PSUTI Publ., 2013, 144 p. (in Russian).

43. Ivanov V. A., Dvilyanskiy A. A., Kiryhin D. A., Snarov M. M., Emenka K. G., Chirikov V. E., Ivanov I. V., *Sposob vstraivanija informacii v izobrazhenie, szhatoe fraktal'nym metodom, s uchetom moshhnosti pikselej domena* [The way of embedding information in an image that is compressed fractal method, based on the output pixel domain]. Patent Russia, no. 2546558, 2015.

44. Erunov A. A., Kvasov M. N. Raspredelenie propusknoj sposobnosti skrytogo kanala svjazi, organizovannogo metodom cifrovoj steganografii [Allocation

of the capacity of the covert channel communication, organized by the method of digital steganography]. *Sbornik nauchnykh statej Vserossijskoj nauchno-prakticheskoj konferencii «Sovremennoe sostojanie i perspektivy razvitija sistem svjazi i radiotehnicheskogo obespechenija v upravlenii aviaciej»* [Proceedings of the All-Russian scientific-practical conference «Modern condition and prospects of development of communication systems and radio software in the aviation control»]. Voronezh, N. E. Zhukovsky and Y. A. Gagarin Military Air Academy Publ., 2015, vol. 1, pp. 4–5 (in Russian).

45.Tsvetkov K. U., Fedoseev V. E., Abazina E. S., Erunov A. A. Metod skrytoj peredachi informacii s kodovym uplotneniem v videodannyh pri blochnom delenii I-kadrov [Method of the hidden information transfer with using of the code consolidation in the video data by block division of I-frames]. *Sbornik nauchnykh statej Vserossijskoj nauchno-prakticheskoj konferencii «Akademicheskie Zhukovskie chtenija»* [Proceedings of the All-Russian scientific-practical conference «Zhukovsky Academic reading»]. Voronezh, N. E. Zhukovsky and Y. A. Gagarin Military Air Academy Publ., 2015, vol. 1, pp. 4–5 (in Russian).

46. Tsvetkov K. U., Fedoseev V. E., Korovin V. M., Abazina E. S., Imitatsionnaja model' skrytoy peredachi informatsii s kodovym uplotneniyem v structure szhimayemykh videodannykh [Simulation model of hidden communication with a code consolidation in the structure of the compression video data]. Certificate of state registration of the computer program, no. 2015615358, 2015 (in Russian).

47. Dryuchenko M. A. *Statisticheskie i nejrosetevye algoritmy sinteza i analiza steganograficheskiskrytoj informacii v audio- i graficheskih dannyh.* Dis. … kand. tehn. nauk. [Statistical and neural network algorithms of synthesis and analysis steganographically hidden information in audio and graphical data. Ph. D. of Engineering Sciences. Tesis]. Voronezh, Voronezh state University, 2010, 192 p. (in Russian).

Статья поступила 5 июля 2016 г.

Информация об авторах

Абазина Евгения Сергеевна – кандидат технических наук, преподаватель кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: цифровая стеганография, теория приема и обработки сигналов, теория передачи информации. E-mail: e.s.abazina@yandex.ru

Ерунов Анатолий Александрович – адъюнкт кафедры сетей и систем связи космических комплексов. Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: цифровая стеганография, теория приема и обработки сигналов, теория передачи информации. E-mail: erun_to@mail.ru

Адрес: 197198, Россия, г. Санкт-Петербург, Ждановская наб., д. 13.

Digital Steganography: Status and Development Outlook

E. S. Abazina, A. A. Erunov

Problem statement: *digital steganography is a relatively young branch of knowledge, the development of which is counted since the 90-ies of the last century. Despite this digital steganography is of great interest to specialists studying the issues of information security, engineers of information security tools and experts in the field of information theory and digital signal processing. Publications on techniques and methods of digital steganography, over the last five years are characterized by development of mathematical models of multimedia containers, use signals with spread spectrum, error-correcting codes, the involvement of elements of new mathematical tools.* ***Objective:*** *to summarize and clarify the main concepts and definitions of digital steganography, to clarify and systematize the classification of its policies and practices to the prospective studies in this area.* ***Result:*** *presents the basic concepts and definitions of digital steganography, the questions unsettled terminology in this area. It identifies basic publication in the field of digital steganography, given a refined classification of its policies and methods. There are the main directions of prospective research in this area and work done in certain areas in this article.*

Keywords: *steganography, hidden channels, digital watermarking, fractal wideband signals, pseudorandom sequences, genetic algorithms, cellular automata, management of hidden bandwidth, multi-channel stegosystem.*

Information about Authors

Evgeniya Sergeevna Abazina – Ph.D. of Engineering Sciences, Lecturer at the Department of Networks and Communication Systems of Space Complexes. Mozhaiskiy Military Space Academy. Field of research: digital steganography, the theory of signals. E–mail: e.s.abazina@yandex.ru

Anatoliy Aleksandrovich Erunov – Doctoral Student. The postgraduate student of the Department of Networks and Communication Systems of Space Complexes. Mozhaiskiy Military Space Academy. Field of research: digital steganography, the theory of signals. E–mail: erun_to@mail.ru

Address: Russia, 197198, Saint Petersburg, Zhdanovskaya street, 13.