Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей»

О.О. Евсютин [1], А.С. Кокурина [1], Р.В. Мещеряков [2]
[1] Томский государственный университет систем управления и радиоэлектроники, Томск, Россия;
[2] Институт проблем управления имени В.А. Трапезникова РАН, Москва, Россия

Аннотация

Передача, обработка и хранение информации в инфраструктуре «интернета вещей» сопряжены с необходимостью решения ряда задач обеспечения информационной безопасности. Основная сложность заключается в том, что инфраструктура «интернета вещей» неоднородна и включает в себя множество различных устройств, в том числе с ограниченными вычислительными ресурсами. Одним из подходов к решению данных задач является встраивание дополнительной информации в передаваемые и хранимые цифровые объекты. В данной работе представлен обзор методов встраивания информации в цифровые данные для обеспечения безопасности в «интернете вещей», включающий методы стеганографического встраивания информации и методы встраивания цифровых водяных знаков. Рассмотрены методы встраивания информации в цифровые изображения, а также данные беспроводных сенсорных сетей, предлагаемые для использования в «интернете вещей». Выявлены достоинства и недостатки, присущие отдельным методам и группам методов, проведён анализ их применимости для защиты данных в «интернете вещей». Выявлены актуальные направления в данной области исследований.

Ключевые слова: защита информации, интернет вещей, встраивание информации, цифровые изображения, стеганография, цифровой водяной знак.

Цитирование: **Евсютин, О.О.** Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» / О.О. Евсютин, А.С. Кокурина, Р.В. Мещеряков // Компьютерная оптика. – 2019. – Т. 43, № 1. – С. 137-154. – DOI: 10.18287/2412-6179-2019-43-1-137-154.

Введение

«Интернет вещей» можно определить как глобальную динамическую сетевую инфраструктуру, где физические и виртуальные «вещи» имеют идентификаторы и физические атрибуты и интегрируются в информационную сеть с использованием различных интерфейсов [1]. Логическая структура «интернета вещей» может быть представлена совокупностью взаимодействующих интеллектуальных устройств. При этом с технической точки зрения в «интернете вещей» могут быть использованы любые технологии взаимодействия, а также способы обработки и передачи данных, исходя из их целевого предназначения.

В настоящее время концепция «интернета вещей» активно развивается. Многие «умные» устройства активно используются людьми в повседневной жизни. Перспективным является использование интеллектуальных устройств в различных сферах деятельности в масштабе государства: в медицине, для мониторинга экологической обстановки. Однако концепция «интернета вещей» не только предоставляет новые возможности, но также ставит новые задачи в области информационной безопасности. Вмешательство злоумышленников в управление интеллектуальными устройствами способно привести к серьёзным финансовым потерям или даже создать угрозу жизни и здоровью людей [2]. Чтобы защитить объекты «интернета вещей», необходимо обеспечить безопасность подготовки и подключения интеллектуальных устройств к сети, а также конфиденциальность и целостность обрабатываемых и хранимых данных. Сложность данных задач связана с использованием большого количества разнородных устройств, большая часть которых имеет существенные аппаратные ограничения, что делает невозможным выполнение вычислительно сложных операций с данными.

Наиболее надёжными и используемыми на практике методами защиты данных в цифровой форме являются методы криптографии, включающие шифрование, хэширование и электронную подпись. Однако их использование в «интернете вещей» сопряжено с определёнными сложностями: «тяжеловесность» вычислений, проблема управления ключами и др. Поэтому целесообразно проведение исследований, направленных на получение альтернативных решений.

Альтернативой криптографии являются методы цифровой стеганографии и цифровых водяных знаков (ЦВЗ). Данные методы позволяют скрывать дополнительную информацию в различных цифровых объектах. Обычно целью применения стеганографического сокрытия является обеспечение конфиденциальности данных, а внедрение ЦВЗ в цифровые объекты в большинстве случаев применяется с целью их аутентификации.

Методы цифровой стеганографии и ЦВЗ в первую очередь предназначены для защиты мультимедиаданных. Однако в настоящее время некоторыми исследователями предпринимаются попытки использования данных методов для решения задач безопасности в «интернете вещей». Целью настоящей статьи является обзор и систематизация подобных работ с выявлением перспективных направлений исследований и актуальных задач.

1. Классификация методов встраивания информации в цифровые объекты

Существует два научных направления, изучающих методы встраивания дополнительной информации в цифровые объекты: цифровая стеганография и цифровые водяные знаки.

Цифровая стеганография представляет собой науку о методах сокрытия информации в цифровых объектах с сохранением в тайне факта наличия этой информации. Использование методов цифровой стеганографии позволяет обеспечить конфиденциальность скрываемой информации.

В настоящее время такие методы активно изучаются и развиваются. При этом большая часть существующих работ посвящена сокрытию информации в мультимедиаконтенте [3–6]. Алгоритм стеганографического встраивания информации в общем случае должен обеспечивать незаметность, т.е. минимальность отличий объекта с вложением от оригинального объекта-контейнера, высокую ёмкость и устойчивость к стегоанализу. Дополнительным требованием можно считать робастность – устойчивость стегоконтейнера к различным воздействиям, возникающим при его обработке и передаче по каналам связи.

Наиболее популярными контейнерами для встраивания являются цифровые изображения. Все методы стеганографического сокрытия информации в цифровых изображениях делятся на методы сокрытия в пространственной области и методы сокрытия в частотной области. Сокрытие в пространственной области предполагает изменение пикселей изображения, сокрытие в частотной области – изменение частотных коэффициентов, полученных после применения к пикселям некоторого частотного преобразования. В самом простом случае один или несколько младших битов пикселей или частотных коэффициентов изображения заменяются битами секретного сообщения. Такой метод называется методом наименее значимого бита (LSB). Данный метод очень популярен, поскольку он прост в реализации, не требует больших вычислительных ресурсов и позволяет скрыть в изображении большой объём информации при абсолютной незаметности для человеческого глаза. Однако вложение по методу LSB легко обнаруживается с помощью стегоанализа и разрушается от любого изменения стегоизображения. Другим крайне простым, но популярным методом встраивания является метод «плюс/минус один» (PM1) [7]. В отличие от LSB данный метод не просто изменяет младший бит элемента данных контейнера, а случайным образом увеличивает или уменьшает пиксель или частотный коэффициент на единицу в зависимости от значения бита сообщения. За счёт этого данный метод позволяет добиться большей устойчивости к стегоанализу, однако он также не обладает минимальной робастностью. Напротив, метод модуляции индекса квантования (QIM), заключающийся в модуляции величин элементов данных цифрового изображения в зависимости от значений встраиваемых битов, обладает большей робастностью, но в классическом варианте уязвим к стегоанализу, основанному на гистограммах, поскольку QIM сужает число возможных вариантов значений элементов данных, в которые производится встраивание [8]. Приведённые методы представляют собой примеры, иллюстрирующие изначально разные подходы к сокрытию информации в цифровых изображениях. На сегодняшний день существует большое количество гораздо более сложных методов встраивания в пространственной и частотной области, различных по эффективности встраивания и практической применимости.

В инфраструктуре «интернета вещей» непосредственная передача изображений особенно актуальна для различных медицинских приложений, когда информация о пациенте и его истории болезни скрывается в соответствующих медицинских снимках, например, УЗИ или МРТ. В иных случаях секретная информация может быть скрыта в любых произвольных изображениях. Однако стеганографическое встраивание информации может применяться и к другим типам данных, таким как текст, исполняемые файлы программ, интернет-трафик и т.д.

Вторым направлением сокрытия информации в цифровых объектах является внедрение ЦВЗ. ЦВЗ представляет собой некоторое сообщение, либо сгенерированное на основе исходных данных, либо содержащее служебную информацию о них, такую как время создания, идентификатор автора, аутентификационные данные. В отличие от стеганографии, внедрение ЦВЗ обычно применяется с целью защиты самого цифрового объекта, а не дополнительной информации, скрытой в нём. Целью встраивания ЦВЗ является обеспечение контроля целостности и подлинности данных. Выделяют три класса методов встраивания ЦВЗ: хрупкие, полухрупкие и робастные. Хрупкий ЦВЗ разрушается от любого воздействия на контейнер, полухрупкий ЦВЗ устойчив к некоторым преобразованиям, робастный ЦВЗ обнаруживается в цифровом объекте даже после существенных искажений.

В большинстве случаев водяной знак содержит малый объём информации, поэтому ёмкость алгоритмов внедрения ЦВЗ не является ключевым параметром, незаметность обычно важна в той же мере, что и для алгоритмов стеганографии. Применение ЦВЗ является популярным способом защиты цифрового мультимедиаконтента [9, 10]. Однако с учётом специфики ЦВЗ их часто применяют для защиты самых разных типов данных. В работе [11] приводится подробная классификация данных, не относящихся к мультимедиа, для защиты которых могут применяться ЦВЗ. Среди таких данных различная медицинская информация, сенсорные данные, реляционные базы данных, пространственные данные, графы и другие.

Далее будут рассмотрены современные исследования, в которых методы стеганографии и ЦВЗ применяются для защиты данных в «интернете вещей».

2. Обзор методов стеганографического встраивания информации в цифровые объекты в инфраструктуре «интернета вещей»

Стеганографическое встраивание информации в цифровые изображения, используемые в «интернете вещей»

Сначала рассмотрим работы, посвящённые решению задач информационной безопасности в «интернете вещей» за счёт стеганографического встраивания информации, сопровождая текстовое описание рассматриваемых научно-технических решений рисунками, иллюстрирующими их основные особенности. Однако чтобы чрезмерно не увеличивать объём статьи, будем приводить рисунки только в тех случаях, когда предлагаемый алгоритм встраивания или постановка задачи исследования обладают некоторой специфичностью, не характерной или малоизвестной для проблемной области, которой посвящён настоящий обзор.

Как уже было отмечено ранее, в качестве контейнеров для стеганографического сокрытия данных чаще всего выступают цифровые изображения.

Авторы работы [12] предлагают три алгоритма защиты данных в инфраструктуре «интернета вещей» с помощью стеганографии, где изображения RGB используются в качестве носителей информации. Подходящие позиции для встраивания в битовом представлении пикселей находятся с использованием секретного ключа. Значения битов в выбранных позициях сравниваются с битами сообщения для сокрытия. Первый алгоритм находит три подходящие позиции в трёх составляющих пикселя и изменяет каждое из значений младших битов так, чтобы впоследствии наличие или отсутствие вложения можно было однозначно определить. Для извлечения информации алгоритм сначала проверяет младшие биты всех трёх каналов, а затем вычисляет позиции скрытых битов для тех каналов пикселя, где значение младшего бита соответствовало наличию вложения. При ёмкости в 1,24 бит/пиксель значение PSNR равно 60 – 61 дБ. Второй алгоритм использует только каналы G и B для сокрытия информации. Он находит два набора положений в двух каналах пикселя, а на этапе сравнения битов сообщения и битов, расположенных на выбранных позициях, из двух наборов выбирается тот, который даёт бóльшую ёмкость. В этом случае при аналогичной ёмкости значение PSNR равно 53 – 53,5 дБ. Третий алгоритм использует три канала пикселя для сокрытия информации. Он находит два набора подходящих положений в трёх каналах, при встраивании ёмкость также максимизируется. При той же ёмкости значение PSNR составляет 50,5 – 51 дБ. Помимо высокой ёмкости и незаметности встраивания, результаты представленных экспериментов также демонстрируют устойчивость предложенных алгоритмов к RS-стегоанализу.

Авторы работы [13] утверждают, что в связи с ограниченностью ресурсов устройств «интернета вещей», а именно: небольшим объёмом памяти, ограниченной мощностью аккумулятора, низкими вычислительными возможностями, – LSB-стеганография является лучшим решением для обеспечения информационной безопасности, чем классические криптографические схемы. Для улучшения качества встраивания предлагается выбирать для каждого сообщения наиболее подходящий контейнер с помощью максимальной степени совпадения. Для вычисления степени совпадения сообщение, предназначенное для встраивания, побитно сравнивается с битами младшей битовой плоскости пикселей изображения либо с младшими битами коэффициентов дискретного косинусного преобразования (ДКП). Степень совпадения определяется количеством совпавших элементов. После вычисления степени совпадения сообщения и каждого из потенциальных контейнеров, доступных в базе изображений, сообщение должно быть встроено в контейнер, характеризующийся максимальной степенью совпадения. Данное решение подходит для предварительного анализа изображений при работе с любым стеганографическим алгоритмом, в основе которого лежит метод LSB. Результаты экспериментов демонстрируют положительное влияние алгоритма на устойчивость к RS- и SVD-стегоанализу. Однако необходимость анализа большого числа контейнеров для встраивания одного сообщения увеличивает время обработки данных, что противоречит изначальной цели экономии вычислительных ресурсов и заряда аккумулятора.

Авторы [14] предлагают стеганографический метод защиты медицинской информации, подходящий для передачи данных в «интернете вещей» в реальном времени, например, для систем мониторинга здоровья. Изображение-контейнер в цветовом пространстве RGB разбивается на отдельные плоскости. Защищаемые данные, представленные в виде двоичного вектора, также разбиваются на три вектора равной длины, которые впоследствии должны быть встроены в соответствующие плоскости с использованием одного и того же ключа. Два адресных вектора, а именно: вектор основного адреса (MAV) и дополнительный адресный вектор (CAV), – используются в качестве псевдослучайных адресов для адресации местоположений пикселей в процессе сокрытия информации. Встраивание данных происходит по методу замены двух или трёх младших битов. Дополнительно в изображение-контейнер внедряется хрупкий ЦВЗ, предназначенный для контроля целостности данных после их передачи. Авторы предложенного метода отмечают, что применение стеганографического встраивания в пространственной области изображения не требует больших вычислительных ресурсов, что делает метод применимым для «интернета вещей». Также к достоинствам данного метода относится незаметность встраивания и высокая ёмкость: значение PSNR равно 37,68 дБ при ёмкости 6 бит / пиксель и 37,25 дБ при ёмкости 9 бит/пиксель.

В статье [15] предлагается стеганографический метод защиты электронной информации о здоровье

пациента в «интернете вещей», сочетающий в себе применение интерполяции и модульной арифметики. Защищаемые данные, представленные в виде двоичной последовательности, преобразуются в последовательность чисел в системе счисления по основанию 4 или 8 и встраиваются в медицинское изображение. Согласно описанному алгоритму, входное изображение размером $M \times N$ сначала уменьшается до размера $M/2 \times N/2$, затем полученное изображение увеличивается по методу повторения пикселей (PRM), становясь изображением-контейнером. Для встраивания информации контейнер разбивается на блоки 2×2 пикселя. Левый верхний пиксель блока является опорным и не изменяется в процессе встраивания. К значениям остальных пикселей блока прибавляется разность между соответствующими значениями элементов сообщения и значениями пикселей контейнера по модулю 4 или 8. Проведённые авторами эксперименты, в том числе и со стандартными (немедицинскими) изображениями, демонстрируют высокое визуальное качество стегоизображений, а также высокую ёмкость: значение PSNR равно 39,25 дБ при ёмкости 2,25 бит/пиксель. Изображение-контейнер может быть полностью восстановлено после извлечения вложения, т.е. метод является обратимым. Помимо этого, к заявленным достоинствам предложенного метода относятся устойчивость к анализу гистограммы и вычислительная эффективность.

В работе [16] представлена схема стеганографической защиты информации в «интернете вещей», основанная на векторном квантовании цифровых изображений. Процедура встраивания информации состоит в следующем. Сначала к изображению-контейнеру применяют метод векторного квантования блоками 4×4 пикселя. Далее вычисляются модули разности значений пикселей блоков изображения-контейнера и изображения, восстановленного после сжатия. Количество битов, которое может быть скрыто в пикселях данного блока, определяется наибольшим из двоичных логарифмов полученных разностей, но не может превышать семи битов. Биты сообщения встраиваются в пиксели блока восстановленного изображения с номерами с 3-го по 15-й путём замены трёх младших битов. В первые три пикселя блока аналогичным образом внедряется индекс блока в кодовой книге, в последний пиксель – количество битов, скрытых в отдельно взятом элементе блока. Результаты экспериментов демонстрируют следующее соотношение между визуальным качеством и ёмкостью стегоизображений: PSNR равно 33,59 дБ при ёмкости 1,9 бит/пиксель. Авторы также отмечают, что их схема позволяет обеспечить устойчивость к наиболее распространённым методам стегоанализа, например, хи-квадрат.

Авторы работы [17] представляют схему безопасной локализации беспроводных устройств, основанную на применении стеганографического сокрытия информации в цифровых изображениях. Для экспериментов с предлагаемой схемой в работе рассматривается система, состоящая из мультимедийных мобильных сенсорных узлов и головных узлов кластеров. Сенсорные узлы отправляют запросы на определение местоположения на головной узел вместе со своими идентификаторами и изображениями-контейнерами. На стороне головного узла происходит встраивание информации о местоположении в полученный контейнер по методу LSB. Затем стегоизображение отправляется обратно на сенсорные узлы, которые сравнивают два изображения и извлекают информацию о местоположении. Основное достоинство описанного метода, заявленное авторами работы, заключается в том, что только узел, содержащий оригинальное изображение-контейнер, соответствующее принятому стегоизображению, может получить информацию о локализации. Однако исходное изображение передаётся по сети в открытом виде. Если перехватить пару (исходное изображение, стего-контейнер), то можно извлечь встроенную информацию, что является серьёзной уязвимостью. Кроме того, авторами работы не рассматриваются случаи сбоев в работе узлов, а также не анализируется ресурсозатратность и быстродействие предлагаемой схемы.

Поскольку в инфраструктуре «интернета вещей» взаимодействие пользователя с различными «умными» приборами чаще всего происходит посредством мобильных приложений, важно обеспечивать их безопасность. В работе [18] предлагается метод защиты мобильных Android-приложений с помощью LSB-стеганографии, идея которого основывается на том, что в мобильных приложениях содержится большое количество изображений в формате PNG, в которых можно скрыть компоненты основного кода приложения путём их стеганографического встраивания в изображения, ёмкость при этом равна в среднем 3,05 бит/пиксель. Схема спроектирована таким образом, чтобы злоумышленник не мог получить основной код и обойти процедуру обнаружения несанкционированных изменений, просто обойдя синтаксис сравнения. Согласно данной схеме изображения в приложении (графические элементы интерфейса) отображаются в изначальном виде только при успешном запуске. В случае внесения в приложение злонамеренных искажений изображения будут отображены некорректно либо вообще не будут отображены, что позволит пользователю визуально обнаружить подделку. Схема работы предлагаемого метода проиллюстрирована на рис. 1.

Описанный метод успешно препятствует как статическому, так и динамическому анализу кода. По словам авторов, предложенная схема подходит практически для любых Android-приложений и является более надёжной, чем обфускация кода приложения. Однако внедрение данного подхода может потребовать модификации операционной системы мобильных устройств, что приведёт к значительным затратам на реализацию.

В перечисленных выше работах стеганография является самостоятельным методом обеспечения ин-

формационной безопасности. Однако во многих работах предлагается применять стеганографию вместе с криптографией для достижения наилучшего уровня безопасности.

Рис. 1. Защита мобильного Android-приложения с помощью сокрытия его кода в PNG-изображениях [18]

Например, в работе [19] представлена модель обеспечения безопасности текстовой медицинской информации для передачи в «интернете вещей», объединяющая стеганографическое встраивание информации и шифрование. На первом этапе конфиденциальные данные пациента зашифровываются с использованием гибридной схемы шифрования на основе AES и RSA. На втором этапе зашифрованные данные встраиваются в область дискретного вейвлет-преобразования (ДВП) изображения-контейнера путём замены ДВП-коэффициентов элементами зашифрованного сообщения. При встраивании 256 байт значение PSNR составляет 51,3 дБ, т.е. является достаточно высоким, однако оценить соотношение ёмкости и качества не представляется возможным, т.к. авторы не указывают размеры тестовых изображений. В работе отсутствует анализ устойчивости предложенной схемы к стегоанализу и различным деструктивным воздействиям, способным возникнуть при хранении, передаче и обработке информации.

В работе [20] описана двухуровневая система безопасности данных, передаваемых в сети «интернета вещей», основанная на сочетании стеганографии и криптографии. Во время фазы передачи информации между сенсорным узлом и сервером аутентификации происходит вычисление хэш-кода сообщения по алгоритму MD5, а затем простой метод шифрования, например, основанный на операции XOR, применяется к данным. Полученный хэш-код и зашифрованная информация встраиваются в изображение по методу LSB. На стороне сервера аутентификации информация извлекается из изображения, происходит расшифрование зашифрованных данных с последующим вычислением хэш-кода, который сравнивается с хэш-кодом, извлечённым из стегоизображения. В случае, если целостность данных не была нарушена, аутентификация происходит успешно, в противном случае передача данных блокируется. Во время фазы передачи данных между сервером аутентификации и облаком используется более сложный метод стеганографического встраивания MSB-LSB, предложенный авторами работы, и стандартные алгоритмы безопасного шифрования, например, AES. Достоинством описанного метода является малая вычислительная сложность операций, предназначенных для выполнения на стороне сенсорного узла.

На сочетании стеганографии и криптографии также основан метод, описанный в работе [21]. На стороне отправителя с помощью алгоритма MD5 вычисляется хэш-код секретного сообщения. Само сообщение делится на четыре фрагмента, каждый из которых встраивается в одну область ДВП выбранного цифрового изображения-контейнера. Встраивание осуществляется по методу LSB. По каналу связи передаётся одновременно хэш-код и полученное стегоизображение. На стороне получателя сообщение извлекается из стегоизображения, далее вычисляется его хэш-код, который сравнивается с отправленным хэш-кодом. Таким образом, предложенная схема позволяет обеспечить конфиденциальность передаваемой информации и аутентификацию сообщения. Авторы отмечают, что данная схема имеет небольшую вычислительную сложность, а её реализация не требует серьёзных затрат.

В статье [22] представлен метод обеспечения безопасности смарт-замков. Управление доступом к такому замку производится с помощью смартфона, при этом решение о доступе принимается сервером, с которым смартфон взаимодействует по протоколу Bluetooth Low Energy (BLE). Предлагаемый метод направлен на преодоление уязвимости данного протокола к атаке «человек посередине» за счёт совместного использования стеганографии и шифрования и устроен следующим образом. Пользователь смартфона вводит ключ доступа через соответствующее приложение. Ключ доступа зашифровывается по алгоритму AES, а затем зашифрованный ключ внедряется в выбранное изображение. Изображение отправляется на сервер по протоколу BLE. На стороне сервера из полученного изображения извлекается зашифрованный ключ доступа, который затем расшифровывается. Далее происходит проверка, совпадает ли полученный ключ доступа с правильным, и принимается решение о том, следует ли открывать смарт-замок. Схема работы предлагаемого метода проиллюстрирована на рис. 2.

В работе не представлено конкретного стеганографического алгоритма, однако очевидно, что описанный метод может применяться при разных алгоритмических реализациях. Авторы утверждают, что использование тайного стеганографического канала воспрепятствует попыткам злоумышленника перехватить ключ доступа. Однако сам факт передачи изображений между смартфоном и сервером, управляющим доступом к смарт-замку, будет демаскирующим признаком. И предлагаемое решение не защищено от повторной передачи сообщений, ранее перехваченных злоумышленником, которому в этом случае даже не требуется пытаться извлечь встроенное сообщение.

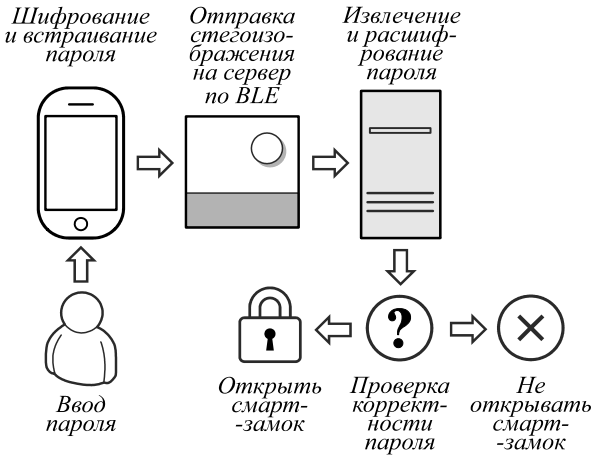

Рис. 2. Управление доступом к смарт-замку со скрытой передачей пароля пользователя внутри изображения [22]

Работа [23] относится к области визуальной криптографии и описывает схему разделения секрета, когда исходная информация может быть восстановлена из определённого количества фрагментов от разных источников. Предлагаемая схема предназначена для обеспечения безопасной передачи изображений в инфраструктуре «интернета вещей», при этом любые интеллектуальные устройства могут захватывать изображения и отправлять в облако для предварительной обработки. В основе данной схемы лежит схема разделения секрета Шамира и стеганографическое встраивание. Предлагаемая схема состоит из двух модулей: модуля генерации зашифрованных или теневых изображений и ключевого модуля для встраивания теневых изображений в контейнеры. Секретное изображение разделяется на несколько теневых, которые встраиваются в изображения-контейнеры, значение PSNR полученных стегоизображений варьируется от 45,5 до 55 дБ. Особенностью предложенной схемы является возможность полного восстановления как секретного изображения, так и изображений-контейнеров, т.е. обратимость.

Стеганографическое встраивание информации в данные беспроводных сенсорных сетей в «интернете вещей»

Значительное количество работ, посвящённых стеганографическому сокрытию информации в изображениях в «интернете вещей», обусловлено тем, что это наиболее распространённый вид цифровых объектов в классической стеганографии. Однако подобные решения неактуальны для тех систем «интернета вещей», которые оперируют потоками данных невизуального характера от различных датчиков. Тем не менее, таких работ известно достаточно мало.

Примером работы, в которой контейнером для стеганографического сокрытия информации в «интернете вещей», являются данные, не относящиеся к мультимедиа, служит статья [24]. В ней представлены два метода сокрытия отчёта о некорректных действиях водителей, передаваемого между интеллектуальными датчиками транспортных средств в автомобильных беспроводных сетях (VANET). Сети VANET предназначены для повышения безопасности дорожного движения, и их датчики позволяют передавать информацию о состоянии автомобильного трафика в режиме реального времени. Один из методов, предложенных в статье, основан на LSB-стеганографии. В качестве контейнера для сокрытия информации используется радиомаяковый сигнал – это сообщение, которое содержит текущее состояние отправителя с точки зрения положения, скорости и т.д. Поскольку точность сенсорных датчиков ограничена, в передаваемых данных присутствует шум, который может использоваться для эффективного стеганографического сокрытия информации. Доступная ёмкость составляет 13 бит. Секретная информация шифруется перед внедрением. Соответствующая схема представлена на рис. 3.

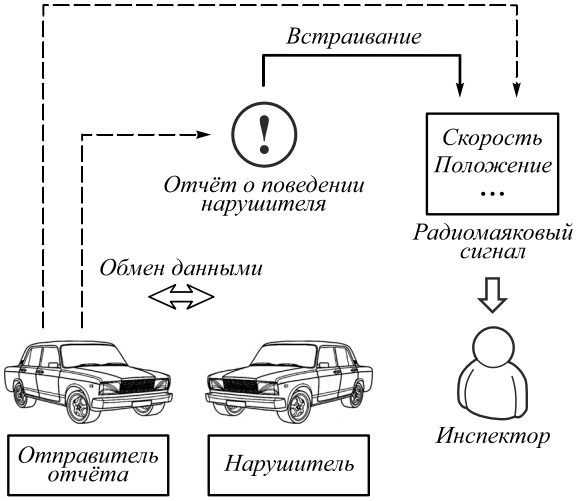

Рис. 3. Сокрытие информации в радиомаяковом сигнале сети VANET [24]

Авторы показывают, что предложенный метод подходит для современных автомобилей и является вычислительно возможным в рамках ограниченных ресурсов объектов «интернета вещей». Благодаря избыточному кодированию, метод является защищённым от случайных потерь данных, возможных в сетях VANET.

Ещё один подобный пример представлен в статье [25], посвящённой агрегации и защите конфиденциальности данных в сетях датчиков тела, предназначенных для непрерывного мониторинга состояния здоровья. В таких сетях есть два типа сенсорных датчиков. Часть из них собирает данные, не относящиеся к конфиденциальной информации, например, датчики температуры тела и движения. Другие датчики собирают конфиденциальные данные, например, датчик ЭКГ. Общая схема показана на рис. 4.

Согласно предложенной схеме, такой датчик сжимает конфиденциальные данные без потерь с помощью дельта-кодирования. Далее на него поступают данные с «обычных» датчиков. Для снижения нагрузки на сеть к этим данным применяется технология пакетной комбинации, и несколько пакетов объединяется в один. В него с помощью операции XOR встраивается сжатая конфиденциальная информация.

Последовательность пакетов с «обычными» данными внутри объединённого пакета, которые будут служить контейнерами для встраивания, определяется на основе различных параметров, таких как младшие биты пакетов, количество битов первого сжатого пакета и других, с применением хэш-функции. Данный метод позволяет сократить затраты ресурсов на передачу информации за счёт сжатия и комбинации данных, а также обеспечить секретную передачу конфиденциальной медицинской информации.

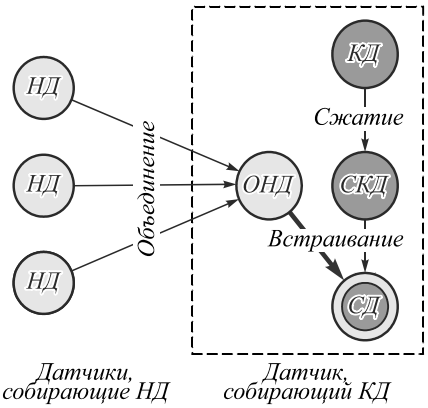

Рис. 4. Защита конфиденциальных данных, вырабатываемых сетями датчиков тела, где НД – неконфиденциальные данные, КД – конфиденциальные данные, СКД – сжатые конфиденциальные данные, ОНД – объединённые неконфиденциальные данные, СД – стегоданные [25]

3. Встраивание ЦВЗ в цифровые объекты в инфраструктуре «интернета вещей»

Встраивание ЦВЗ в цифровые изображения и видеоданные, используемые в «интернете вещей»

Рассмотрим работы, описывающие методы встраивания ЦВЗ в цифровые данные в «интернете вещей», относящиеся к мультимедиа. Сразу отметим, что в данном параграфе будут описаны научно-технические решения, не выходящие за пределы известных направлений в области встраивания ЦВЗ, поэтому их описание не будет дополняться поясняющими схемами.

Пример метода, работающего с цифровыми изображениями, представлен в работе [26]. В данной работе предлагается схема защиты изображений микрочипов ДНК, основанная на использовании хрупких ЦВЗ. Данная схема позволяет защитить как полное изображение, так и некоторую его часть, представляющую область интереса (ROI). Процесс сокрытия водяного знака состоит из сегментации, смещения и непосредственного встраивания. Сегментация применяется для выделения пятен на изображении микрочипа ДНК и получения растровой маски, в соответствии с которой на следующем этапе происходит смещение пикселей, заключающееся в их уменьшении на единицу. Далее элементы ЦВЗ аддитивным образом встраиваются в блоки 2×2 пикселя. Блоки классифицируются на подходящие для встраивания и не подходящие для него в зависимости от соотношения между пикселями в блоке. Данный метод характеризуется незаметностью (значение PSNR равно приблизительно 95 – 100 дБ при встраивании 256 бит) и обратимостью встраивания. Последнее особенно важно в контексте необходимости дальнейшего анализа изображений. Среднее время встраивания (10 изображений) составляет 685 мс.

Статья [27] также посвящена цифровым изображениям. В ней представлен алгоритм встраивания ЦВЗ в цифровые изображения в беспроводных мультимедийных сенсорных сетях, основанный на ДВП. В соответствии с данным алгоритмом к изображению применяется трёхуровневое ДВП, после чего квадрант LH3 разбивается на блоки малого размера, для каждого из которых строятся нуль-деревья ДВП-коэффициентов с корнем в квадранте LH3 и потомками в квадранте LH2. Среди всех деревьев выделяется множество значимых, которые далее используются для встраивания ЦВЗ. Критерием значимости является превышение ДВП-коэффициентами в LH3 и LH2 двух пороговых значений, зависящих от свойств ДВП-блока и адаптивного параметра. ЦВЗ встраивается в значимые коэффициенты отдельных блоков в LH3. Операция встраивания является аддитивно-мультипликативной: ДВП-коэффициент складывается с произведением собственного значения и масштабированного значения пикселя ЦВЗ. Авторы указывают на проблему разрушения ЦВЗ из-за помех в беспроводных каналах связи и потери пакетов и позиционируют свой алгоритм как решение этой проблемы. Основная идея состоит в том, чтобы привязать параметры встраивания к характеристикам сети, в частности к коэффициенту потери пакетов. За это отвечают адаптивные параметры, с помощью которых можно управлять избыточностью встраивания. Кроме того, в [27] решается задача выбора параметров канала передачи данных, обеспечивающих наименьший расход энергии.

В области цифровой стеганографии и ЦВЗ достаточно популярно направление, связанное с использованием видеоданных в качестве контейнеров для встраивания. В «интернете вещей» оно представлено гораздо менее широко. В качестве примера можно отметить работу [28], в которой предлагается схема ЦВЗ для безопасной передачи видео в беспроводных сенсорных сетях. Авторы рассматривают ситуацию, когда в беспроводной системе видеонаблюдения снимаемый видеосигнал подменяется злоумышленником, и предлагают решение для противодействия данной атаке. ЦВЗ встраивается в каждый фрейм видео в формате MPEG-2. Каждый бит ЦВЗ встраивается в два ДКП-коэффициента следующим образом: предварительно вырабатываются два вспомогательных бита как результат действия логических операций «И» и «ИЛИ» на бит ЦВЗ и один из битов DC-коэффициента ДКП-блока, после чего вспомогательные биты встраиваются в выбранные ДКП-коэффициенты по методу LSB. Младшие биты всех прочих ДКП-коэффициентов псевдослучайным образом изменяются для защиты от корреляционного анализа. Описанная схема не обладает робастностью, однако данное свойство не является необходимым для защи-

ты от подмены видеосигнала. В то же время её практическая реализация будет сопровождаться проблемой распределения секретной информации между источником видеосигнала и приёмником, поскольку и секретный ключ, и ЦВЗ должны быть известны обоим устройствам.

Встраивание ЦВЗ в данные беспроводных сенсорных сетей в «интернете вещей»

Бóльшая часть работ, описывающих решение задач информационной безопасности в «интернете вещей» с помощью ЦВЗ, предполагает работу с данными беспроводных сенсорных сетей. Данные исследования образуют новое направление в области встраивания ЦВЗ в цифровые данные, поэтому в большинстве случаев текстовое описание будет дополнено рисунками.

В статье [29] ЦВЗ используются для аутентификации данных в сенсорных сетях. В данной работе предлагается оригинальный подход к агрегации сенсорных данных, в соответствии с которым набор значений, поступающих от каждой группы датчиков, представляется в виде матрицы. Каждую из таких матриц авторы исследования предлагают рассматривать как псевдоизображение. Поскольку расположенные рядом датчики в общем случае фиксируют близкие значения измеряемой величины, такое псевдоизображение будет обладать пространственной избыточностью, как и обычное изображение. Собственно агрегация состоит в JPEG-подобном сжатии сформированного псевдоизображения. Перед сжатием в псевдоизображение встраивается ЦВЗ с использованием метода прямого расширения спектра (*direct spread spectrum sequence*, DSSS), в соответствии с которым один бит ЦВЗ встраивается в блок соседних «пикселей». Операция встраивания состоит в том, что значения «пикселей» в блоке изменяются на малые величины под управлением псевдослучайной последовательности. Поскольку отдельные датчики не взаимодействуют друг с другом, встраивание битов ЦВЗ осуществляется для них независимым образом. Схема, иллюстрирующая описанный подход, приведена на рис. 5.

В [30] авторы предлагают метод проверки целостности данных от различных источников, например, датчиков мониторинга здоровья или окружающей среды, основанный на встраивании ЦВЗ в потоки данных. Для внедрения ЦВЗ используется метод расширения спектра с использованием псевдослучайных ортогональных кодов. Благодаря применению предложенного метода, целостность потоков данных может быть проверена путём извлечения ЦВЗ, даже если данные проходят через несколько этапов процесса агрегации. Предложенная схема водяных знаков сохраняет естественные корреляции, которые могут существовать между несколькими потоками данных, что является важным фактором в контексте необходимости агрегации данных. Также к достоинствам описанного метода можно отнести его применимость для устройств, имеющих ограниченные аппаратные ресурсы. Недостатком данной схемы, как отмечают её авторы, является то, что процесс декодирования требует исследования полной длины последовательности данных, что увеличивает время обработки.

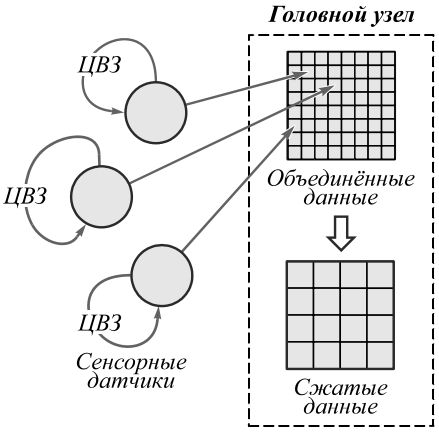

Рис. 5. Встраивание ЦВЗ в данные беспроводной сенсорной сети, устойчивое к агрегации данных [29]

В более поздней работе [31] тех же авторов предлагается технология обфускации сенсорных данных, основанная на применении ЦВЗ. Для внедрения ЦВЗ также используется метод расширения спектра. Обфускация реализуется путём добавления масштабированного водяного знака к данным. В отличие от традиционных схем использования ЦВЗ, где он должен быть незаметен, для целей обфускации амплитуда водяного знака должна быть максимально большой. Данная технология отличается наличием службы контекстуализации, которая обеспечивает агрегирование и фильтрацию данных в реальном времени для большого числа пользователей. Благодаря применению контекстуализации, ненужные данные исключаются из рассмотрения, уменьшается объём данных для обработки и анализа, а значит, уменьшается и количество необходимых вычислений. Данный метод обфускации обратим только для пользователей, прошедших проверку подлинности и имеющих необходимые привилегии. Соответствующая схема показана на рис. 6.

Сочетание ЦВЗ и контекстуализации позволяет затрачивать всего 284 мс для обработки 1152000 точек данных. В работе отмечены два недостатка предложенного метода обфускации: недостаточная защищённость используемых псевдошумовых кодов и уязвимость против атаки, направленной на удаление водяного знака с использованием статистической оценки. Однако авторы заверяют, что оба недостатка могут быть успешно исправлены в будущем.

В статье [32] предлагается протокол запросов QuerySec для двухуровневых сенсорных сетей, отличающийся эффективным энергопотреблением. ЦВЗ в данном протоколе применяются для обеспечения целостности данных. Ответ на запрос к узлу хранения состоит из двух частей: результата запроса и информации для проверки целостности. Для формирования ЦВЗ данные, полученные с датчика, предварительно упорядочиваются, после чего для каждого элемента данных рассчитывается t бит кода обнаружения ошибок, например, циклический избыточный код. Однако встраивание ЦВЗ заключается в его объединении с

полезными данными с помощью конкатенации, поэтому фактически эта работа не относится к направлению встраивания информации в цифровые данные.

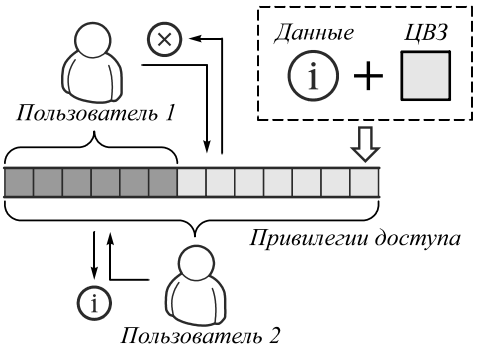

Рис. 6. Разграничение доступа пользователей к сенсорным данным с использованием обфускации на основе ЦВЗ [31]

Одним из типов данных, достаточно широко используемых в «интернете вещей», являются данные позиционирования. Такого рода данные в настоящее время позволяют собирать многие интеллектуальные устройства, например, смартфоны.

Авторы работы [33] предлагают онлайн-схему водяных знаков для защиты прав на траекторные потоки. Основная идея заключается в том, чтобы встроить водяной знак в последовательность значений, определяющих расстояния между парами мест расположения объектов. При этом местоположения объектов идентифицируются с использованием предлагаемого в работе алгоритма. Для определения пространственных границ потока данных авторы используют концепцию окна обработки, суть которой в том, что локально храниться во время обработки может только определённое число местоположений. По мере поступления большего количества входных данных более старые данные вытесняются, чтобы освободить место для новых. Для внедрения ЦВЗ необходимо идентифицировать местоположения объектов в потоке данных продвижением окна обработки, как это показано на рис. 7.

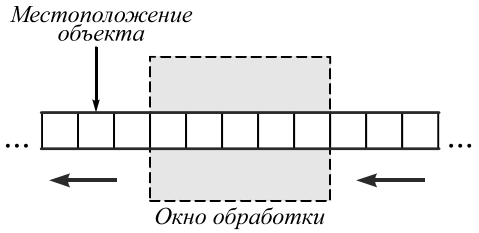

Рис. 7. Обработка потока траекторных данных с помощью передвигающегося окна [33]

Если в одном окне обработки отображаются два последовательных местоположения объектов, вычисляется расстояние между местоположениями. Далее бит водяного знака встраивается в это расстояние путём замены битов в заранее определённой позиции. Данная схема устойчива к различным атакам, таким как геометрические преобразования, добавление шума, сегментация и сжатие траектории. Указано, что процесс встраивания и обнаружения ЦВЗ был протестирован на 100 траекториях, каждая из которых имела 10 тысяч местоположений, временные затраты при этом составили 3340 мс.

Статья [34] описывает другой метод внедрения ЦВЗ в данные позиционирования – данные LiDAR, представляющие собой информацию о положении точек на поверхности Земли, хранимую в стандартизированном формате. Предлагаемая авторами схема водяных знаков может использоваться для защиты авторских прав и отслеживания источника данных. Для встраивания ЦВЗ сначала определяется вектор позиций маркеров, т.е. позиций, в которые будут встроены биты ЦВЗ, с использованием псевдослучайного генератора. Встраивание выполняется в круглую область вокруг позиций маркера, которая разбивается на более мелкие области, равномерно распределённые в круге, как это показано на рис. 8. Круговые области, отмеченные серым цветом, частично перекрываются, и соответствующие маркеры не используются для встраивания битов ЦВЗ.

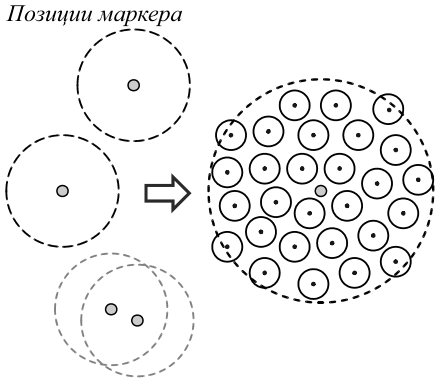

Рис. 8. Выбор области встраивания ЦВЗ в данные позиционирования [34]

На основе точек в полученных областях рассчитывается вектор расстояний, к которому применяется ДКП. Непосредственное внедрение ЦВЗ совершается путём модуляции последнего коэффициента ДКП. Результаты экспериментов демонстрируют устойчивость к наиболее вероятным атакам, таким как обрезка или случайное удаление точек. Время встраивания ЦВЗ для 29 миллионов точек составляет 12 с, извлечения – 10 с.

Некоторые авторы используют сочетание технологии ЦВЗ и шифрования. Подобный подход представлен в работе [35]. Чтобы установить доверие между узлом датчика и базовой станцией, авторы предлагают использовать водяные знаки. Для обеспечения контроля целостности предлагаемая схема присоединяет хрупкий ЦВЗ к исходным данным до того, как они будут переданы базовой станции. ЦВЗ генерируется путём объединения длины целочисленных данных, частоты возникновения цифр и времени захвата данных узлом датчика, а затем шифруется с помощью секретного ключа по алгоритму DES. Время генерации ЦВЗ занимает от 0,4 до 0,9 мс для разного количества пакетов (от 10 до 50). Время извлечения и верификации занимает от 0,5 до 1,2 мс соответственно. В качестве основного достоинства метода заявляется возможность его применения в условиях ограничен-

ности вычислительных ресурсов, что характерно для инфраструктуры «интернета вещей». Однако неясно, каким образом данное заявление сочетается с использованием шифрования на стороне датчиков. При этом нужно отметить, что данная работа, как и [32], не относится к классическому встраиванию ЦВЗ, поскольку сенсорные данные при встраивании ЦВЗ не изменяются, а объединяются с битами ЦВЗ с помощью конкатенации. Поэтому предлагаемая схема фактически осуществляет выработку и проверку кодов аутентичности сообщений для сенсорных данных.

В статье [36] предложена схема обеспечения безопасности данных с датчиков, основанная на совместном применении ЦВЗ и метода Compressed Sensing, который предназначен для восстановления полного сигнала из его разреженного или сжатого представления. В [36] данный метод используется для получения разреженного сигнала на стороне датчика с последующим восстановлением исходного сигнала на стороне базовой станции. На стороне датчика ЦВЗ генерируется на основе защищаемых данных с помощью хэш-функции, а затем встраивается в исходный сигнал, элементы которого дополняются пустыми символами в зависимости от значения бита ЦВЗ. Беспроводной канал передаёт данные, разреженные по методу Compressed Sensing, на базовую станцию. Декодер базовой станции восстанавливает полный сигнал, после чего ЦВЗ извлекается из контейнера. Для проверки целостности данных извлечённый ЦВЗ сравнивается с ЦВЗ, полученным на основе принятых данных. Авторы работы отмечают, что использование метода Compressed Sensing имеет преимущество перед традиционными методами криптографии, поскольку на этапе кодирования не требуется выполнение вычислительно сложных операций. При этом вычислительная сложность декодирования не является проблемой, поскольку базовая станция не имеет серьёзных аппаратных ограничений.

В работе [37] представлена схема защиты целостности данных «интернета вещей», основанная на применении хрупких ЦВЗ. Каждый сенсорный узел генерирует ЦВЗ с помощью хэш-функции SHA-1. Водяной знак встраивается внутрь пакета данных. Узел приёмника получает данные, а затем извлекает водяной знак и восстанавливает обнаруженные данные в соответствии с заданным правилом. Восстановленные данные используются для создания ЦВЗ в соответствии с тем же алгоритмом. Целостность проверяется путём сравнения восстановленного водяного знака и извлечённого водяного знака. Поскольку алгоритм внедрения ЦВЗ является обратимым, после его извлечения исходные данные восстанавливаются без потерь. Описанная схема разработана авторами с учётом ограничений ресурсов в беспроводных сенсорных сетях, поэтому она может успешно применяться для устройств с небольшими вычислительными возможностями. Однако данная работа входит в тот класс работ, в котором под встраиванием ЦВЗ понимается добавление к данным некоторой избыточности без изменения самих данных, поскольку биты пакета данных при встраивании ЦВЗ не изменяются, а объединяются с битами ЦВЗ с помощью конкатенации с дополнительным перемешиванием.

Авторы работы [38] предлагают метод обеспечения целостности сенсорных данных за счёт применения группирования данных с сенсорных датчиков для создания и внедрения ЦВЗ. Группы из переменного количества элементов данных образуются путём их конкатенации, размер группы зависит от исходных данных и секретного ключа. Для генерации ЦВЗ применяется хэш-функция MD5, причём для её вычисления требуется объединить две соседние группы. На рис. 9 приведена схема, показывающая, каким образом происходит вычисление и встраивание ЦВЗ после разбиения данных на группы.

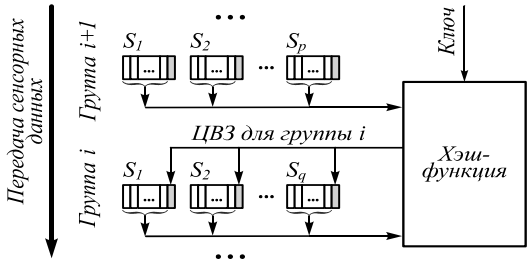

Рис. 9. Встраивание ЦВЗ в группы сенсорных данных [38]

Встраивание ЦВЗ выполняется в первую из двух последовательно расположенных групп по методу LSB. На стороне получателя для проверки целостности некоторой $(i+1)$-й группы необходима также предыдущая i-ая группа. В случае, если при проверке были обнаружены различия в ЦВЗ, извлечённом из принятых данных, и ЦВЗ, сгенерированном на их основе, невозможно сразу определить, в какой из двух групп произошла ошибка, поэтому для принятия окончательного решения нужно также выполнить проверку целостности для i-й группы. Описанная схема не требует больших вычислительных ресурсов для реализации, поэтому подходит для использования в «интернете вещей». Среднее время встраивания зависит от размера группы, для размера группы 500 оно не превышает 300 мс. К недостаткам метода можно отнести то, что ЦВЗ является хрупким, поэтому в случае каких-либо воздействий на информацию он будет разрушен, и реализовать проверку целостности будет невозможно.

В статье [39] аналогичное группирование элементов потока данных применяется в методе аутентификации данных в беспроводных сенсорных сетях. Авторы [39] взяли за основу идею алгоритмов внедрения ЦВЗ в цифровые изображения с использованием ошибок предсказания пикселей и применили её для защиты данных с датчиков. Сенсорный узел группирует данные потока, и две соседние неперекрывающиеся группы образуют группу аутентификации. Часть последовательно расположенных элементов данных служит для генерации ЦВЗ. К каждому из этих элементов применяется хэш-функция MD5, и все результаты объединяются с помощью операции XOR.

Остальные элементы данных группы аутентификации служат для встраивания ЦВЗ. Бит ЦВЗ скрывается в каждом из таких элементов путём сложения с соответствующим удвоенным элементом, уменьшенным на величину ошибки предсказания. Ошибка предсказания корректируется после изменения каждого элемента. Основными достоинствами данного метода авторы называют низкую вычислительную сложность и обратимость. Также они отмечают отсутствие существенных задержек в передаче потоковых данных при внедрении ЦВЗ согласно описанной схеме.

В [40] представлен метод, позволяющий связывать наборы данных с источником их происхождения. Для этого в набор данных предлагается встраивать дополнительную информацию о его происхождении (принадлежности). Эту информацию авторы именуют меткой принадлежности, однако по своему назначению и свойствам она полностью соответствует понятию ЦВЗ. Метод рассчитан на работу с произвольными наборами однотипных данных, обладающих избыточностью на уровне отдельных значений. Метка принадлежности представляет собой двоичную последовательность фиксированной длины. Эта последовательность разбивается на частично перекрывающиеся части, которые записываются в n младших битов элементов набора данных. Два дополнительных бита служат для проверки: бит проверки параметра содержит свёртку наиболее значимых битов элемента данных со значением количества частей метки принадлежности, бит проверки метки содержит свёртку наиболее значимых битов элемента данных со значением самой метки. На рис. 10 показана схема встраивания для значения $n=6$ с перекрытием фрагментов в 2 бита.

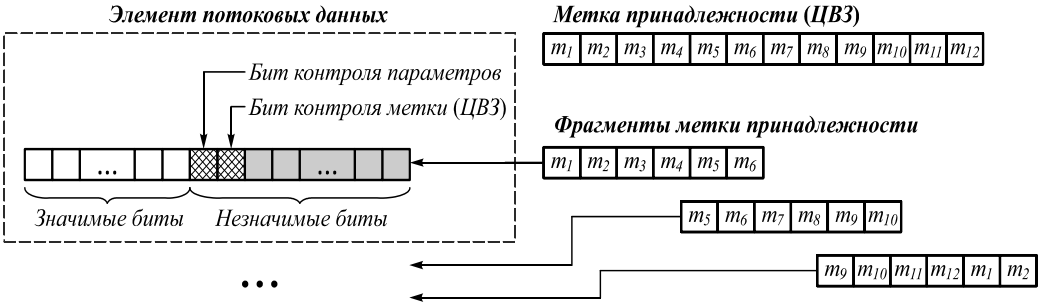

Рис. 10. Встраивание метки принадлежности в потоковые данные [40]

Достоинством метода является то, что независимо от полного объёма данных метка принадлежности может быть извлечена из ограниченной выборки, что достигается за счёт избыточного встраивания. Следует отметить, что авторы данного исследования явно не связывают его с «интернетом вещей», однако в качестве рекомендуемых приложений указывают подтверждение принадлежности различных сенсорных данных, а также GPS-данных, что актуально для «интернета вещей».

4. Обсуждение результатов

В предыдущем параграфе был рассмотрен ряд работ, посвящённых стеганографическому встраиванию информации в разные цифровые данные для её безопасной передачи в «интернете вещей». Обобщение полученных результатов представлено в табл. 1.

Изображения наиболее популярны в методах стеганографии, предлагаемых для использования в «интернете вещей», как и в классических приложениях. Табл. 1 является демонстрацией данного факта. Однако в ряде случаев авторы не обосновывают причины позиционирования своих исследований как обеспечивающих безопасность в «интернете вещей». Практически во всех остальных случаях причиной применения предлагаемого метода для «интернета вещей» называется низкая вычислительная сложность. Для достижения этого свойства в большинстве работ предлагается использовать методы, основанные на методе LSB в пространственной области. Однако LSB имеет серьёзные недостатки: уязвимость перед стегоанализом и отсутствие минимальной робастности. В параграфе 1 были приведены примеры других методов встраивания информации в цифровые изображения, сопоставимых по сложности с LSB, но отличающихся большей эффективностью, таких как PM1 и QIM. Кроме того, необходимо отметить, что использование пространственного встраивания также является не вполне обоснованным решением. Применение частотного преобразования к цифровому изображению требует дополнительных вычислительных затрат, однако пространственное встраивание без обеспечения свойства робастности приводит к необходимости передавать по сети исключительно несжатые изображения, что существенно увеличивает нагрузку на сеть.

Эффективность встраивания оценивается по критериям незаметности, в частности, по метрике PSNR, и ёмкости. Конкретные значения этих характеристик приводятся при описании некоторых алгоритмов, авторы которых указали в своих работах соответствующие сведения. Поскольку данная информация представлена не во всех рассмотренных статьях, а условия проведения вычислительных экспериментов, в том числе используемые базы тестовых изображений, различны, корректное сравнение эффективности алгоритмов по двум данным характеристикам не представляется возможным. Кроме того, указанные характеристики являются классическими при оценке алгоритмов сокрытия информации в изображениях, но они недостаточно информативны для задач безопасности в «интернете вещей». Устойчивость перед стегоанализом в большинстве работ также не анализируется.

Табл. 1. Характеристики методов стеганографии

Источник	Цель применения	Контейнер	Метод встраивания	Применимость в «интернете вещей»
[12]	Конфиденциальность данных	Сжатые JPEG-изображения	Замена битов в пространственной области	Не обосновано
[13]	Улучшение качества встраивания	Сжатые и несжатые изображения	LSB в пространственной области или в области ДКП	Не обосновано
[14]	Конфиденциальность медицинской информации	Несжатые изображения	Замена битов в пространственной области	Низкая вычислительная сложность
[15]	Конфиденциальность медицинской информации	Несжатые изображения	Интерполяция контейнера и аддитивное встраивание с применением модульной арифметики	Низкая вычислительная сложность
[16]	Конфиденциальность данных	Изображения, сжатые с помощью векторного квантования	Замена битов в пространственной области	Не обосновано
[17]	Безопасная локализация беспроводных устройств	Несжатые изображения	LSB в пространственной области	Не обосновано
[18]	Защита Android-приложений от обратной инженерии	Несжатые изображения	LSB в пространственной области	Мобильное устройство является шлюзом для сервисов «интернета вещей»
[19]	Конфиденциальность медицинской информации	Несжатые изображения	Замена коэффициентов ДВП	Не обосновано
[20]	Конфиденциальность и целостность данных	Несжатые изображения	LSB в пространственной области	Низкая вычислительная сложность
[21]	Конфиденциальность и аутентификация данных	Несжатые изображения	LSB в области ДВП	Низкая вычислительная сложность
[22]	Преодоление уязвимости «человек посередине» протокола BLE	Изображения	Не указано	Не обосновано
[23]	Конфиденциальность изображений	Несжатые изображения	Схема разделения секрета Шамира	Не обосновано
[24]	Скрытая передача отчётов о некорректном поведении водителей	Радиомаяковые сигналы сетей VANET	LSB в пространственной области	Низкая вычислительная сложность
[25]	Агрегация и конфиденциальность медицинской информации	Сети датчиков тела	Операция XOR	Низкая вычислительная сложность, снижение нагрузки на сеть

Наконец, ни в одной работе не рассматривается, каким образом гетерогенная инфраструктура «интернета вещей» влияет на процесс создания и передачи стегоизображений. Таким образом, можно сделать вывод, что предложенные методы сокрытия информации не являются специфическими для «интернета вещей».

Стоит отдельно отметить работы [24, 25], поскольку контейнерами для сокрытия информации в них являются не цифровые изображения, а данные беспроводных сетей, что делает данные методы предназначенными именно для защиты информации в «интернете вещей». Но подобные работы в настоящий момент находятся в меньшинстве в рассматриваемой проблемной области.

Обобщение результатов обзора работ в области внедрения ЦВЗ в цифровые данные в «интернете вещей» представлено в табл. 2.

Здесь наблюдается обратная ситуация: защита цифровых изображений в «интернете вещей» с помощью ЦВЗ представлена только в двух работах, ещё в одной речь идёт о защите видеосигнала, а почти во всех остальных работах контейнерами для дополнительной информации являются данные беспроводных сенсорных сетей.

Представленные алгоритмы направлены на решение достаточно узких задач, в связи с чем разнородность приведённых авторами результатов экспериментов с реальными данными, как и разнородность самих этих данных, не позволяет корректно сравнивать эффективность алгоритмов. Поэтому основное внимание в настоящем обзоре сфокусировано на исследовании применимости данных алгоритмов в «интернете вещей».

Табл. 2. Характеристики методов ЦВЗ

Источник	Цель применения	Контейнер	Метод встраивания	Применимость в «интернете вещей»
[26]	Целостность изображений микрочипов ДНК	Несжатые изображения микрочипов ДНК	Аддитивное встраивание	Низкая вычислительная сложность
[27]	Аутентификация изображений в беспроводных мультимедийных сенсорных сетях	Несжатые изображения	Аддитивно-мультипликативное встраивание в ДВП-коэффициенты	Энергоэффективность, устойчивость к помехам в беспроводных каналах связи и потере пакетов
[28]	Защита от подмены видеосигнала	Видеосигнал	LSB в области ДКП	Не обосновано
[29]	Аутентификация данных	Данные беспроводной сенсорной сети	Расширение спектра	Низкая вычислительная сложность, снижение нагрузки на сеть
[30]	Целостность данных	Данные беспроводной сенсорной сети	Расширение спектра	Низкая вычислительная сложность, сохранение естественной корреляции между потоками данных
[31]	Обфускация данных	Данные беспроводной сенсорной сети	Расширение спектра	Низкая вычислительная сложность, масштабируемость
[33]	Защита прав на траекторные потоки	Данные позиционирования	Замена битов	Устойчивость к атакам, связанным с зашумлением и искажением данных, потоковая обработка
[34]	Защита авторских прав и отслеживание источника данных	Данные LiDAR	Модуляция коэффициента ДКП	Устойчивость к атакам, связанным с зашумлением и искажением данных
[36]	Целостность данных	Данные беспроводной сенсорной сети	Дополнение данных пустым символом	Низкая вычислительная сложность
[38]	Целостность данных	Данные беспроводной сенсорной сети	LSB для произвольных данных	Низкая вычислительная сложность
[39]	Аутентификация данных	Данные беспроводной сенсорной сети	Аддитивное встраивание с применением ошибок предсказания	Низкая вычислительная сложность, быстродействие
[40]	Привязка наборов данных к источнику их происхождения	Произвольные последовательности данных (в том числе сенсорные данные, данные GPS)	LSB для произвольных данных	Низкая вычислительная сложность

В большинстве случаев авторы обосновывают предлагаемые ими решения низкой вычислительной сложностью алгоритмов, позволяющей осуществлять их реализацию в условиях ограниченных аппаратных ресурсов. Во многих работах указаны затраты времени на внедрение и извлечение ЦВЗ, и малые затраты времени также отмечаются авторами как одно из доказательств эффективной работы их алгоритмов в «интернете вещей». Это является достоинством таких алгоритмов, но наряду с этим очевидно, что время обработки существенно зависит от оборудования, на котором выполнялось тестирование, однако характеристики данного оборудования во многих статьях опускаются.

Среди методов непосредственно встраивания данных распространён метод расширения спектра, но также используются методы замены битов, в том числе LSB, и аддитивное встраивание. Кроме того, в отдельных работах под встраиванием ЦВЗ подразумевается присоединение к передаваемым данным криптографического хэш-кода или кода контроля целостности. Это не имеет отношения к методам ЦВЗ, поэтому такого рода работы, отмеченные в обзоре, исключены из табл. 2.

Для схем обеспечения безопасности данных, поступающих с многочисленных сенсорных датчиков, актуально совместное решение задач агрегации и защиты данных. Примеры работ, реализующих такой подход, представлены в [25, 29, 31, 36].

Также следует отметить, что ряд работ, посвящённых как стеганографическому встраиванию [15, 23], так и ЦВЗ [26, 31, 37, 39], характеризуется таким свойством, как обратимость, т.е. способность полностью восстановить цифровой контейнер после извле-

чения вложения. Данное свойство более актуально для инфраструктуры «интернета вещей», чем в случае классических методов встраивания информации, поскольку данные, передаваемые между интеллектуальными устройствами, часто используются для дальнейшего анализа. Внесение необратимых изменений на этапе сокрытия информации может существенно исказить результаты.

Подводя итоги проведённого обзора, можно выделить ряд проблем, связанных с разработкой методов встраивания информации, предназначенных для использования в инфраструктуре «интернета вещей». Такой проблемой является соблюдение баланса между уровнем безопасности и вычислительной сложностью. Ограниченность ресурсов различных датчиков побуждает исследователей обращаться к самым простым из возможных методов встраивания, таким как LSB, что исключает робастность и устойчивость перед стегоанализом. Другой проблемой является необходимость последующей обработки передаваемых данных. Из этого следует, что метод встраивания информации должен либо быть обратимым, либо обеспечивать уровень незаметности встраивания, позволяющий выполнять необходимые операции с данными. Также необходимо учитывать применение операции агрегации. В сенсорных сетях это типовая операция, уменьшающая количество данных, поступающих от датчиков, и ЦВЗ должен сохраняться после применения данной операции, поэтому актуальным направлением является развитие методов, учитывающих данное требование.

Исходя из полученных результатов, сформулируем актуальные задачи в области методов сокрытия информации для последующей передачи в «интернете вещей». Актуальным является поиск новых вычислительно эффективных алгоритмов встраивания информации в цифровые данные, отличающихся повышенной незаметностью, робастностью и устойчивостью к стегоанализу. Другим заслуживающим внимания направлением является обеспечение одновременного решения задач агрегации и защиты данных. Ещё одна актуальная задача – обеспечение обратимости встраивания для последующей корректной обработки цифровых объектов.

Заключение

В данной статье был рассмотрен ряд актуальных работ в области встраивания информации в цифровые объекты, передаваемые в «интернете вещей». Результаты анализа рассмотренных работ показали, что на сегодняшний день универсального решения задачи обеспечения безопасности в «интернете вещей» за счёт стеганографического встраивания и встраивания ЦВЗ не найдено. Более того, многие методы, позиционируемые их авторами как направленные на защиту данных в «интернете вещей», фактически малопригодны для использования в данной области. Таким образом, разработка новых эффективных методов является перспективным направлением исследований.

Благодарности

Данная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания ТУСУР на 2017–2019 гг. (проект № 2.3583.2017/4.6). Кроме того, авторы выражают благодарность рецензентам за конструктивные замечания, которые помогли улучшить данную статью.

Литература

1. **Li, S.** The internet of things: a survey / S. Li, L.D. Xu, S. Zhao // Information Systems Frontiers. – 2015. – Vol. 17, Issue 2. – P. 243-259. – DOI: 10.1007/s10796-014-9492-7.
2. **Boavida, F.** People-centric internet of things – Challenges, approach, and enabling technologies / F. Boavida, A. Kliem, T. Renner, J. Riekki, C. Jouvray, M. Jacovi, S. Ivanov, F. Guadagni, P. Gil, A. Triviño. – In: Intelligent Distributed Computing IX / ed. by P. Novais, D. Camacho, C. Analide, A.E.F. Seghrouchni, C. Badica. – Cham: Springer, 2016. – P. 463-474. – DOI: 10.1007/978-3-319-25017-5_44.
3. **Hmood, A.K.** On the capacity and security of steganography approaches: An overview / A.K. Hmood, H.A. Jalab, Z.M. Kasirun, B.B. Zaidan, A.A. Zaidan // Journal of Applied Sciences. – 2010. – Vol. 10, Issue 16. – P. 1825-1833. – DOI: 10.3923/jas.2010.1825.1833.
4. **Bazyar, M.** A recent review of MP3 based steganography methods / M. Bazyar, R. Sudirman // International Journal of Security and its Applications. – 2014. – Vol. 8, Issue 6. – P. 405-414. – DOI: 10.14257/ijsia.2014.8.6.35.
5. **Cheddad, A.** Digital image steganography: Survey and analysis of current methods / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // Signal Processing. – 2010. – Vol. 90, Issue 3. – P. 727-752. – DOI: 10.1016/j.sigpro.2009.08.010.
6. **Sadek, M.M.** Video steganography: a comprehensive review / M.M. Sadek, A.S. Khalifa, M.G.M. Mostafa // Multimedia Tools and Applications. – 2015. – Vol. 74, Issue 17. – P. 7063-7094. – DOI: 10.1007/s11042-014-1952-z.
7. **Fridrich, J.** Steganography in digital media: Principles, algorithms and applications / J. Fridrich. – New York: Cambridge University Press, 2010. – 437 p. – ISBN: 978-0-521-19019-0.
8. **Mitekin, V.** A new QIM-based watermarking algorithm robust against multi-image histogram attack / V. Mitekin, V. Fedoseev // Procedia Engineering. – 2017. – Vol. 201. – P. 453-462. – DOI: 10.1016/j.proeng.2017.09.687.
9. **Bianchi, T.** Secure watermarking for multimedia content protection: A review of its benefits and open issues / T. Bianchi, A. Piva // IEEE Signal Processing Magazine. – 2013. – Vol. 30, Issue 2. – P. 87-96. – DOI: 10.1109/MSP.2012.2228342.
10. **Kannan, D.** An extensive research on robust digital image watermarking techniques: A review / D. Kannan, M. Gobi // International Journal of Signal and Imaging Systems Engineering. – 2015. – Vol. 8, Issues 1-2. – P. 89-104. – DOI: 10.1504/IJSISE.2015.067047.
11. **Panah, A.S.** On the properties of non-media digital watermarking: A review of state of the art techniques / A.S. Panah, R.V. Schyndel, T. Sellis, E. Bertino // IEEE Access. – 2016. – Vol. 4. – P. 2670-2704. – ISSN 2169-3536. – DOI: 10.1109/ACCESS.2016.2570812.
12. **Bairagi, A.K.** An efficient steganographic approach for protecting communication in the Internet of Things IoT critical infrastructures / A.K. Bairagi, R. Khondoker, R. Islam // Information Security Journal: A Global Perspective. – 2016. – Vol. 25, Issues 4-6. – P. 192-212. – DOI: 10.1080/19393555.2016.1206640.

13. **Li, H.** The maximum matching degree sifting algorithm for steganography pretreatment applied to IoT / H. Li, L. Hu, J. Chu, L. Chi, H. Li // Multimedia Tools and Applications. – 2018. – Vol. 77, Issue 14. – P. 18203-18221. – DOI: 10.1007/s11042-017-5075-1.
14. **Parah, S.A.** High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems / S.A. Parah, J.A. Sheikh, F. Ahad, G.M. Bhat. – In: Internet of things and big data analytics toward next-generation intelligence / ed. by N. Dey, A.E. Hassanien, C. Bhatt, A.S. Ashour, S.C. Satapathy. – Cham, Switzerland: Springer International Publishing AG, 2018. – P. 409-437. – DOI: 10.1007/978-3-319-60435-0_17.
15. **Parah, S.A.** Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication / S.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan // Future Generation Computer Systems. – 2018. – In Press. – DOI: 10.1016/j.future.2018.02.023.
16. **Huang, C.-T.** VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements / C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, S.-J. Wang // Journal of Supercomputing. – 2016. – Vol. 74, Issue 9. – P. 4295-4314. – DOI: 10.1007/s11227-016-1874-9.
17. **Tondwalkar, A.** Secure localisation of wireless devices with application to sensor networks using steganography / A. Tondwalkar, P. Vinayakray-Jani // Procedia Computer Science. – 2016. – Vol. 78. – P. 610-616. – DOI: 10.1016/j.procs.2016.02.107.
18. **Kim, S.R.** Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications / S.R. Kim, J.N. Kim, S.T. Kim, S. Shin, J.H. Yi // The Journal of Supercomputing. – 2018. – Vol. 74, Issue 9. – P. 4261-4280. – DOI: 10.1007/s11227-016-1848-y.
19. **Elhoseny, M.** Secure medical data transmission model for IoT-based healthcare systems / M. Elhoseny, G. Ramírez-González, O.M. Abu-Elnasr, S.A. Shawkat, A. N, A. Farouk // IEEE Access. – 2018. – Vol. 6. – P. 20596-20608. – DOI: 10.1109/ACCESS.2018.2817615.
20. **Das, R.** Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques / R. Das, I. Das // Proceedings of the 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN). – 2016. – P. 296-301. – DOI: 10.1109/ICRCICN.2016.7813674.
21. **Yassin, A.A.** Toward for strong authentication code in cloud of internet of things based on DWT and steganography / A.A. Yassin, A.M. Rashid, Z.A. Abduljabbar, H.A.A. Alasadi, A.J.Y. Aldarwish // Journal of Theoretical and Applied Information Technology. – 2018. – Vol. 96, Issue 10. – P. 2922-2935.
22. **Bapat, C.** Smart-lock security re-engineered using cryptography and steganography / C. Bapat, G. Baleri, S. Inamdar, A.V. Nimkar. – In Book: Security in computing and communications / ed. by S.M. Thampi, G.M. Pérez, C.B. Westphall, J. Hu, C.I. Fan, F.G. Mármol. – Singapore: Springer Nature Singapore Pte Ltd., 2017. – P. 325-336. – DOI: 10.1007/978-981-10-6898-0_27.
23. **Li, L.** Distortion less secret image sharing scheme for Internet of Things system / L. Li, M.S. Hossain, A.A. Abd El-Latif, M.F. Alhamid // Cluster Computing. – 2017. – P. 1-15. – DOI: 10.1007/s10586-017-1345-y.
24. **De Fuentes, J.M.** Applying information hiding in VANETs to covertly report misbehaving vehicles / J.M. de Fuentes, J. Blasco, A.I. González-Tablas, L. González-Manzano // International Journal of Distributed Sensor Networks. – 2014. – Vol. 10, Issue 2. – P. 1-15. – DOI: 10.1155/2014/120626.
25. **Ren, J.** A sensitive data aggregation scheme for body sensor networks based on data hiding / J. Ren, G. Wu, L. Yao // Personal and Ubiquitous Computing. – 2013. – Vol. 17, Issue 7. – P. 1317-1329. – DOI: 10.1007/s00779-012-0566-6.
26. **Pizzolante, R.** On the protection of consumer genomic data in the Internet of Living Things / R. Pizzolante, A. Castiglione, B. Carpentieri, A. De Santis, F. Palmieri, A. Castiglione // Computers & Security. – 2018. – Vol. 74. P. 384-400. – DOI: 10.1016/j.cose.2017.06.003.
27. **Wang, H.** Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks / H. Wang // Journal of Supercomputing. – 2013. – Vol. 64, Issue 3. – P. 883-897. – DOI: 10.1016/j.cose.2017.06.003.
28. **Wang, J.** A cross-layer authentication design for secure video transportation in wireless sensor network / J. Wang, G.L. Smith // International Journal of Security and Networks. – 2010. – Vol. 5, Issue 1. – P. 63-76. – DOI: 10.1504/IJSN.2010.030724.
29. **Zhang, W.** Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach / W. Zhang, Y. Liu, S.K. Das, P. De // Pervasive and Mobile Computing. – 2008. – Vol. 4, Issue 5. – P. 658-680. – DOI: 10.1016/j.pmcj.2008.05.005.
30. **Panah, A.S.** In the shadows we trust: A secure aggregation tolerant watermark for data streams / A.S. Panah, R.V. Schyndel, T. Sellis, E. Bertino // Proceedings of the IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). – 2015. – P. 1-9. – DOI: 10.1109/WoWMoM.2015.7158149.
31. **Yavari, A.** Scalable role-based data disclosure control for the Internet of Things / A. Yavari, A.S. Panah, D. Georgakopoulos, P.P. Jayaraman, R. Van Schyndel // Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS). – 2017. – P. 2226-2233. – DOI: 10.1109/ICDCS.2017.307.
32. **Yi, Y.** A digital watermarking approach to secure and precise range query processing in sensor networks // Y. Yi, R. Li, F. Chen, A.X. Liu, Y. Lin // 2013 Proceedings IEEE INFOCOM. – 2013. – P. 1950-1958. – DOI: 10.1109/INFCOM.2013.6566995.
33. **Yue, M.** Rights protection for trajectory streams / M. Yue, Z. Peng, K. Zheng, Y. Peng. – In: Database systems for advanced applications / ed. by S.S. Bhowmick, C.E. Dyreson, C.S. Jensen, M.L. Lee, A. Muliantara, B. Thalheim. – Cham, Switzerland: Springer International Publishing, 2014. – P. 407-421. – DOI: 10.1007/978-3-319-05813-9_27.
34. **Lipuš, B.** Robust watermarking of airborne LiDAR data / B. Lipuš, B. Žalik // Multimedia Tools and Applications. – 2018. – Vol. 77, Issue 21. – P. 29077-29097. – DOI: 10.1007/s11042-018-6039-9.
35. **Hameed, K.** Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks / K. Hameed, A. Khan, M. Ahmed, A.G. Reddy, M.M. Rathore // Future Generation Computer Systems. – 2018. – Vol. 82. – P. 274-289. – DOI: 10.1016/j.future.2017.12.009.
36. **Wang, C.** Data secure transmission model based on compressed sensing and digital watermarking technology / C. Wang, Y. Bai, X. Mo // Wuhan University Journal of Natural Sciences. – 2014. – Vol. 19, Issue 6. – P. 505-511. – DOI: 10.1007/s11859-014-1045-x.

37. **Zhang, G.** A new digital watermarking method for data integrity protection in the perception layer of IoT / G. Zhang, L. Kou, L. Zhang, C. Liu, Q. Da, J. Sun // Security and Communication Networks. – 2017. – Vol. 2017. – 3126010 (12 p.). – DOI: 10.1155/2017/3126010.
38. **Kamel, I.** Simplified watermarking scheme for sensor networks / I. Kamel, H. Juma // International Journal of Internet Protocol Technology. – 2010. – Vol. 5, Issues 1-2. – P. 101-111. – DOI: 10.1504/IJIPT.2010.032619.
39. **Shi, X.** A reversible watermarking authentication scheme for wireless sensor networks / X. Shi, D. Xiao // Information Sciences. – 2013. – Vol. 240. – P. 173-183. – DOI: 10.1016/j.ins.2013.03.031.
40. **Chong, S.** Self-identifying data for fair use / S. Chong, C. Skalka, J.A. Vaughan // Journal of Data and Information Quality. – 2015. – Vol. 5, Issue 3. – 11 (30 p.). – DOI: 10.1145/2687422.

Сведения об авторах

Евсютин Олег Олегович, 1987 года рождения, в 2009 году окончил Томский государственный университет систем управления и радиоэлектроники (ТУСУР) по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем». Кандидат технических наук (2012 год), работает доцентом кафедры безопасности информационных систем ТУСУР. Область научных интересов: информационная безопасность, обработка цифровых изображений, приложения клеточных автоматов. E-mail: *eoo@keva.tusur.ru* .

Кокурина Анна Сергеевна, 1994 года рождения, в 2018 году окончила ТУСУР по специальности «Информационно-аналитические системы безопасности». Работает младшим научным сотрудником кафедры безопасности информационных систем ТУСУР. Область научных интересов: информационная безопасность, стеганография. E-mail: *annakokurina94@yandex.ru* .

Мещеряков Роман Валерьевич, 1974 года рождения, в 1997 году окончил Алтайский государственный технический университет им. И.И. Ползунова по специальности «Информационно-измерительная техника и технологии». Кандидат технических наук (2000 год), доктор технических наук (2012 год), профессор РАН. Работает главным научным сотрудником в Институте проблем управления им. В.А. Трапезникова Российской академии наук. Область научных интересов: обработка, анализ, синтез речевого сигнала и текста, системный анализ, информационная безопасность, математическое моделирование. E-mail: *mrv@ipu.ru* .

ГРНТИ: 28.23.15
Поступила в редакцию 11 августа 2018 г. Окончательный вариант – 17 декабря 2018 г.

A review of methods of embedding information in digital objects for security in the internet of things

O.O. Evsutin [1], A.S. Kokurina [1], R.V. Meshcheryakov [2]
[1] Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia,
[2] V.A. Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russia

Abstract

Transmission, processing and storage of information in the infrastructure of the Internet of Things are related to the necessity for solving a number of problems in information security. The main difficulty lies in the fact that the infrastructure of the Internet of Things is not homogeneous and contains many different devices, including those with limited computing resources. One of the approaches to solving these problems is to embed additional information into the transmitted and stored digital objects. In this paper we present a review of methods of embedding information in digital data to provide security in the Internet of Things, including methods of steganographic embedding of information and methods for embedding digital watermarks. We reviewed methods of embedding information into digital images, as well as wireless sensor network data, proposed for use in the Internet of Things. In this paper we defined the advantages and disadvantages of individual methods and groups of methods, also we analyzed their applicability for data protection in the Internet of Things. Relevant trends in this field of research have been identified.

Keywords: information security, Internet of Things, information embedding, digital images, steganography, digital watermark.

Citation: Evsutin OO, Kokurina AS, Meshcheryakov RV. A review of the methods of embedding information in digital objects for security in the Internet of things. Computer Optics 2019; 43(1): 137-154. DOI: 10.18287/2412-6179-2019-43-1-137-154.

Acknowledgements: The work was funded by the Russian Federation Ministry of Education and Science (grant 2.3583.2017/4.6).

References

[1] Li S, Xu LD, Zhao S. The internet of things: a survey. Information Systems Frontiers 2015; 17(2): 243-259. DOI: 10.1007/s10796-014-9492-7.

[2] Boavida F, Kliem A, Renner T, Riekki J, Jouvray C, Jacovi M, Ivanov S, Guadagni F, Gil P, Triviño A. People-centric internet of things – Challenges, approach, and enabling technologies. In Book: Novais P, Camacho D, Analide C, Seghrouchni AEF, Badica C, eds. Intelligent Distributed Computing IX. Cham: Springer; 2016: 463-474. DOI: 10.1007/978-3-319-25017-5_44.

[3] Hmood AK, Jalab HA, Kasirun ZM, Zaidan BB, Zaidan AA. On the capacity and security of steganography approaches: An overview. Journal of Applied Sciences 2010; 10(16): 1825-1833. DOI: 10.3923/jas.2010.1825.1833.

[4] Bazyar M, Sudirman R. A recent review of MP3 based steganography methods. International Journal of Security and its Applications 2014; 8(6): 405-414. DOI: 10.14257/ijsia.2014.8.6.35.

[5] Cheddad A, Condell J, Curran K, Mc Kevitt P. Digital image steganography: Survey and analysis of current methods. Signal Processing 2010; 90(3): 727-752. DOI: 10.1016/j.sigpro.2009.08.010.

[6] Sadek MM, Khalifa AS, Mostafa MGM. Video steganography: a comprehensive review. Multimedia Tools and Applications 2015; 74(17): 7063-7094. DOI: 10.1007/s11042-014-1952-z.

[7] Fridrich J. Steganography in digital media: Principles, algorithms and applications. New York: Cambridge University Press; 2010. ISBN: 978-0-521-19019-0.

[8] Mitekin V, Fedoseev V. A new QIM-based watermarking algorithm robust against multi-image histogram attack. Procedia Engineering 2017; 201: 453-462. DOI: 10.1016/j.proeng.2017.09.687.

[9] Bianchi T, Piva A. Secure watermarking for multimedia content protection: A review of its benefits and open issues. IEEE Signal Processing Magazine 2013; 30(2): 87-96. DOI: 10.1109/MSP.2012.2228342

[10] Kannan D, Gobi M. An extensive research on robust digital image watermarking techniques: A review. International Journal of Signal and Imaging Systems Engineering 2015; 8(1-2): 89-104. DOI: 10.1504/IJSISE.2015.067047.

[11] Panah AS, Schyndel RV, Sellis T, Bertino E. On the properties of non-media digital watermarking: A review of state of the art techniques. IEEE Access 2016; 4: 2670-2704. DOI: 10.1109/ACCESS.2016.2570812.

[12] Bairagi AK, Khondoker R, Islam R. An efficient steganographic approach for protecting communication in the Internet of Things IoT critical infrastructures. Information Security Journal: A Global Perspective 2016; 25(4-6): 192-212. DOI: 10.1080/19393555.2016.1206640.

[13] Li H, Hu L, Chu J, Chi L, Li H. The maximum matching degree sifting algorithm for steganography pretreatment applied to IoT. Multimedia Tools and Applications 2018; 77(14): 18203-18221. DOI: 10.1007/s11042-017-5075-1.

[14] Parah SA, Sheikh JA, Ahad F, Bhat GM. High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems. In Book: Dey N, Hassanien AE, Bhatt C, Ashour AS, Satapathy SC, eds. Internet of things and big data analytics toward next-generation intelligence. Cham, Switzerland: Springer International Publishing AG; 2018: 409-437. DOI: 10.1007/978-3-319-60435-0_17.

[15] Parah SA, Sheikh JA, Akhoon JA, Loan NA. Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. Future Generation Computer Systems 2018; In Press. DOI: 10.1016/j.future.2018.02.023.

[16] Huang C-T, Tsai M-Y, Lin L-C, Wang W-J, Wang S-J. VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements. Journal of Supercomputing 2016; 74(9): 4295-4314. DOI: 10.1007/s11227-016-1874-9.

[17] Tondwalkar A, Vinayakray-Jani P. Secure localisation of wireless devices with application to sensor networks using steganography. Procedia Computer Science 2016; 78: 610-616. DOI: 10.1016/j.procs.2016.02.107.

[18] Kim SR, Kim JN, Kim ST, Shin S, Yi JH. Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications. The Journal of Supercomputing 2018; 74(9): 4261-4280. DOI: 10.1007/s11227-016-1848-y.

[19] Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, N A, Farouk A. Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 2018; 6: 20596-20608. DOI: 10.1109/ACCESS.2018.2817615

[20] Das R, Das I. Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques. Proceedings of the Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) 2016: 296-301. DOI: 10.1109/ICRCICN.2016.7813674.

[21] Yassin AA, Rashid AM, Abduljabbar ZA, Alasadi HAA, Aldarwish AJY. Toward for strong authentication code in cloud of internet of things based on DWT and steganography. Journal of Theoretical and Applied Information Technology 2018; 96(10): 2922-2935.

[22] Bapat C, Baleri G, Inamdar S, Nimkar AV. Smart-lock security re-engineered using cryptography and steganography. In Book: Thampi SM, Pérez GM, Westphall CB, Hu J, Fan CI, Mármol FG, eds. Security in computing and communications. Singapore: Springer Nature Singapore Pte Ltd; 2017: 325-336. DOI: 10.1007/978-981-10-6898-0_27.

[23] Li L, Hossain MS, Abd El-Latif AA, Alhamid MF. Distortion less secret image sharing scheme for Internet of Things system. Cluster Computing 2017; 1-15. DOI: 10.1007/s10586-017-1345-y.

[24] De Fuentes JM, Blasco J, González-Tablas AI, González-Manzano L. Applying information hiding in VANETs to covertly report misbehaving vehicles. International Journal of Distributed Sensor Networks 2014; 10(2): 1-15. DOI: 10.1155/2014/120626.

[25] Ren J, Wu G, Yao L. A sensitive data aggregation scheme for body sensor networks based on data hiding. Personal and Ubiquitous Computing 2013; 17(7): 1317-1329. DOI: 10.1007/s00779-012-0566-6.

[26] Pizzolante R, Castiglione A, Carpentieri B, De Santis A, Palmieri F, Castiglione A. On the protection of consumer genomic data in the Internet of Living Things. Computers & Security 2018; 74: 384-400. DOI: 10.1016/j.cose.2017.06.003.

[27] Wang H. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. Journal of Supercomputing 2013; 64(3): 883-897. DOI: 10.1016/j.cose.2017.06.003.

[28] Wang J, Smith GL. A cross-layer authentication design for secure video transportation in wireless sensor network. International Journal of Security and Networks 2010; 5(1): 63-76. DOI: 10.1504/IJSN.2010.030724.

[29] Zhang W, Liu Y, Das SK, De P. Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. Pervasive and Mobile Computing 2008; 4(5): 658-680. DOI: 10.1016/j.pmcj.2008.05.005.
[30] Panah AS, Schyndel RV, Sellis T, Bertino E. In the shadows we trust: A secure aggregation tolerant watermark for data streams. Proceedings of the IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2015: 1-9. DOI: 10.1109/WoWMoM.2015.7158149.
[31] Yavari A, Panah AS, Georgakopoulos D, Jayaraman PP, Van Schyndel R. Scalable role-based data disclosure control for the Internet of Things. Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS) 2017: 2226-2233. DOI: 10.1109/ICDCS.2017.307.
[32] Yi Y, Li R, Chen F, Liu AX, Lin Y. A digital watermarking approach to secure and precise range query processing in sensor networks. 2013 Proceedings IEEE INFOCOM 2013: 1950-1958. DOI: 10.1109/INFCOM.2013.6566995.
[33] Yue M, Peng Z, Zheng K, Peng Y. Rights protection for trajectory streams. In Book: Bhowmick SS, Dyreson CE, Jensen CS, Lee ML, Muliantara A, Thalheim B, eds. Database systems for advanced applications. Cham, Switzerland: Springer International Publishing; 2014: 407-421. DOI: 10.1007/978-3-319-05813-9_27.
[34] Lipuš B, Žalik B. Robust watermarking of airborne LiDAR data. Multimedia Tools and Applications 2018; 77(21): 29077-29097. DOI: 10.1007/s11042-018-6039-9.
[35] Hameed K, Khan A, Ahmed M, Reddy AG, Rathore MM. Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. Future Generation Computer Systems 2018; 82: 274-289. DOI: 10.1016/j.future.2017.12.009.
[36] Wang C, Bai Y, Mo X. Data secure transmission model based on compressed sensing and digital watermarking technology. Wuhan University Journal of Natural Sciences 2014; 19(6): 505-511. DOI: 10.1007/s11859-014-1045-x.
[37] Zhang G, Kou L, Zhang L, Liu C, Da Q, Sun J. A new digital watermarking method for data integrity protection in the perception layer of IoT. Security and Communication Networks 2017; 2017: 3126010. DOI: 10.1155/2017/3126010.
[38] Kamel I, Juma H. Simplified watermarking scheme for sensor networks. International Journal of Internet Protocol Technology 2010; 5(1-2): 101-111. DOI: 10.1504/IJIPT.2010.032619.
[39] Shi X, Xiao D. A reversible watermarking authentication scheme for wireless sensor networks. Information Sciences 2013; 240: 173-183. DOI: 10.1016/j.ins.2013.03.031.
[40] Chong S, Skalka C, Vaughan JA. Self-identifying data for fair use. Journal of Data and Information Quality 2015; 5(3): 11. DOI: 10.1145/2687422.

Authors' information

Oleg Olegovich Evsutin (b. 1987) graduated from the Tomsk State University of Control Systems and Radioelectronics (TUSUR) in 2009, majoring in Complex Information Security of Computer Systems. He received his Candidate in Engineering (2012) degree from the Tomsk State University. He is the associate professor at the TUSUR's Security of Information Systems sub-department. His current research interests include information security, digital images processing, applications of cellular automata theory. E-mail: *eoo@keva.tusur.ru* .

Anna Sergeevna Kokurina (b. 1994) graduated from TUSUR in 2018, majoring in Information and Analytical Security Systems. She is the junior researcher at the TUSUR's Security of Information Systems sub-department. Her current research interests include information security, steganography. E-mail: *annakokurina94@yandex.ru* .

Roman Valeryevich Meshcheryakov (b. 1974) graduated from Altai State Technical University in 1997, majoring in Information Processing and Measurement Equipment and Technology. He received his Candidate in Engineering (2000) and Doctor in Engineering (2012) degrees. He is the chief researcher of the V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences. His current research interests include processing, analysis, synthesis of speech signals and texts, system analysis, information security, mathematical modeling. E-mail: *mrv@tusur.ru* .

Received August 11, 2018. The final version – December 17, 2018.

Дизайн: М.А. Вахе. Оформление и вёрстка: М.А. Вахе, Е.В. Семиколенных, С.В. Смагин.
Лит. редактор и корректор Ю.Н. Литвинова. Консультант по оформлению англоязычного блока М.И. Котляр.
E-mail: *ko@smr.ru*, *http://www.computeroptics.ru*

Подписано в печать 12.03.2019 г. Усл. печ. л. 17,9.
Заказ № 11/6. Тираж 207 экз. Печать офсетная. Формат 62x84 1/8.
Цена: 550 рублей / Price of 550 rubles (6+)

Редакция: Институт систем обработки изображений РАН – филиал ФНИЦ «Кристаллография и фотоника» РАН, (443010, г. Самара, ул. Молодогвардейская, 151)
Соучредители: Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский национальный исследовательский университет имени академика С.П. Королева» (443086, г. Самара, Московское шоссе, д.34),
Федеральное государственное учреждение «Федеральный научно-исследовательский центр «Кристаллография и фотоника» Российской академии наук» (117342, г. Москва, ул. Бутлерова, д 17А)
Отпечатано в типографии ООО «Предприятие «Новая техника» (443013 г. Самара, пр-кт. Карла Маркса, 24-76)