окружающей среды, планировке территорий, образовательных, разведывательных и военных целях. На спутниковых снимках отсутствуют знаки и обозначения объектов, поэтому есть необходимость в размещении на них служебной информации.

Использование стеганографических возможностей встраивания информации в картографические изображения позволит упростить работу с данными об определенном объекте исследования. Данные об объекте можно хранить непосредственно в самом изображении. При встраивании, исходное изображение можно разделить на слои и в каждый слой встроить определенную информацию. В этом случае, при извлечении некоторой информации, необходимости извлекать все, не будет.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: СОЛОН-Пресс, 2002.

2. Как карты передают географическую информацию [Электронный ресурс]/ArcGIS Recourses – 2010. – Режим доступа: http://resources.arcgis.com/ru/help/getting-started/articles/026n0000000q000000.htm.

УГРОЗЫ ТЕХНОЛОГИЙ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

С.Ю. Вашкевич, А.Е. Мишустина, Е.Е. Гачко, Т.С. Аубакирова

Особенностью развития современной сферы разработки мобильных и встроенных приложений становится использование наиболее перспективных технологий, из которых особо можно выделить технологию дополненной реальности (AR, augmented reality). Анализ рынка показал, что приложения, использующие AR-технологии, становятся популярны не только в сфере развлечений, но и получают множество вариантов практического применения.

При оценке рисков дополненной реальности в первую очередь обращают внимание на отвлекающие факторы. К примеру, слишком большое количество информации, находящейся в поле зрения водителя, может привести к фатальным последствиям. Менее вероятна угроза проникновения в системы дополненной реальности хакеров с последующим вторжением в частную жизнь, похищением цифровых данных и рисками физической безопасности. Можно подменить выходную информацию AR-систем, заставляя пользователя поверить, что сгенерированные компьютером объекты (например, поддельные дорожные знаки) реальны. Противоположный сценарий: так как приложениям дополненной реальности нужен доступ к реальным данным, собранным при помощи различных датчиков, вредоносные приложения могут похищать информацию о наблюдаемых объектах и местоположении пользователя.

В отчете 2016 Emerging Technology Domains Risk Survey [1] дополненная реальность названа одной из десяти технологических областей, которые в случае взлома могут привести к серьезным сбоям (в сфере безопасности, конфиденциальности, финансовой или операционной). Классические методы и средства повышения безопасности (например, шифрование данных, передаваемых по беспроводным каналам) позволяют защитить входные и выходные данные приложений. Но для этого необходимо иметь четкое представление об интеграции средств безопасности в сферу дополненной реальности.

Литература

1. 2016 Emerging Technology Domains Risk Survey [Электронный ресурс] / Software Engineering Institute. Carnegie Mellon Institute. – Режим доступа: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf. – Дата доступа: 18.05.2017.

ИСПОЛЬЗОВАНИЕ ВЕКТОРНОЙ ГРАФИКИ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ WEB-СИСТЕМ

О.Н. Виничук

Цифровое изображение – графическая форма представления данных, предназначенная для зрительного восприятия. Будучи закодированным с помощью особого алгоритма и записанным на носитель, этот массив данных становится файлом, который зачастую имеет достаточно большой размер. В современном процессе полиграфического производства все

иллюстрации и элементы оформления представлены цифровыми изображениями различных типов. Основной гипотезой, положенной в основу данной статьи, является возможность преобразования изображения в svg формат для возможности масштабирования изображения до любого размера без потери качества, возможность сокращения размера файла путем сжатия и обработки изображения. SVG-изображение – это набор графических операторов, описывающих формирование простых графических элементов, таких, как векторы, многоугольники, окружности, дуги. При выводе на матричные устройства векторная графика предварительно преобразуется в растровую графику, преобразование производится программными или аппаратными средствами современных видеокарт.Важным моментом является тот факт, что в браузере SVG-графика отрисовывается с помощью растровых механизмов. Поддержка полупрозрачностей в каждом слое, градиенты линейные, градиенты радиальные, визуальные эффекты (тени, отмывки, блестящие поверхности, текстуры, паттерны любой конструкции, символы любой сложности).

Избыточность данных является центральным понятием цифрового сжатия данных. Плюсом векторных изображений SVG является сравнительно небольшой размер файлов, их содержащих. Это делает удобной передачу векторных изображений по электронным каналам связи. Особое распространение векторные изображения получили в рекламной продукции благодаря возможности качественного полиграфического воспроизведения четких линий, ярких цветов, ровных заливок и геометрически правильных контуров. Использование SVG значительно упрощает реализацию деловой графики и делает вывод любой графической информации строгим и структурированным.

Литература

1. Электронный научный журнал «Медиаскоп» [Электронный ресурс] / Электронный научный журнал «Медиаскоп» – Режим доступа - http://www.mediascope.ru. – Дата доступа: 28.02.2017.

ВОПРОСЫ ПРИМЕНЕНИЯ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ

Г.А. Власова, Н.А. Козырев

Стремительное развитие Интернета и внедрение интернет-технологий во все сферы жизнедеятельности человека привело к появлению так называемого Интернета Вещей (Internet of Things, IoT). В настоящее время более 99% всех изготовленных микропроцессоров используется во встроенных системах и менее 1% - в традиционных компьютерах. IoT рассматривается комиссиями Европарламента и Совета Европы как основной путь развития информационных и интернет-технологий [1]. Подключение к сети Интернет десятков миллиардов новых устройств, которые ранее не рассматривались в качестве информационных, формирует новые требования к информационной безопасности, в том числе к криптографическим методам защиты.

Массовый характер применения и небольшие потоки передаваемых данных привели к необходимости использования алгоритмов малоресурсной или «легковесной криптографии» (lightweight cryptography, LWC) для реализации в устройствах, имеющих ограниченные вычислительные возможности. Как правило, к реализации малоресурсной криптографии предъявляются следующие требования: низкая потребляемая энергия; малые размеры микросхемы; обработка небольших потоков информации с приемлемым быстродействием; дешевизна устройств. При этом в отличие от объемов требуемых ресурсов, криптостойкость должна снижаться незначительно. Однако легко реализовать любые две из трех целей разработки: безопасность и экономичность, безопасность и производительность или стоимость и производительность, но очень трудно оптимизировать все три цели такой разработки одновременно [1]. Так, безопасность и высокое быстродействие можно реализовать параллельными методами вычислений, но при этом увеличивается стоимость устройства. Увеличение времени обработки позволяет, обеспечив требуемую криптостойкость, уменьшить размеры микросхемы, снижая соответственно производительность устройства. Увеличение криптостойкости за счет увеличения длины ключа приводит к уменьшению экономичности и быстродействия устройства. Таким образом, разработка устройств, реализующих алгоритмы