МОДУЛЬ ВНЕДРЕНИЯ ИНФОРМАЦИИ В ЗВУКОВЫЕ ФАЙЛЫ В ФОРМАТЕ MP3 НА ОСНОВЕ МЕТОДА ФАЗОВОГО КОДИРОВАНИЯ

Е.В. Бондарчук, И.А. Мурашко

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Существуют два основных направления в компьютерной стеганографии. Первое направление основано на цифровой обработке сигналов. Второе использует иные принципы.

Метод фазового кодирования, предлагающий использовать слабую чувствительность системы слуха человека к незначительным изменениям фазы сигнала, был предложен В. Бендером, Н. Моримото и др. Основная идея метода – фаза начального сегмента аудиосигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз. Это объясняется тем, что к разности фаз человеческое ухо более чувствительно. Фазовое кодирование, когда оно может быть применено, является одним из наиболее эффективных способов кодирования по критерию отношения сигнал-шум [1].

Фазовое кодирование включает в себя следующие шаги:

– разделяется оригинальный звуковой сигнал на более мелкие сегменты таким образом, чтобы их общая длина была равна длине сообщения;

– с помощью дискретного преобразования Фурье создается матрица фаз;

– вычисляется разность фаз между соседними сегментами;

– секретное сообщение встраивается только в фазу первого сегмента;

– с учетом разности фаз создается новая матрица фаз, используя новую фазу первого сегмента;

– звуковой сигнал восстанавливается путем применения обратного дискретного преобразования Фурье с использованием новой матрицы и исходной матрицы величин, после чего звуковые сегменты сцепляются.

Чтобы извлечь секретное сообщение из звукового файла получатель должен знать длину сегмента. После чего получатель с помощью дискретного преобразования Фурье может извлечь секретную информацию [2].

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев – М.: СОЛОН-ПРЕСС, 2009. – 265 с.

2. Нигматулин, Э.В. Обзор методов цифровой аудиостеганографии / Нигматуллин Э.В., Ковырзина К.С. // Электронный сборник статей по материалам XLII студенческой международной научно-практической конференции. Новосибирск, 31 мая 2016 г.: изд. АНС «СибАК». – 2016. – № 5 (41). – Новосибирск, 2016. – С. 118–124.

СТЕГАНОГРАФИЧЕСКОЕ ВСТРАИВАНИЕ СЛУЖЕБНОЙ ИНФОРМАЦИИ В КАРТОГРАФИЧЕСКИЕ ИЗОБРАЖЕНИЯ

Ю.В. Борохова

Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации. Задачу встраивания и выделения сообщений из другой информации выполняет стеганографическая система. Основными объектами стеганографии являются: контейнер – любая информация, предназначенная для сокрытия тайных сообщений; сообщение – это термин, используемый для общего названия передаваемой скрытой информации; стеганографический канал – канал передачи стегоконтейнера; ключ – секретный ключ, необходимый для сокрытия информации.

Картография – наука об исследовании, моделировании и отображении пространственного расположения, сочетания и взаимосвязи объектов, явлений природы и общества. В настоящее время картографическое производство опирается на материалы космических снимков.

Спутниковые изображения находят применение во многих отраслях деятельности – сельском хозяйстве, геологических и гидрологических исследованиях, лесоводстве, охране

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