Автоматизированное проектирование и программирование выполняется на основании составления компонент G_{kf} функционального графа G_{YF}, который сравнивается с контрольным графом G'_{YF}. Для каждой компоненты составляется исходный блок $|M_{фтм}|$ функционально-топологической матрицы смежности (рисунок 2, *а*).

В центральной части рисунка 2, *б* приводится контрольный граф как результат визуализации результатовии автоматизированного проектирования и программирования.

Из анализа графов, приведенных на рисунках 1 и 2, следует их изоморфизм, что является свидетельством корректного процесса выполненных проектных работ. В соответствии с этим сформированный программный продукт можно считать условно безопасным, который следует допускать к соответствующим испытаниям и прочим процедурам доказательства безопасности МПЦ.

Кроме этого, как показали исследования, применение графо-функциональных методов исходной интерпретации технологических объектов является более эффективным, по сравнению с графопараметрическими методами с позиции ресурсоемкости и влияния на показатели эксплуатационной надёжности систем ЖА. В частности, реализация новых методов позволяет сократить временные ресурсы на автоматизированное проектирование и программирование до четырех раз, увеличить глубино контроля устройств ЖА до двух раз, повысить эксплуатационную готовность систем ЖА до 18 % и сократить непродуктивный простой поездов до 16 %.

Таким образом, подтверждается целесообразность исследования и продолжения реализации его направлений.

УДК 625.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ПЕРЕДАЧИ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА НА ОСНОВЕ СТЕГАНОГРАФИИ

В. М. КОВАЛЕНКО, С. Н. БЕЛАН
Государственный университет инфраструктуры и технологий, г. Киев, Украина

Введение. В настоящее время развитие стеганографии вызвано распространением персональных компьютеров мультимедийных приложений и развитием информационных систем, а также сетей общего пользования. Современную стеганографию правильно было бы называть компьютерной или цифровой стеганографией, так как скрытые сообщения обычно встраиваются в данные, представленные в некотором цифровом (электронном) формате [1–3].

Постановка проблемы. Основной проблемой обеспечения безопасности информационных компьютерных систем является задача ограничения круга лиц, имеющих доступ к конкретной информации, и защиты ее от несанкционированного доступа. В связи с быстрым развитием мультимедийных технологий возникает все большая потребность в защите прав и интеллектуальной собственности, представленной в цифровом виде, так как возможна кража и модификация сообщения при передаче или представлении информации. Поэтому одним из наиболее эффективных видов защиты мультимедийной информации является цифровой стеганографический способ защиты сообщения, который можно использовать в железнодорожных мультимедийных сетях связи для защиты сообщений.

Цель работы. Повышение объема передающейся информации в мультимедийных сетях связи на железной дороге с помощью стеганографии на основе графических контейнеров.

Суть работы. Методы сокрытия информации в графических файлах базируются на модификации цифрового представления графических изображений, выступающих в роли контейнеров. В стеганографических системах в качестве контейнеров выступают оцифрованные изображения, так как они обладают свойствами, которые могут позволить произвести незаметное внедрение данных.

Суть метода замены наименее значащего бита Least Significant Bits (LSB) заключается в сокрытии информации путем изменения последних битов изображения [4]. Цифровые изображения являют собой матрицу пикселей. Цвет и яркость каждого пикселя представляется двоичным кодом. Младший значащий бит кода каждого пикселя изображения несет в себе меньше всего информации. Человек, обычно, не способен заметить изменение в этом бите, для него он является шумом и

его можно использовать для встраивания информации. В изображение формата BMP хранится матрица значений оттенков для каждой точки хранимого изображения. Если каждый из компонентов пространства RGB (каналов цвета) хранится в одном байте, матрица может принимать значения от 0 до 255 включительно, что соответствует 24-битной глубине цвета. Особенностью зрения человека является то, что оно слабо различает незначительные колебания цвета. Для 24-битного цвета изменение в каждом из трех каналов одного наименее значимого бита (крайнего правого) приводит к изменению менее чем на 1 % интенсивности данной точки, что позволяет изменять их незаметно для зрения по своему усмотрению.

Принцип работы стеганографического метода защиты сообщений заключается в следующем. Пусть, имеется 24-битное изображение в градациях серого. Пиксели кодируются тремя байтами, и в них расположены значения каналов RGB. Изменяя наименее значащий бит, мы меняем значение байта на единицу. Такие градации, мало того, что незаметны для человека, они могут вообще не отобразиться при использовании низкокачественных устройств вывода. Применение стеганографического метода LSB в среднем требует, чтобы только половина бит изображения-контейнера были изменены.

Существует небольшая модификация представленной методики стеганографии, позволяющая использовать для встраивания сообщения в два или более младших бит на байт. Это увеличивает объем скрытой информации в объекте-контейнере, но скрытность сильно снижается, что облегчает обнаружение результатов осаждения информации.

Суть модификации. Определённый текст в соответствии с кодировкой ASCII преобразуется в числовой вид, символы заменяются на соответствующие числовые коды. На следующем шаге с помощью секретного ключа определяется место осаждения информации. Замена значений трех составляющих цвета (красный, зелёный, синий) будет осуществляться не в двоичном, как в классическом LSB методе, а в десятичном виде. Замене подлежат наименее значимые (правые) цифры значений соответствующего цветового канала. При использовании символов кириллицы (ASCII коды >127) потребуется задействовать и зеленую составляющую пикселя, или же как альтернатива увеличить количество задействованных в процессе осаждения пикселей. При замене в красную составляющую будет записываться первая цифра двоичного кода символа, а в синюю составляющую вторая цифра двоичного кода символа. Такой механизм будет изменять не один младший бит, как это было бы в классическом методе LSB, а целую группу бит, причем необязательно начиная с младшего разряда. Но при этом все равно будет достигаться незначительное изменение цвета пикселя, в то же время, при применении данного варианта будет улучшаться такая характеристика, как максимально возможное количество информации в графическом контейнере изображения.

Изображения, при использовании данного программного средства, можно сохранять в любом графическом формате, но при этом не предусматривается использование графического формата jpg со сжатием. В формате jpg приходят операции, что в свою очередь приводят к замене группы значений на усредненное, тем самым повреждая информацию, что была кодирована до этого.

В работе решается задача внедрения скрытой информации в шумы изображения. Цифровой шум является дефектом изображения, который вносят фотосенсоры и электроника устройств, которые их используют, из-за несовершенства технологий и фотонной природы света. Цифровой шум появляется на изображении в виде наложенной маски из пикселей случайных цветов и яркости. На большинстве цифровых камер шум имеет визуально более крупные зерна, чем пиксели на изображении. Это побочный эффект для алгоритма получения полноцветного изображения. Цифровой шум менее заметен в трех матричных системах или матрицах без фильтра. В цветном изображении шум может иметь разную интенсивность в зависимости от каналов изображения, что визуально его окрашивает. Некоторые изображения (фотографии) имеют большое количество шумов, которые можно использовать с пользой в данной модификации.

В работе внедрялись биты секретного сообщения до четырех младших бит, что не приводит к искажениям визуальной картины. Кроме младших разрядов кодов всех пикселей дополнительно встраиваются еще до четырех бит в коды пикселей шума, что увеличивает объем передаваемого сообщения в контейнере фиксированной длины. Этот дополнительный объем зависит от количества пикселей, принадлежащих шуму изображения.

Заключение. Из ключевых принципов при построении стеганографических систем можно выделить визуальную неразличимость заполненного и незаполненного контейнеров, а также аутентичность и целостность секретной информации. Изменение количества заменяемых бит позволяет варьировать пропускную способность стеганографической системы и существует необходимость исследования возможности использования старших бит для встраивания информации. Подробно описан метод стеганографического сокрытия данных, проанализированы некоторые его свойства (например, максимальная емкость контейнера). В качестве достоинств данного метода можно выделить, что размер файла-контейнера становится неизменным, при замене одного бита в канале синего цвета внедрение невозможно заметить визуально.

Список литературы

1 **Bennett, K.** Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text / K. Bennett. – Purdue Univ., CERIAS Tech. Rep. – 2004.

2 **Конахович, Г. Ф.** Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

3 **Urbanovich, N.** The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // New Electrical and Electronic Technologies and their Industrial Implementation. – 2011. – P. 147–148.

4 **Albdour, N.** Selection Image Points Method for Steganography Protection of Information / N. Albdour // WSEAS Transactions on signal processing. – 2018. – Vol. 14. – P. 151–159.

УДК 656.25 (078.5)

БЕЗОПАСНОСТЬ АППАРАТУРЫ СИСТЕМ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ ПРИ ВОЗДЕЙСТВИИ ЭЛЕКТРОМАГНИТНЫХ ПОМЕХ

Д. В. КОМНАТНЫЙ

Гомельский государственный технический университет им. П. О. Сухого, Республика Беларусь

На современном этапе развития систем железнодорожной автоматики и телемеханики (СЖАТ) происходит не просто широкое внедрение микропроцессорных и микроэлектронных систем, но переход к новым концепциям разработки и эксплуатации систем управления движением поездов – цифровизации и интеллектуализации. Это объясняется необходимостью на новом уровне решить две основные задачи функционирования железнодорожного транспорта: обеспечение требуемой провозной способности и высокого уровня безопасности движения поездов. Наиболее эффективным путем решения этих задач является создание комплексной системы управления и обеспечения безопасности движения поездов. В современных условиях повышение безопасности движения требует не только развития традиционных систем ЖАТ, но и привлечения дополнительных ресурсов на базе информационных технологий и цифровых систем. Таким образом, на базе систем СЦБ организуется система обеспечения безопасности движения, а на базе АСУ – система управления процессами перевозок. Взаимодействуя между собой, эти системы образуют комплексную систему управления, кроме того, независимо они выходят на региональный уровень управления. Следовательно, система управления процессами перевозок в настоящее время является единым комплексом, основанным на единой вычислительной среде и единой цифровой сети. В ней образуют три контура безопасности. Первый – централизованный, он заключается в централизации управления маршрутами и координатного управления в диспетчерском центре управления. Второй – децентрализованный, его образуют системы СЦБ и технической диагностики. Третий – бортовой, в составе которого имеются системы АЛС и автоведения.

Вместе с тем возрастает чувствительность элементной базы вычислительных комплексов к электромагнитным помехам и воздействиям. Это объясняется увеличением степени интеграции полупроводниковых изделий, снижением энергии рабочих сигналов этих изделий, увеличением плотности монтажа, усложнением схемотехнических решений.

Число возможных видов электромагнитных воздействий также увеличилось. В том числе появилась техническая возможность создания сверхширокополосных импульсов электромагнитного поля для преднамеренного воздействия этими импульсами на микроэлектронные технические средства (ТС) с целью создания большого потока сбоев в этих средствах или вывода их из строя. Объектами воздействия электромагнитными импульсами преднамеренного воздействия (ЭИПВ) может оказаться и аппаратура современных систем управления процессами перевозок железнодорожных