АЛГОРИТМ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОСИГНАЛИЗАЦИИ МОБИЛЬНЫХ ОБЪЕКТОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дубина С. С. Чернецкий А. М.

Сечко Г. В. – канд. техн. наук, доцент

Решается задача защиты информации в микроконтроллерах автосигнализации мобильных объектов, причём под защитой понимается противодействие нарушению целостности (несанкционированному изменению, искажению, уничтожению информации) и противодействие считыванию

Современная автосигнализация мобильных объектов, и в первую очередь транспортных средств, реализуется на микроконтроллерах. В каждом микроконтроллере заложена своя программа, в соответствии с которой контроллер управляет каким-либо устройством, выдавая управляющие сигналы. На разработку данного программного обеспечения производители тратят большие средства и время. В этих условиях актуальной является задача защиты информации в микроконтроллерах автосигнализации мобильных объектов, причём под защитой понимается противодействие нарушению целостности (несанкционированному изменению, искажению, уничтожению информации) [1] и противодействие считыванию. Поскольку устройства автосигнализации используют радиоканал передачи данных для взаимодействия между центральным блоком и пультом дистанционного управления, то параллельно с защитой необходимо повысить помехоустойчивости канала связи между данными устройствами.

На современном рынке существует три вида автосигнализаций: статические, динамические и диалоговые. Так как основную долю рынка занимают динамические автосигнализации, то было принято решение защищать информацию именно в них. Для понимания сути работы алгоритма введем следующие понятия: протокол передачи данных, посылка, сообщение. Сигнал в радиоэфир передается по определенному правилу. В общем случае протокол передачи данных состоит из преамбулы (специфический набор данных дающий понять принимаемому устройству, что принимаемая информация есть искомая), и информационной части (информация, которая представляет команду для устройства управления). Посылка представляет собой команду, передаваемую устройству управления автосигнализацией. Сообщение – это совокупность посылок (как минимум одна), которые идентичны друг другу. Суть алгоритма перехвата такова, что после подачи в радиоэфир сигнала, предназначенного для управления автосигнализацией, устройство перехвата, анализируя передаваемый сигнал, выдает в эфир радиопомеху, которая ставится в определенном месте информационной части посылки, и искажает данную команду [3]. Само устройство перехвата в данный момент времени запоминает неискаженную часть посылки. Данное действие не позволяет устройству управления автосигнализацией воспринимать передаваемую команду адекватно. Так как команда (посылка) в радиоэфир передается неоднократно, то это позволяет устройству перехвата одновременно принимать передающуюся посылку, выставлять помеху и запоминать искаженную команду, однако помеха ставится в месте, отличном от предыдущего, что даёт возможность устройству перехвата восстановить истинную команду путем сложения неискаженных частей.

Предложенный алгоритм учитывает очистку передаваемых автосигнализацией сигналов от случайных помех в радиоэфире, возникающих вблизи крупных промышленных объектов, которых в густонаселенных городах достаточно много.

Существует необходимость защиты более современных видов сигнализаций – диалоговых. Преимущество данных сигнализаций заключается в том, что и устройство дистанционного управления и блок управления автосигнализацией имеют известный только им ключ шифрования [2], а также существует обратная связь между данными устройствами управления (подтверждение принятой / отправленной команды). Однако благодаря современным технологиям считывания информации с кристалла микроконтроллера, ключи шифрования становятся известны злоумышленникам, что позволяет взламывать защищенный канал передачи данных путем перехвата радиосигнала и его анализа без необходимости постановки помех. Ставится задача разработать алгоритм «прыгающего» диалогового кода. Суть метода сводится к тому, что по псевдослучайному закону будут меняться правила (протокол) передачи информации. Передаваемая команда будет передаваться по частям, а каждая часть команды – по своему протоколу, который каждый раз будет меняться, а также будет максимально соответствовать различным протоколам передачи информации используемых в автосигнализация различных производителей. Данный способ позволит надежно защитить канал передачи информации, т.к. на данный момент все автосигнализации используют протоколы передачи данных позволяющие их легко идентифицировать в эфире среде им подобных.

Список использованных источников:

1. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» // Нац. реестр правовых актов Респ. Беларусь. – № 2/1552 (зарегистрировано 17 ноября 2008 г.).

2. Бабаш А.В., Шанкин Г.П. Криптография / Учебное пособие., 2007. – 512 с.
3. Карпушкин, Э. М. Радиосистемы передачи информации / Уч. метод. пособие для студентов учреждений, обеспечивающих получение высшего образования по спец. "Радиоэлектронные системы". – Минск: БГУИР, 2008. – 62 с.

СПОСОБ СЖАТИЯ ТЕРМИНАЛЬНЫХ ИЗОБРАЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Клепацкий В. И.

Лашкевич Е. М. – м-р техн. наук, ассистент

Ставится задача уменьшения объема передаваемых данных при передаче изображения удаленного компьютера по каналам связи в режиме реального времени. Проведен анализ существующих алгоритмов сжатия, на основе которого обоснована необходимость применения предложенного комплексного способа, главным достоинством которого является невысокая нагрузка на канал связи.

Одним из типов видеоданных, необходимость сжимать который существует в реальном времени, является видео, происходящее на экране пользователя и передаваемое на экран удаленного компьютера. На сегодняшний день чаще всего это видео высокого разрешения, для которого требуется канал с высокой пропускной способностью, которой во многих случаях недостаточно. В связи с этим возникает задача минимизировать объем данных, передаваемых по сети для управления удаленным компьютером.

Существуют технологии, позволяющие на порядки сжимать изображение (фрактальное сжатие и др.), но требовательные к быстродействию, что не удовлетворит условиям передачи изображения в реальном времени.

В терминальном режиме работы пользователь чаще всего работает с базами данных или документами, поэтому основные изменения изображения сосредоточены вокруг курсора, и глобально изображение на экране меняется нечасто. Этим можно воспользоваться для уменьшения количества сетевого трафика.

На сегодняшний день существует несколько программных продуктов, позволяющих передавать изображение удаленного компьютера (Microsoft RDP, Citrix ICA, Remote Administrator, Team Viewer и др.), и использующих различные алгоритмы. Общие алгоритмы сжатия видео описаны в [3]. Исходя из изложенных в учебном пособии сведений, можно сделать вывод, что для сжатия терминального видео наиболее подходящими являются 2 алгоритма: попиксельное и поблоковое сравнение кадров, т.к. кадры похожи между собой и сравнение необходимо осуществлять в реальном времени.

В [1] используется алгоритм, основанный на попиксельном сравнении изображений. Каждый десятый ключевой кадр кодируется и передается независимо. Для каждого промежуточного кадра записываются номера строк и столбцов, в которых есть изменившиеся пиксели относительно ключевого кадра, а затем – цвета пикселей, находящиеся на пересечении этих строк и столбцов. Цвета пикселей, находящиеся на пересечении этих строк и столбцов образуют изображение меньшего размера, которое можно сжимать так же, как и ключевой кадр. Остальную часть промежуточных кадров можно восстановить по ключевому кадру. Таким образом, получается алгоритм сжатия без потери информации с линейной трудоемкостью. Входные данные для этого алгоритма – 2 изображения, над которыми выполняется попиксельная операция xor. Выходные данные – массив, количество элементов которого равно количеству пикселей в исходном изображении. Каждый элемент массива является индикатором равенства или неравенства пикселей ключевого и анализируемого изображения.

Алгоритм, основанный на поблоковом сравнении изображений, используется TightVNC [2]. Изображение делится на небольшие неперекрывающиеся квадратные области, называемые ранговыми блоками. По сути, разбивается на пронумерованные квадраты. Определяются номера блоков, в которых есть хотя бы один изменившийся пиксель относительно соответствующего блока ключевого кадра. Изображение меньшего размера, составленное из изменившихся блоков пикселей можно сжимать теми же алгоритмами, что и ключевой кадр. При увеличении размера блока уменьшаются накладные расходы, связанные с хранением номеров изменившихся блоков, но вместе с тем уменьшается и точность определения изменившейся области. Экспериментальным путем установлено, что при размере блока 8*8 пикселей достигается максимальная степень сжатия с учетом количества передаваемых номеров блоков.

Оба этих алгоритма приблизительно одинаковы по скорости работы. Алгоритм, основанный на попиксельном сравнении, оказывается быстрее при вводе пользователем текста или при сворачивании\разворачивании окна. Алгоритм, основанный на поблоковом сравнении демонстрирует лучшие результаты при скроллинге и перемещении окна на некоторое расстояние, близкое к диагональному. Ни один из этих алгоритмов не является безусловно лучшим по степени сжатия.

Для усовершенствования рассмотренных алгоритмов предлагается следующий способ:

Отказаться от ключевого кадра и каждый раз в качестве ключевого использовать предыдущий кадр, ведь он все равно уже отрисован на экране, т.е. полностью передавать только самый первый кадр:

FRAME1= First Bitmap Image;

Массив отличий каждого следующего кадра от предыдущего получаем по формуле