ШИФРОВАНИЕ, СЖАТИЕ И МАСШТАБИРОВАНИЕ ИЗОБРАЖЕНИЙ В ТЕЛЕМЕТРИЧЕСКИХ СИСТЕМАХ

Тарасюк Е. В., Бурак Д. Л.
Кафедра систем управления, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: tarasiuk-ev@bsuir.by, venox771@gmail.com

В настоящее время широко распространена передача цифровых изображений по каналам связи. Зачастую происходит перехват и копирования таких изображений, что приводит к постоянно возрастающему числу нарушений авторских прав на графические работы, в связи с незаконным использованием этих работ, в частности, путем их несанкционированного размещения в интернет-галереях. Таким образом, актуальной является проблема защиты цифровых изображений.

Введение

В связи с тем, что передаваемая информация в телеметрических систем несет частный, или государственный характер, возникает необходимость в точной, секретной и эффективной передачи сигналов, а в частности ТВ – изображений по каналам связи. Многие телеметрические системы имеют несколько модулей (контролируемых пунктов) передачи данных оператору (пункту управления). Каждый модуль в процессе запроса оператора будет отправлять на пункт управления ТВ – изображение, в целях обеспечения безопасной передачи сигнала он будет подвергаться процессу шифрования, шифратором ГРИМ – ВИДЕО.

I. Шифрование изображений

На рисунке 1 представлена блок - схема устройства шифратора.

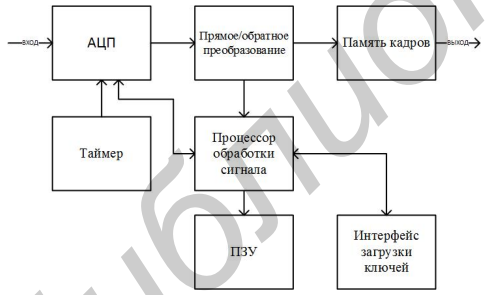

Рис. 1 – блок-схема шифратора

Шифратор имеет низкочастотный вход/выход видео. Техническая идея состоит в следующем. На вход устройства поступает низкочастотный-видеосигнал. Видеоинформация оцифровывается и записывается в видеопамять устройства. Так как стандартный телевизионный сигнал состоит из строк, образующих поля, то для передачи служебной информации используются первые 22 строки каждого телевизионного поля (пустые). Строки перемешиваются в полукадре методом перестановки. Зашифрованная таким образом видеоинформация и является выходом видеокодека. Восстанавливающее устройство проводит обратное преобразование. Закон перестановки строк и пикселов в каждом полукадре меняется.

Используемый в грим-видео кодеке метод блочного шифрования, а в частности метод перестановки состоит в следующем, что исходная информация делится на блоки, в каждом из которых выполняется перестановка элементов. Стандартный телевизионный сигнал уже поделен на блоки. Простейшим примером перестановки является запись исходных данных по строкам некоторой матрицы, а затем чтение данных по ее столбцам. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Таким образом, для матрицы размером NxN число возможных перестановок составит N!xN!. Перестановка строк наиболее приемлема для сохранения качества восстановленного изображения. Для реального изображения перестановки строк может быть вполне достаточно, чтобы скрыть сюжет до неузнаваемости.

Блочное шифрование работает с блоками заранее определенной длины, не меняющимися в процессе шифрования. Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком. Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока. Например, при блочном шифровании с 16-байтовыми блоками исходное сообщение длиной в 38 байтов фрагментируется на два блока длиной по 16 байтов и 1 блок длиной 6 байтов, который затем дополняется 10 байтами пустых символов до длины нормального блока. Данный вид шифрации применяется только для видеоизображения, передаваемого по одному из каналов связи, следующему на пункт управления.

Библиотека БГУИР

II. Усовершенствование алгоритма сжатия, масштабирования и скорости передачи ТВ-изображения по радиоканалу

Усовершенствован алгоритм сжатия и масштабирования картины и программное обеспечение для увеличения скорости передачи по радиоканалу цифрового телевизионного изображения ТВ-канала ИК-ТВ-обнаружителя. Для этих целей в команду получения изображения, подаваемую с ЦПО на отдельный АПК, введён признак фильтрации полученного изображения: 100, 66 и 50 процентов. Полное изображение представляет собой картинку в стандарте PAL с разрешением 768x576 пикселей, из которой формируется соответствующий BMP-файл, впоследствии подвергающийся процессу сжатия, основанном на принципе дифференциального косинусного преобразования, в результате чего по радиоканалу передаётся JPEG-файл размером порядка 20 кБ. Схема алгоритма сжатия, масштабирования и передачи по радиоканалу приведен на рисунке 2.

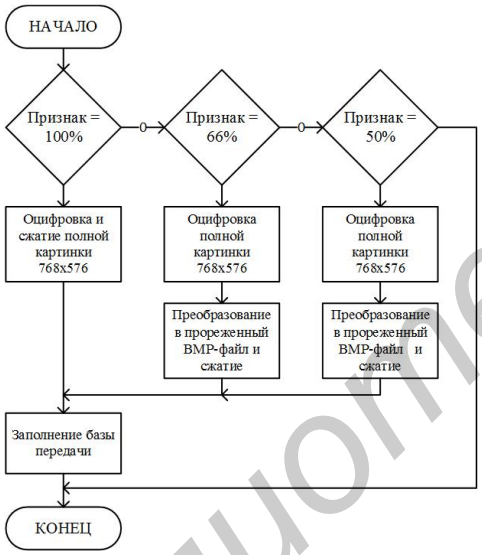

Рис. 2 – Схема алгоритма сжатия, масштабирования и передачи по радиоканалу

В новом алгоритме и реализованном на его основе программном обеспечении происходит дальнейшая обработка большой 100 процентной картинки в зависимости от признака в команде. Она заключается в прорежении пикселов исходного BMP-файла. В частности, для 50 процентной картинки информационной считается каждая третья строка изображения, а для 66 - через строку выбрасывается каждый третий пиксель. Затем из данного массива формируется новый BMP-файл, который подвергается процедуре сжатия, в результате чего его размер уменьшается втрое, что позволяет повысить скорость его передачи на ЦПО. На ЦПО, в свою очередь, в зависимости от признака фильтрации происходит масштабирование полученного изображения на экране монитора, которое представляет собой автоматическое отображение картинки в окне большего или меньшего размера.

III. Заключение

Целостность данных включает такие области, как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных. Активная проверка помогает удостовериться в том, что установленная политика в области безопасности соблюдается, и отследить все аномальные случаи и попытки несанкционированного доступа.

1. Antsipov G.v. an automated remote infra-red and television system of forest fire and ecological monitoring. International forest fire news №23 (December, 2000), p.p. 92-96.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Под ред. А. Б. Васильева. — М.: Триумф, 2002. — 816 с.
3. К. Шеннон. Теория связи в секретных системах // Работы по теории информации и кибернетике / Перевод С. Карпова. — М.: ИЛ, 1963. — С. 243-322. — 830 с.
4. Дж. Миано. Форматы и алгоритмы сжатия изображений в действии. - М.: Издательство Триумф, 2003. - 336 с.
5. Ватолин Д., Ракушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. - М.: ДИАЛОГ-МИФИ, 2003. - 384 с.

Библиотека БГУИР