УДК 621.391.1

О ЗАЩИТЕ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ПРИ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

И. Л. Ерош,
доктор техн. наук, профессор
А. М. Сергеев,
ассистент
Г. П. Филатов,
соискатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассматриваются особенности изображений и требования к их преобразованию для защиты от несанкционированного использования при передаче по каналам связи.

We investigate the requirements on the transformation of images for protection against unauthorized access during their transfer via communication channels.

Введение

При построении систем слежения за статичными или движущимися объектами часто требуется передавать изображения этих объектов на различные расстояния. В качестве коммуникационных сред используются каналы связи стандартов GSM, CDMA, инфраструктура Internet и др. Использование перечисленных коммуникационных сред для информационного взаимодействия между устройствами позволяет строить глобально распределенные информационно-управляющие системы [1].

При этом взаимодействие в системе требуется организовать таким образом, чтобы передаваемые изображения, часто составляющие коммерческую или служебную тайну, невозможно было перехватить или, тем более, подменить.

Требования к средствам защиты

Ввиду того, что актуальность передаваемых изображений может составлять единицы или десятки часов, а передающие устройства в таких системах реализуются в виде встраиваемых автономных модулей с ограниченным вычислительным ресурсом, система защиты может быть не очень сложной, что позволяет использовать классические методы с небольшой длиной ключа или разрабатывать простые методы, обеспечивающие высокую скорость формирования защищенного изображения.

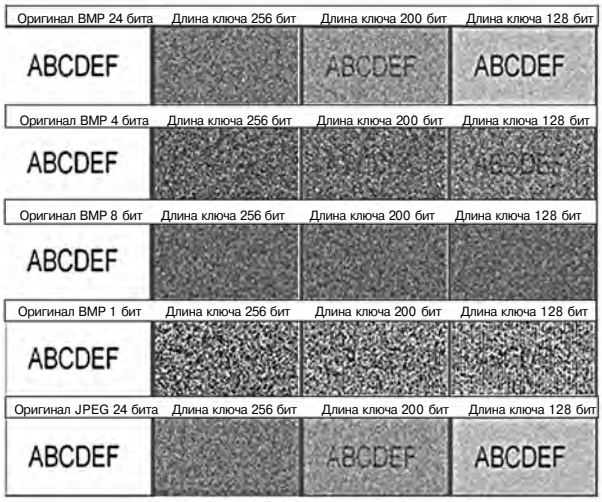
Эксперименты с преобразованием изображений с использованием различных известных криптографических систем [2] при небольшой длине ключа показали, что часто после выполнения процедуры преобразования результирующие данные значительно отличаются от исходных, но на визуализированном защищенном изображении остаются контуры, характерные светлые или темные области, по которым возможно узнавание передаваемого изображения, а в ряде случаев – значительное восстановление с использованием программных систем типа Adobe Photoshop®.

Опыт создания программного обеспечения для улучшения качества видеоизображений, полученных в сложных условиях (расфокусировка, плохая освещенность и др.), показал, что имеется реальная возможность значительного восстановления исходного изображения с применением к защищенному визуализированному изображению методов гамма-коррекции, эквализации гистограммы или соляризации [3], обеспечивающих увеличение визуальной различимости фрагментов изображений.

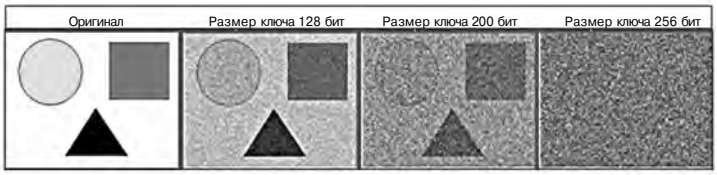
Учитывая тот факт, что человеческое зрение на сегодня является лучшей системой распознавания образов, цифровое представление защищенных изображений и их визуализация на экране дисплея требуют особых подходов при разработке методов защиты и предварительной обработки изображений.

Основное внимание, очевидно, должно быть уделено разрушению не цифровых данных, представляющих собой в электронном виде изображение, а непосредственно самого изображения, его характерных признаков.

а)



б)



Разрешение 304×255 пикселей, цветность 24 бита

в)

Разрешение 1200×1600 пикселей, цветность 24 бита

■ ***Рис. 1.*** *Пример использования поточного шифра RC4 для изображения текста* (*а*)*, разноцветного рисунка* (*б*) *и фотографии* (*в*)

Пример использования RC4 для защиты различных типов изображений приведен на рис. 1.

Поскольку изображения — уникальные цифровые данные, воспринимаемые зрительно и ассоциативно после обработки соответствующим кодеком, то в связи с этим для их (как особого рода информации) преобразования сформулируем особые требования:

— пиксели с одинаковой яркостью должны преобразовываться в пиксели с разной яркостью, что обеспечит разрушение контуров изображения;

— характерные области на исходном изображении должны попадать в различные области в преобразованном изображении.

Для устранения контуров на преобразованном изображении можно обеспечить перемешивание фрагментов пикселей яркости. Для этого коды пикселей выстраиваются в единую битовую строку, после чего нарезаются новые фрагменты, не кратные исходным. Так, например, если пиксель представляется S-битовым словом и число элементов разрешения равно $K \times N$, то результирующая строка одного кадра (изображения) содержит $S \times K \times N$ бит. Выбрав размер нового пикселя в P бит, получим число новых пикселей

$$M = S \times K \times N / P.$$

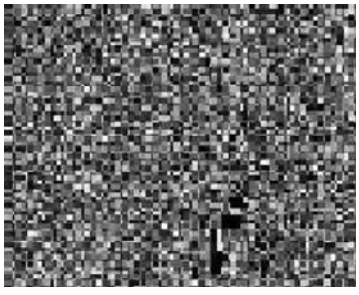
В работе [4] предлагается использовать для формирования защищенных изображений матричное преобразование. Для этого выполняется умножение неособенных матриц над полем GF(2) на вектор-столбцы фрагментов изображений.

В качестве базовых операций матричных преобразований при этом используются не арифметические, а логические операции. Формирование защищенных изображений на передающей стороне распределенной системы и обратное преобразование изображений на приемной стороне выполняются очень быстро, поскольку не требуют значительных вычислительных затрат [4].

На рис. 2 представлен результат преобразования исходного цветного изображения в защищенное с реализацией сформулированных выше требований и использованием матричного преобразо-

а)

б)



■ ***Рис. 2.*** *Защита изображения матричным преобразованием: а — исходное изображение; б — защищенное изображение*

вания. Следует подчеркнуть, что контуры и характерные области на преобразованном изображении полностью отсутствуют.

Заключение

Эксперименты показали, что выполнение сформулированных выше требований в процессе процедуры преобразования изображения неособенными матрицами над полем GF(2) обеспечивает полное разрушение изображения и его характерных признаков.

При необходимости усиление защиты передаваемых двоичных данных, а также электронного представления изображений может быть обеспечено за счет двойного и тройного преобразований, выполняемых уже над защищенными ранее изображениями по известной вычислительной процедуре [4].

Как известно, выполнение матричных преобразований наиболее эффективно на параллельных структурах. При этом предпочтительна реализация преобразований на параллельной структуре, организованной на программируемой логике в виде специализированного вычислителя требуемой конфигурации [5], что позволяет полностью сохранить передающее устройство в классе автономных встраиваемых устройств.

Литература

1. **Сергеев М. Б., Чудиновский Ю. Г.** IP-сеть как основа построения распределенных информационно-управляющих систем // Информационно-управляющие системы для подвижных объектов. СПб.: Политехника, 2002. С. 33–42.
2. **Bruce Schneier** Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley and Sons, Inc., New York, NY, USA; Second edn.; 1996.
3. **Сергеев М. Б., Соловьев Н. В., Стадник А. И.** Методы повышения контрастности растровых изображений для систем цифровой обработки видеоинформации // Информационно-управляющие системы. 2007. № 1(26). С. 2–7.
4. **Ерош И. Л., Сергеев М. Б.** Скоростное шифрование разнородных сообщений // Вопросы передачи и защиты информации: Сб. ст. / СПбГУАП. СПб., 2006. С. 133–155.
5. **Бубликов А. В., Ерош И. Л., Сергеев М. Б.** Особенности использования булевых функций для организации криптографических преобразований потоковой информации // Информационно-управляющие системы. 2003. № 6. С. 54–57.