ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ВИДЕОДАННЫХ С ИСПОЛЬЗОВАНИЕМ РЕШЕНИЯ ЗАДАЧИ ПРОВЕРКИ ИЗОМОРФИЗМА ГРАФОВ

Р.Т. Файзуллин, Г.С. Ржаницын
Омский Государственный Университет им. Ф.М. Достоевского

Рассматривается применение различных подходов к защите видеоданных. Приведено исследование защищенности подходов, связанных с перестановкой строк и столбцов кадров видеоизображений. Предложено построение криптосистемы, использующее связь с решением задачи проверки изоморфизма графов

Надежная защита при хранении и передаче цифровых видеоизображений требуется повсеместно, где предъявляются требования к конфиденциальности, или они представляют собой коммерческую ценность - системы платного телевидения, видео по запросу, конфиденциальные видео конференции, системах медицинской визуализации и тому подобных. Хорошо развитая современная криптография не может стать идеальным решением этой задачи. Как известно, с 1970-х годов было разработано множество достаточно безупречных систем шифрования, которые успешно широко применялись, например системы DES, IDEA, RSA. Но большинство традиционных систем шифрования не могут напрямую использоваться для кодирования цифрового видео в системах реального времени, поскольку их скорость шифрования не достаточно высока, особенно когда алгоритмы реализуются ПО. К тому же, существование различных алгоритмов сжатия в цифровых видео системах делает довольно сложным включение этапа шифрования во всю систему в целом. Таким образом, для защиты содержания цифровых видеоизображений требуются особые системы шифрования. За последние годы было предложено множество различных алгоритмов шифрования в качестве возможного решения проблемы защиты цифровых изображений и видео. Некоторые из них являются объединенной схемой “сжатие-шифрование”, которые специально разработаны для обеспечения надежной защиты MPEG видео, которое в свою очередь привлекает наибольшее внимание в силу заметного преобладания на рынке потребителей электроники. Но они не обеспечивают гарантированной защищенности контента. Определенные успехи наблюдаются в квантовой криптографии, но пока эта технология еще только развивается.

Постановка задачи следующая. По открытому каналу связи от источника (абонента A) к приёмнику (абоненту B) передаётся видеоизображение. Необходимо шифровать видеоизображение, чтобы избежать несанкционированного доступа к передаваемой видеоинформации при подключении третьих лиц (противника M) к каналу связи. При этом необходимо реализовать шифрование так, чтобы ключ к шифру динамически менялся при передаче кадров от источника к приёмнику без передачи в явном виде по каналу связи ключа к шифру.

Для того, чтобы только абонент B (приёмник) мог иметь доступ к посланному изображению, абонент A (источник) преобразует каждый кадр p видеоизображения с помощью функции шифрования E_{AB} и ключа k_{AB} в кадр c зашифрованного видеоизображения:

$$c = E_{AB}(p),$$

который и поступает в канал связи. Приёмник восстанавливает исходный кадр видеоизображения с помощью функции дешифрования D_{AB} и того же секретного ключа k_{AB}:

$$p = D_{AB}(c).$$

Цель противника M – воспрепятствовать осуществлению намерений законных участников информационного обмена (абонентов A и B). Будем считать, что задача противника M – перехватить зашифрованные сообщения и дешифровать их. Дешифрование переданного по каналу связи видеоизображения противником M возможно в случае вычисления им ключа k_{AB}, либо в случае нахождения алгоритма, функционально эквивалентного D_{AB} и не требующего знания k_{AB}.

Краткая характеристика и недостатки используемых на практике методов защиты видеоданных

Цифровое телевидение во многом схоже с широковещательным. Это беспроводная система доставки телевизионного сигнала непосредственно в дом к пользователю. И широковещательные, и спутниковые станции передают информацию, используя радиосигнал. В Москве и Московской области можно принимать сигналы с более, чем 10 спутников. Например, (наиболее популярные) Hot Bird (более 560 каналов), Sirius (около 90 каналов), Astra (более 300) и Eutelsat W4 (НТВ Плюс и еще около 10 каналов).

Радиосигнал со спутника, в принципе, может быть принят любым желающим в территории вещания спутника независимо от желания передающей стороны. Однако в большинстве случаев телекомпания - владелец программы заинтересована в пресечении нелегального приема, например, при передаче программ платного телевидения, деловых телеконференций, или в ограничении территории, на которой можно принимать данную программу по условиям авторского права. Самым популярным способом ограничения доступа является засекречивание передаваемых программ (шифрование сигнала) таким образом, чтобы сделать прием невозможным без специального декодера, предоставляемого про-

вайдером. На практике используется восемь систем кодирования для PAL/SECAM, четыре для NTSC и шесть для сигнала MAC. К примеру , Viaccess, Irdeto, Betacrypt, Nagravision. И, чтобы смотреть любимую программу придется приобрести карточки, ресивер и вносить абонентскую плату.

Метод случайной перестановки коэффициентов ДКП [13]

Данный метод заключается в использовании преобразования блока коэффициентов ДКП 8 х 8 в вектор 1 х 64 в случайном порядке вместо преобразования в «зигзагообразном» порядке. Ключом алгоритма является матрица, представляющая собой набор номеров коэффициентов, задающий последовательность выбора коэффициентов из блока при формировании вектора. Данная матрица формируется с помощью случайных перестановок из исходной матрицы, задающей зигзагообразный порядок выбора коэффициентов. Преимуществом такого метода является высокая скорость шифрования.

Данный алгоритм неустойчив к криптоатакам с использованием как открытого текста, так и только шифротекста. Если криптоаналитик имеет открытый текст и соответствующий ему закрытый шифротекст, то порядок перестановки можно найти, и криптоаналитик получает доступ к любому потоку, зашифрованному с использованием данной перестановки. При наличии только шифротекста вскрытие также возможно, поскольку коэффициенты, как правило, сосредоточены в верхнем левом углу матрицы, и, зная это, можно найти их нужное местоположение. Для увеличения криптостойкости алгоритма восемь младших бит коэффициента DC разделяют на два числа по четыре бита и второе число записывают в последний, наименее значимый для качества изображения коэффициент AC. Это позволяет скрыть коэффициент DC, иначе его легко обнаружить, поскольку его значение обычно намного больше, чем значения коэффициентов AC. Для дальнейшего повышения криптостойкости может применяться алгоритм, состоящий из группирования коэффициентов DC нескольких последовательных блоков, шифрования их традиционным алгоритмом, например AES, и возврата соответствующих зашифрованных бит обратно в поток. Данный метод не является достаточно криптостойким, поскольку не обладает свойством рассеивания. Кроме того, видеоинформацию можно распознать при задании одного DC для всех блоков потока и правильном восстановлении двух-трех первых коэффициентов AC для каждого блока.

Метод селективного шифрования [13]

Существует несколько криптографических решений, основанных на многоуровневой структуре MPEG, которые выполняют селективное шифрование. Базовый метод селективного шифрования основан на наличии *I,B* и *P* типов кадров в стандарте MPEG (рис. 11). Он заключается в шифровании ключевых *I* кадров, поскольку, теоретически, *P* и *B* кадры бесполезны без соответствующих *I* кадров. При этом шифрованию подвергается около десяти процентов потока, а это снижает требования к вычислительным ресурсам.

Данный метод имеет следующие недостатки. В *P* и *B* кадрах часто содержатся *I* макроблоки, что делает видимой довольно большую часть изображения. Кроме того, большая межкадровая корреляция также способствует проявлению части скрытой информации. Таким образом, шифрование только *I* кадров не является достаточным. При шифровании всех *I* макроблоков тоже возникают ряд проблем. Во-первых, идентификация *I* макроблока в потоке MPEG – задача ресурсоемкая, поскольку требуется анализировать поток побитово. Во-вторых, существуют потоки, либо *I,B,P* кадры с начальных стадий MPEG (ДКП, квантование, предсказание движения) состоящие только из *I* кадров, либо содержащие количество *I* макроблоков того же порядка, что и количество *I* кадров. В этих случаях шифрование *I* кадров и *I* макроблоков в *P* и *B* кадрах по объему шифруемых данных (до 90 % всего потока) и соответственно по требуемой вычислительной мощности приближается к полному шифрованию. Существует вариант реализации метода селективного шифрования SECMPEG, не совместимый со стандартным MPEG из-за дополнительной информации в заголовках и требующий поэтому специализированного декомпрессора. SECMPEG использует DES или RSA и позволяет выбрать один из четырех уровней защиты: первый уровень – шифруются все заголовки; второй уровень – шифруются заголовки, коэффициент DC и нижние коэффициенты AC в *I* кадрах; третий уровень – шифруются *I* кадры и *I* макроблоки в *P* и *B* кадрах; четвертый уровень – полное шифрование потока.

Метод шифрования на основе изменяемых кодовых таблиц [13]

Методы селективного шифрования обладают недостатком: поскольку шифрование происходит до сжатия, то оно может увеличивать размер сжатого видео. Для устранения этого недостатка используется схема шифрования со сжатием, осуществляющая одновременно шифрование и сжатие на этапе кодирования по Хаффману

Алгоритм заключается в создании 2^k таблиц Хаффмана и задании ключа в виде вектора $\vec{p} = (p_1 \ldots p_n)$, где p_i – число длиной k бит, являющееся номером одной таблицы из $n = 2^k$. Для каждого j-го входящего символа (байта) используется p_m–я таблица для кодирования и шифрования, где $m = ((i - 1) \bmod n) + 1$, т.е. для каждого поступающего на вход кодера Хаффмана байта в соответствии с i-м элементом вектора $\vec{p}$ выбирается кодовая таблица, а затем из нее – кодовое слово, соответствующее данному байту. В данной схеме ключом является

набор таблиц и управляющий вектор $\vec{p}$. Быстродействие этого алгоритма очень высокое и практически не влияет на скорость работы MPEG кодека. Данный алгоритм небезопасный, так как кодирование Хаффмана – это простой подстановочный шифр с символами переменной длины, не обладающий свойством рассеивания. Поэтому данный шифр чувствителен к криптоатаке с выбранным открытым текстом, которая позволяет за некоторое конечное число попыток найти все кодовые таблицы. Вскрытие с известным открытым текстом затруднено из-за сложности для криптоаналитика синхронизировать открытый текст и шифротекст.

Особенности защиты аналоговых видеосигналов [9]

Основные требования к такой системе шифрования - она должна быть недорогой, надежной, причем качество сигнала при этом не должно ухудшаться. Первое требование очевидно и означает, что стоимость декодера не должна существенно влиять на стоимость всей приемной установки. Высокая надежность предполагает, что требуется специальное устройство - декодер, который, по крайней мере, не может быть изготовлен в домашних условиях и содержит ключ или специальную карту, защищенные от копирования. Самый простой метод защиты - искажение синхросигнала так, что стандартный телевизионный приемник не может восстановить изображение, оно появляется на экране в виде отдельных полос или сегментов. Информация о синхросмеси передается в сигнале в скрытой форме и обнаруживается декодером, который восстанавливает стандартные синхроимпульсы. Более высокая надежность достигается добавлением инвертирования части сигнала, смещением его уровня. Еще более сложный путь - сдвиг во времени отдельных строк изображения, или рассечение строк и перестановка местами рассеченных частей, или перестановка местами строк.

Засекречивание звуковых сигналов в цифровом телевидении не представляет особой проблемы, здесь может широко использоваться весь арсенал методов, разработанных ранее для цифровой радиосвязи. В одной из практически реализованных систем цифровой поток зашифровывается с помощью передаваемого вместе с сигналом кодового слова длиной 56 бит, генерируемого псевдослучайным образом и сменяемого с интервалом от долей до нескольких секунд Кодовое слово в свою очередь зашифровывается с помощью ключа, обновляемого раз в несколько недель, а тот последний рассылается абонентам по спутниковому каналу также в засекреченном виде Алгоритм декодирования записывается в кристалле микропроцессора, помещаемом либо в декодере, либо в абонентской карточке и работающем только при наличии ключа. Степень секретности такого кода весьма высока.

Абонентские карты свои пароли наружу не выдают. Но сами они декодировать видеопоток тоже не могут - не хватает мощности. Поэтому декодирование проводится в два этапа. Карточка вставляется в специальный блок тюнера - CAM (Conditional Access Module, модуль условного доступа). При приеме кодированного канала CAM-модуль транслирует карте всю служебную информацию, идущую на канале параллельно видеосигналу (примерно как телетекст). На закрытых каналах в этой информации есть, среди прочего, и схема восстановления телесигнала. Эта схема зашифрована, и вот именно для ее расшифровки в смарт-карте есть ключи. Получив от CAM-модуля такую схему, карта расшифровывает ее собственным процессором и возвращает назад. А CAM-модуль, который часто называют декодером, с помощью этой расшифрованной схемы восстанавливает телесигнал.

Схемы восстановления передаются каждые десять-пятнадцать секунд. Но зашифрованы они одним ключом, который хранится в смарт-карте и меняется гораздо реже вещателем канала. Пока карта вставлена в работающий тюнер, ей транслируется вся служебная информация, идущая на канале параллельно обычной картинке. Либо со спутника, если тюнер с CAM-модулем подключен к спутниковой антенне. А если это тюнер кабельной сети - тогда через кабель.

Современная смарт-карта позволяет вести «управление через эфир» - команды для смарт-карты передаются вместе с телевизионным сигналом, как телетекст. Так можно посылать новые ключи для декодирования каналов - карта их запомнит и будет использовать. Кроме того, через эфир можно просто включать-выключать карточки.

Команды повторяются круглосуточно (к примеру, если тюнер во время передачи команды выключен), и даже если зрителей сотни тысяч, цикл обращений ко всем их карточкам проходит за десятки минут.

Irdeto/Luscrypt

В одной из первых использовавшихся в Европе систем вместо строчного синхроимпульса подставлялся пакет синусоидальных колебаний с частотой 2,5 МГц, применялись также различные варианты инвертирования изображения. Разновидность этого метода под названием Irdeto/Luscrypt используется при кодировании программы RTL-4 на спутнике Astra. Схожий результат получается при передаче цифровых звуковых сигналов в интервале обратного хода луча, используемой Европейским вещательным союзом в системе "Евровидение". Цифровой пакет нарушает структуру строчного синхроимпульса и сбивает работу амплитудного селектора, поэтому на приеме необходимо специальное устройство регенерации синхросмеси.

Системы со смещением уровня отдельных компонентов видеосигнала оказались не очень надежными и постепенно от них отказались в пользу более совершенных методов со смещением во времени отдельных элементов изображения, которые обеспечивают значительно более высокую надежность. Среди

систем, позволяющих распознать изображение, но затрудняющих его просмотр наиболее известна Discret, где изображение каждой строки задерживается на 0,1 или 2 мкс с помощью дополнительных аналоговых линий задержки, подключаемых к каналу на период строки по псевдослучайному закону. На приемной стороне закон чередования восстанавливается по кодовому слову, передаваемому совместно с сигналом и расшифровываемому декодером.

Videocrypt

В системе Videocrypt кодер рассекает каждую строку в одной из 256 точек, выбранных по псевдослучайному закону, и меняет местами части рассеченной строки. При этом полностью разрушается структура изображения по вертикали, но частично сохраняется горизонтальная структура - титры, надписи, меню программ Информацию, необходимую для восстановления изображения, декодер получает из двух источников: один ключ передается в закодированном виде в интервале кадрового гасящего импульса, другой распространяется в виде специальной абонентской карточки, рассылаемой подписчикам периодически. Videocrypt - наиболее распространенный метод кодирования ТВ сигналов, передаваемых в системе PAL.

Nagravision

Более сложная система Nagravision требует на приеме памяти объемом в полукадр. Изображение на передающей стороне записывается в буфер и передается построчно, но с перемешиванием порядка строк по псевдослучайному закону. На приеме операции производятся в обратном порядке. В системе Nagravision вертикальная структура изображения не нарушается, но любая горизонтальная полоска как бы размазывается по всему экрану. Эта система в свое время была выбрана в качестве основной испанскими вещательными компаниями.

Syster

Метод кодирования по системе Nagravision требует наличия в декодере цифровых микросхем памяти, объема которых достаточно для запоминания информации и полукадре, что заметно повышает стоимость декодера. Для ее сни-жения была разработана модификация метода (Syster), в которой строки в полукадре разделены на шесть блоков и перемешивание строк осуществляется внутри каждого блока. Это усовершенствование позволило уменьшить объем необходимой памяти и в конечном счете удешевить декодер. Для авторизации (опознавания) декодера применяется специальный ключ со встроенной микросхемой, аналогичной карточке в системе VideoCrypt. Система кодирования изображения Syster используется на российских спутниках ГАЛС-1, -2 (36°E). Ее также использует крупнейшая вещательная компания Франции Canal Plus для передачи программ через спутник Telecom HB.

Videocipher II

Все применяемые на североамериканском континенте системы засекречивания имеют общую особенность, повышающую их надежность: абонентский декодер работает в интерактивном режиме и активизируется только когда, когда получает от центра управления соответствующую команду. В наиболее распространенной системе Videocipher II, разработанной компанией General Instruments из видеосигнала полностью удаляются обычные сигналы синхронизации, полярность сигнала инвертируется, а сигналы цветового опознавания переносятся на нестандартную частоту. Обычный ТВ приемник не может принять такой сигнал, и требуется установка специального декодера. Каждому декодеру присвоен индивидуальный номер ,и при включении он посылает свой номер по телефонным линиям в центр управления компании General Instruments, где он опознается и по спутниковому каналу подается специальное сообщение санкционирующее прием и содержащее инструкции по декодированию. Таким способом практически исключается использование "пиратских" декодеров.

Сигналы двух звуковых каналов в системе Videocipher II передаются в цифровом виде совместно с сигналами синхронизации и другой служебной информацией в интервале строчного гасящего импульса. Аналого-цифровое преобразование осуществляется с точностью 15 бит/отсчет, что обеспечивает динамический диапазон звучания более 75 дБ (теоретически 92 дБ).

В связи с широким распространением стандарта D2-MAC в спутниковом вещании возникла необходимость кодирования телевизионных сигналов этого стандарта. В системе D2-MAC яркостные и цветоразностные компоненты изображения передаются отдельно, поэтому рассечение и перестановка этих компонент также осуществляются раздельно. Эта система, получившая название EuroCrypt, широко используется на спутниках SIRIUS (5,2°E), TELE-X (5°E), INTELSAT-707 (1°W), THOR-1 (0,8°E), TV SAT-2 (0,6°E). Для системы кодирования EuroCrypt разработаны два способа: перестановка компонент с двухкратным рассечением и перестановка компонент цветоразностного сигнала. В первом случае обеспечивается больший уровень засекречивания, сигналы яркости и цветности разрезаются каждый в некоторой точке и компоненты их переставляются местами. Место рассечения изменяется по псевдослучайному закону независимо для каждой компоненты

Для расшифровки на приеме используется абонентская карточка с вмонтированным в нее кристаллом памяти, в которой записаны ключи к коду и инструкции по дешифровке. Eurocrypt применяется более чем в 80% всех ТВ каналов, использующих сигналы D2- и D2-MAC.

Перестановка строк и столбцов

Широко распространенный подход к шифрованию видеоданных, приемлемый для сохранения качества изображения и требований быстродействия заключается в перестановке строк или столбцов кадров видеоизображения [1]. Необходимо отметить, что такой шифр нельзя назвать стойким. Нами был произведен ряд экспериментов по восстановлению изображений, зашифрованных подобными методами. На рисунках 1 и 2 показан пример такого восстановления.

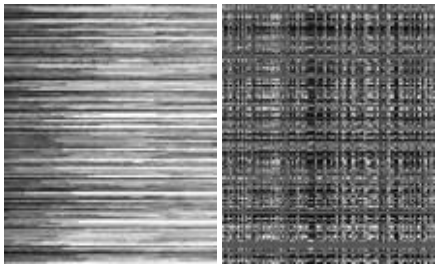

Рис. 1 а), б). Зашифрованные изображения

Рис. 2 а), б). Восстановленные изображения

Здесь в качестве критерия для отбора строк и столбцов выбрана мера близости, основанная на метрике $d(a_i, a_j) = \sum_{k=1}^{m} | a_{i,k} - a_{j,k} |$, где A – матрица, соответствующая изображению. Оказалость, что в данной метрике практически не возникает коллизий, и исходное изображение легко восстанавливается, аналогично тому, как восстанавливается текст по анализу биграмм и триграмм [2]. Трудоемкость восстановления оценивается как $O(n^3)$.

Очевидно, что подобное восстановление возможно, потому что изображение обладает большой пространственной избыточностью.

Для защиты от подобной атаки предлагается использовать несколько подходов:

1. Применение нескольких раундов шифра двойной перестановки, совместно с обратимым искажающим преобразованием, которое должно уменьшать корреляцию между строками и столбцами.
2. Применение нескольких раундов циклической перестановки строк и столбцов, совместно с обратимым искажающим преобразованием.
3. Применение комбинации этих двух подходов.

Следует отметить, что данный подход учитывает специфику защищаемой информации.

Оценить эффективность такого метода достаточно просто. Для этого достаточно исследовать распределение пикселей зашифрованного изображения, относительно их исходного положения. Предлагается исследовать распределение пикселей, которые до шифрования были соседними. Если среднее расстояние между такими пикселями будет равно математическому ожиданию между произвольно взятыми точками изображения, то можно говорить о том, что защита является надежной. Также необходимо проверить последовательности координат зашифрованного изображения с помощью различных критериев РРСП (равномерно распределенная случайная последовательность)

Вычисление плотности вероятности, математического ожидания и дисперсии расстояния между двумя случайно выбранными точками на прямоугольной области размерами a и b (a>b):

$$M\xi = \frac{1}{a^2 b^2} \int_0^a \int_0^a \int_0^b \int_0^b \sqrt{(x-y)^2 + (z-k)^2}\, dx\,dy\,dz\,dk$$

$$M\xi = \frac{a^2+b^2}{15a^2b^2} + \frac{\sqrt{a^2+b^2}}{3} - \frac{(a^2+b^2)^{\frac{5}{2}}}{15a^2b^2} +$$

$$+ \frac{b^2}{6a}\ln\left(\frac{b}{\sqrt{a^2+b^2}-a}\right) + \frac{a^2}{6b}\ln\left(\frac{a}{\sqrt{a^2+b^2}-b}\right)$$

$$D\xi = M\xi^2 - (M\xi)^2$$

$$M\xi^2 = \frac{1}{a^2 b^2} \int_0^a \int_0^a \int_0^b \int_0^b (x-y)^2 + (z-k)^2\, dx\,dy\,dz\,dk =$$

$$= \frac{a^2+b^2}{6}$$

$$p(x) = \begin{cases} 0, x < 0 \\ p_1(x), x < a, x < b \\ p_2(x), b \le x \le a \\ p_3(x), b < x \le \sqrt{a^2+b^2} \\ 0, x > \sqrt{a^2+b^2} \end{cases}$$

$$p_1(x) = \frac{1}{2a^2b^2}\left(\frac{x^4}{2} - (a+b)x^2 + \frac{ab\pi x^3}{2}\right)$$

$$p_2(x) = \frac{x}{4a^2b^2\sqrt{x^2-b^2}} \times$$

$$\left(\begin{array}{l} \mathbf{-ab^3}\ln(b+x) - 2ax^2\sqrt{x^2-b^2} - \\ -2ab^2x - b^2x\sqrt{x^2-b^2} + b^3 a\ln(b+x) - \\ -2abx\arcsin\left(\frac{\sqrt{r^2-b^2}}{r}\right)\sqrt{x^2-b^2} + \\ +ab\pi x\sqrt{x^2-b^2} + 2ax^2 \end{array}\right)$$

$$p_3(x)=\frac{r^4}{4a^2b^2\sqrt{x^2-a^2}\sqrt{x^2-b^2}}\times$$
$$\left(\begin{array}{l}2b\sqrt{x^2-b^2}-\\-\sqrt{x^2-b^2}\sqrt{x^2-a^2}+\\+2a\ \sqrt{x^2-a^2}\end{array}\right)+$$
$$+\frac{r^2}{4a^2b^2\sqrt{x^2-a^2}\sqrt{x^2-b^2}}\times$$
$$\left(\begin{array}{l}2ab\sqrt{x^2-b^2}\sqrt{x^2-a^2}\arcsin\left(\frac{a}{x}\right)-\\-b^2\sqrt{x^2-b^2}\sqrt{x^2-a^2}-\\-a^2\sqrt{x^2-b^2}\sqrt{x^2-a^2}-\\-2ab\sqrt{x^2-b^2}\sqrt{x^2-a^2}\arcsin\left(\frac{\sqrt{x^2-b^2}}{x}\right)-\\-2ab^2\sqrt{x^2-a^2}\end{array}\right)$$

Для исследования было взята фотография автора:

$Размеры: a=160, b=120$

$M\xi =$ **73.3836767**

Dξ **= 1281.502662**

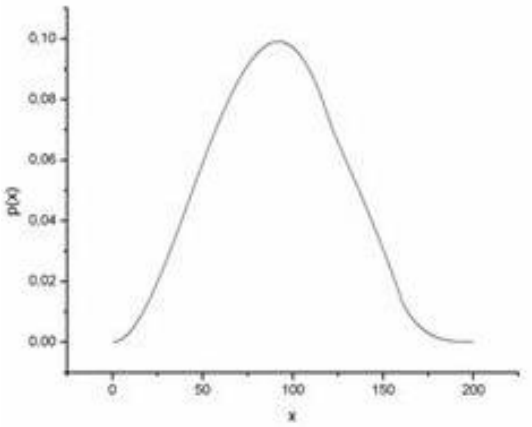

Рис. 3. График p(x)

Ниже представлены наглядные результаты экспериментов с разным числом раундов шифрования.

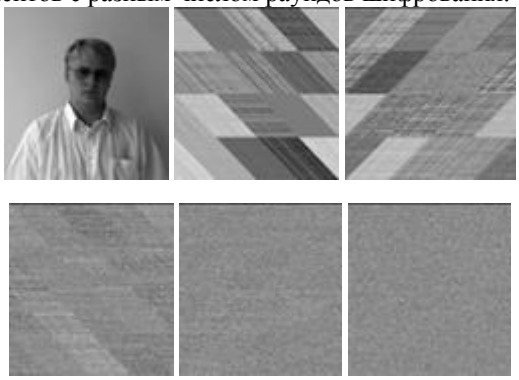

Рис. 4. а) исходное изображение б) 1 раунд шифрования в) 2 раунда г) 5 раундов д) 8 раундов е) 10 раундов

Двойная перестановка совместно с перестановкой блоков изображения. В качестве искажающего преобразование выбрано «отражение» относительно диагоналей.

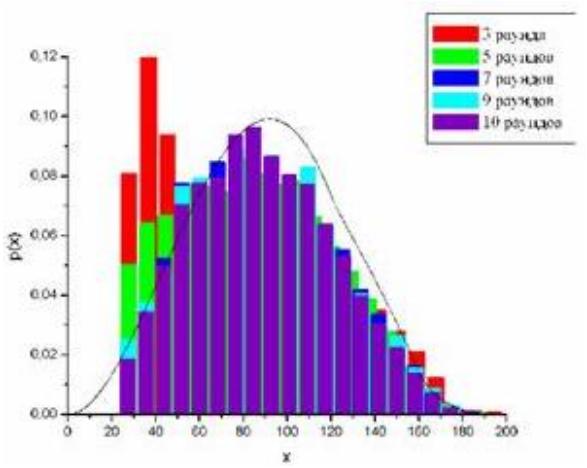

Рис.5 Распределение расстояния между точками, которые были соседними до шифрования

Циклические сдвиг строк и столбцов

Рис. 6. а) исходное изображение б) 1 раунд шифрования в) 2 раунда г) 3 раунда

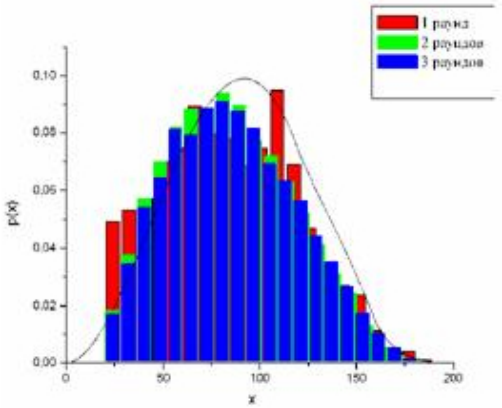

Рис.7 Распределение расстояния между точками, которые были соседними до шифрования

Последовательности координат проходят тесты на РРСП

Применялись следующие тесты РРСП:

- Спектральный тест.
- Тест приращения энтропии.

Кроме того, у этого метода есть еще одно полезное свойство – можно восстанавливать поврежденные изображения, так как после шифрования местонахождение исходных пикселей равновероятно.

Примеры восстановления поврежденных изображений:

Рис. 8. а) исходное изображение б) после шифрования

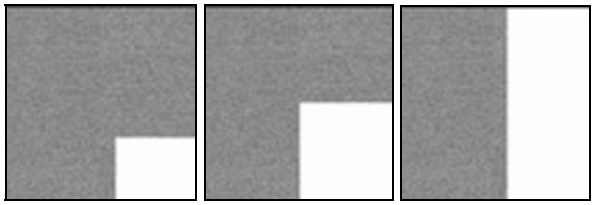

Рис. 9 а), б), в) поврежденные изображения

Рис. 10 а), б), в) после дешифрования

Рис. 11 а), б), в) после применения фильтра

Исходя из этого, представляется перспективным использовать для защиты видеоданных шифр на основе многораундовой двойной перестановки. Двойная перестановка применяется несколько раз совместно с обратимым искажающим преобразованием. Кроме того, поскольку процедура дешифрования шифра двойной перестановки может быть сведена к решению задачи проверки изоморфизма графов [3], можно использовать алгоритмы её решения для построения криптосистемы, реализующей защищенный видеоканал. Особенностью этой криптосистемы является неявная передача ключа к шифру. То есть ключ шифрования динамически изменяется в процессе передачи и является результатом решения задачи проверки изоморфизма для соответствующих графов.

Если пикселям нешифрованного изображения соответствует матрица С, то шифру двойной перестановки изображения будет соответствовать матрица $C' = P_1 * C * P_2^T$, где P_1, P_2 - матрицы перестановок, реализующие перестановку строк (P_1) и перестановку столбцов (P_2) матрицы С. Будем далее в тексте обозначать перестановки и соответствующие им матрицы одинаково. Построим по С матрицу C_2, а по C' - матрицу C_2':

$$C_2 = \begin{pmatrix} 0 & C \\ C^T & 0 \end{pmatrix}, \; C_2' = \begin{pmatrix} 0 & C' \\ C'^T & 0 \end{pmatrix}$$

Матрицы C_2 и C_2' - симметрические матрицы. Они могут рассматриваться как матрицы смежности некоторых взвешенных неориентированных двудольных графов.

Формулировка задачи проверки изоморфизма графов в терминах матриц смежности и матриц перестановок следующая. Даны два графа G_1 и G_2, представленные их матрицами смежности A_1 и A_2. G_1 и G_2 изоморфны тогда и только тогда, когда существует такая матрица перестановки P, что $A_1 = PA_2P^T$.

Поскольку $C' = P_1CP_2^T \Leftrightarrow C'^T = P_2C^TP_1^T$, то

$$C' = P_1CP_2^T \Leftrightarrow C_2' = PC_2P^T,$$

где

$$P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix},$$

поскольку

$$PC_2P^T = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}\begin{pmatrix} 0 & C \\ C^T & 0 \end{pmatrix}\begin{pmatrix} P_1^T & 0 \\ 0 & P_2^T \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & P_1C \\ P_2C^T & 0 \end{pmatrix}\begin{pmatrix} P_1^T & 0 \\ 0 & P_2^T \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & P_1CP_2^T \\ P_2C^TP_1^T & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & C' \\ C'^T & 0 \end{pmatrix} = C_2'.$$

Таким образом, если один кадр является шифром двойной перестановки другого, то соответствующие им графы - графы с матрицами смежности C_2 и C_2'-изоморфные графы. Изоморфизм графов, задаваемый матрицей перестановки Р задает перестановку строк и столбцов пикселей изображения перестановки P_1 и P_2. То есть дешифрование шифра двойной перестановки равносильно решению задачи проверки изоморфизма взвешенных неориентированных графов.

Для всех алгоритмов решения задачи проверки изоморфизма графов эта задача является тем более сложной, чем больше мощность групп автоморфизмов графов, проверяемых на изоморфизм. Группа

автоморфизмов графа G_1 с матрицей смежности A_1 состоит из всех матриц перестановки P таких, что $A_1 = PA_1P^T$.

Вместо передачи абоненту B перестановок P_1 и P_2, необходимых тому для дешифрования зашифрованного кадра, абонент A будет передавать ему C'. Обладая и C' и C, ставя и решая задачу проверки изоморфизма графов абонент B получает P, а следовательно и P_1 и P_2. Нетривиальность группы автоморфизмов графов, отвечающих C_2 и C_2', влечёт неединственность решения задачи поиска изоморфизма графов, то есть задачи поиска решающих перестановок P_1 и P_2, что неприемлемо, поскольку для функционирования строимой нами криптосистемы абоненты A и B должны обладать одной и той же перестановкой, дающей ключ к шифру – k_{AB}. Поэтому изображения, предназначенные для неявной передачи ключа к шифру по открытому каналу связи (называемые в дальнейшем "сигнальными") должны быть такими, что группы автоморфизмов соответствующих им графов тривиальны.

Момент времени, в который происходит смена перестановки P_0, наступает через равные промежутки времени Δt. Пусть t^M – время, которое, предположительно, требуется противнику M для несанкционированного получения P_0, t^P – время, которое требуется абонентам A и B для определения P_0, t^C – время, необходимое для процедуры шифрования одного кадра абонентом A, его пересылки по каналу связи и его дешифрования абонентом B.

Для того, чтобы задача дешифрования видеоизображения противником M не являлась для него вычислительно эффективной, тогда как оставалась бы таковой для A и B, необходимо выполнение неравенства

$$t^P + kt^C \le \Delta t < t^M,$$

где k – количество кадров, передаваемых без смены перестановки.

Для решения задачи проверки изоморфизма используем метод спектрального расщепления, описанный в [3]. Чтобы его использование было вычислительно эффективно, необходимо, чтобы графы обладали свойством тривиальности группы автоморфизмов [4].

Построение криптосистемы.

1. Пусть абоненты обладают набором одинаковых изображений, таких, что соответствующие им графы обладают тривиальной группой автоморфизмов.
2. Абоненты выбирают одно из изображений с помощью какого-либо протокола с нулевым разглашением.
3. Один из абонентов применяет случайную двойную перестановку к выбранному изображению и рассылает ее всем остальным.
4. Абонент, получивший изображение, подвергшееся перестановке, зная какое изображение было выбрано на шаге 2, ставит задачу проверки изоморфизма и вычисляет перестановку.
5. Полученная двойная перестановка объявляется текущим ключом.

Для демонстрации возможностей была разработана программа, реализующая все вышеизложенное. Она позволяет как вести диалог нескольким абонентам, так и осуществлять трансляцию одного видеоизображения нескольким клиентам. Среда разработки – Borland C++ Builder 6.0. Из ее особенностей можно отметить, что вместо набора изображений у абонентов имеется алгоритм их генерации. Протокол выбора изображений (параметров алгоритма генерации) построен на базе протокола конференц-связи, описанного в [5].

Литература

1. Володин А.А., Митько В.Г., Спинко Е.Н. Обработка видео в системах телевизионного наблюдения // Вопросы защиты информации. М.: 2002. С. 34-47.
2. Алферов А.А., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии // М: Гелиос АРВ, 2001.
3. Faizullin R., Prolubnikov A. An Algorithm of the Spectral Splitting For The Double Permutation Cipher // Pattern Recogniton and Image Analysis. MAIK, Nauka. Vol. 12, p. 365-375. No. 4, 2002.
4. Пролубников А.В., Файзуллин Р.Т. Класс графов, задача проверки изоморфизма для которых разрешима за полиномиальное время алгоритмом спектрального расщепления // Математические структуры и моделирование: Сб. научн. тр. Под ред. А.К.Гуца. Омск: Омск. гос. университет, 2003. Вып. 11. С.28-57.
5. Burmester M. Desmedt Y. A secure and efficient conference key distribution system // Advanced in Cryptology – EUROCRYPT'89. LNSC 434. – 1990. – pp. 122 – 133.
6. "Засекречивание ТВ сигнала" (http://www.smolsat.com/secret.html)
7. 'A basic intro to VideoCrypt' (http://www.heyrick.co.uk/willow/vcrypt.html)
8. «Защита телеканалов и возможность ее преодоления» (http://www.computerra.ru/offline/2002/469/21579/print.html)
9. Системы кодирования спутниковых каналов (http://sat-tv.infonet.by/kod.htm)
10. Жельников В. Криптография от папируса до компьютера. // М.: ABF, 1996
11. Брассар Ж. Современная криптология. // М.: Полимед, 1999.
12. Петраков А.В., Лагутин В.С. Телеохрана. // М.: Энергоатомиздат, 1998. С. 245–257.
13. Lintian Qiao and Klara Nahrstedt. Comparison of MPEG Ecryption Algorithms // International Journal on Computers and Graphics, Special Issue: Data Security in Image Communication and Network, 1998, vol. 22.
14. Chung-Ping Wu, C. Jay Kuo. Efficient Multimedia Encryption via Entropy Codec Design // SPIE International Symposium on Electronic Imaging 2001 (San Jose, CA, USA), Proceedings of SPIE, Jan. 2001, vol. 4314.