RECONSTRUCTION OF TECHNOLOGY FOR FRAME VIDEOINFORMATION FLOW TELECOMMUNICATION NETWORK

It is shown that with intensive growth and the use of modern information technologies, the need in enhancing the effectiveness of existing systems transmission and storage of video data. Substantiates the necessity using new techniques with the preliminary compression of video information based on the transformation by orthogonal transformations. Set forth rationale that the provision of timely and reliable information possible on the basis of the development of mutually-univocal video data renewal processes. Developed the technology for reconstruction component transforms, based on the reconstruction of the low-frequency components of the transformants, a significant component of the vector by obtaining positional numbers with unequal adjacent components and vector scaling based component decoding Bodo. Sets out the sequence, and basic recovery steps describe of each constituent the vector transformants. It is shown that the proposed method allows the for reconstructionto restore transformants without introducing errors, provide the necessary credibility.

Index Terms: image reconstruction, transform, statistical code, important components, refinable components.

Баранник Владимир Викторович, доктор технических наук, профессор, начальник кафедры Харьковского университета Воздушных Сил имени Ивана Кожедуба.
E-mail: barannik_v_v@mail.ru.
Баранник Володимир Вікторович, доктор технічних наук, професор, начальник кафедри Харківського університету Повітряних Сил імені Івана Кожедуба.
Barannik Vladimir, Doctor of Technical Science, Professor, chief of chair, Kharkov University of Aircraft of the name of Ivan Kozhedub.

Кривонос Владимир Николаевич инженер Харьковского университета Воздушных Сил имени Ивана Кожедуба.
E-mail: k.v.n-26@mail.ru
Кривонос Володимир Миколайович інженер Харківського університету Повітряних Сил імені Івана Кожедуба.
Krivonos Vladimir, engineer at Kharkov University of Aircraft of the name of Ivan Kozhedub.

УДК 004.627

СПОСОБЫ ЗАЩИТЫ ВИДЕОДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Любовь Рябова, Евгений Подгорный, Карина Мацуева

В статье дан обзор существующих методов ее защиты. Следствием развития видеотехнологий стало массовое распространение случаев незаконного копирования и просмотра видеоданных, − возникла проблема защиты видеоинформации. В частности, видеоданные могут распространяться с нарушением авторских прав (пиратство), а также к ним могут несанкционированно обращаться конкуренты или злоумышленники для получения конфиденциальной информации (шпионаж). Самый простой подход к защите видеоданных − это использование классического шифрования по схемам с открытым или закрытым ключом. Файл видеоданных шифруется, после чего передается по незащищенному каналу связи или записывается на незащищенный носитель. Такой способ обеспечивает весьма высокую степень защиты видеоданных, которая достигается высокой стойкостью используемого для защиты шифра. Однако, зачастую объем шифруемых данных по сравнению с текстовыми и даже звуковыми данными значительно больше, что требует значительных вычислительных ресурсов для шифрования такого объема данных. Это приводит к ограничению возможности использования классического шифрования в таких областях, как интерактивное и кабельное телевидение. Пользователь таких сервисов должен иметь мощную систему, способную в реальном времени, без задержек расшифровывать, а затем и декодировать полученные данные. Поскольку основным стандартом, используемым для кодирования и сжатия видеоинформации, является формат MPEG, то большинство способов защиты разработаны именно для этого формата. В них используются особенности кодирования и структуры потока MPEG для сокращения вычислительных ресурсов на защиту видеоданных. Одним из первых способов защиты данных в формате MPEG был алгоритм перестановки «зигзаг». Суть его заключается в считывании квантованных коэффициентов дискретного косинусного преобразования не способом «зигзаг» для последующего кодирования, как это определено в формате, а случайным образом. Рассмотрены различные методы защиты видеоданных применительно к телекоммуникационным системам реального времени.

Ключевые слова: *видеоданные, защита видеоданных, несанкционированный доступ, кодирование видеоинформации, шифрование данных, методы защиты видеоданных.*

Современная проблематика защиты информации включает множество задач теоретического и практического применения, комплексное решение которых отвечает поставленной целевой функции. В настоящей работе рассмотрен один из теоретических вопросов построения различных способов защиты видеоданных в составе системы автоматизированного управления доступом, основанной на бесконтактной аутентификации объектов – пользователей по телевизионным изображениям их биометрических характеристик (геометрическое строение лица, радужная оболочка глаза и т.д.). Совмещение телевизионной функции в составе компьютера потребовало внедрения специализированного протокола кодирования MPEG видеоданных.

Постановка задачи. На содержательном уровне пёриведем формализацию содержания постановки задачи кодирования. По открытому каналу связи от источника (абонента *A*) к приёмнику (абоненту *B*) передаётся сигнал видеоизображения. Необходимо шифровать этот сигнал видеоизображения, чтобы избежать несанкционированного доступа к передаваемой видеоинформации при подключении третьих лиц (противника *Z*) 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 выходящий кадр *p* видеоизображения с помощью функции шифрования *EAB* и ключа *kAB* в кадр *c* зашифрованного видеоизображения: $S=E(p)\ kAB$, который и поступает в канал связи. Приёмник восстанавливает переданный кадр видеоизображения с помощью функции дешифрования *kd BA* и того же секретного ключа *kAB* определив ключ дешифрации *kd* из условия $k \times kd = 1$: $p = kd\,BA(S)$.

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

По существу видеоданные ничем не отличаются от других данных − это набор битов, которые определенным образом структурированы. Как следствие, самый простой подход к защите видеоданных − это использование классического шифрования по схемам с открытым или закрытым ключом благодаря методам компрессии, основанным на «схожести» последовательных изображений и несовершенстве нашего зрения.

MPEG-кодирование начинается с создания исходного (ключевого) I-кадра, или Intra-кадра. I-кадры играют роль опорных при восстановлении остальных изображений и размещаются последовательно через каждые 10-15 кадров. В интервале между I-кадрами изменяются только некоторые фрагменты изображений, и именно эта разница кодируется. Кроме I-кадров в MPEG-последовательности имеются еще два типа изображений:

– predicted (P) – предсказанные кадры, описывающие различия между текущим и предыдущим кадрами (типа I или P);

– bi-directional interpolated (B) – интерполированные в двух направлениях (вперед и назад) кадры, содержащие лишь указатели на предыдущие или последующие кадры типа I или P.

Основу файла формата MPEG составляют *I-кадры*, сжатие которых выполняется только с применением внутрикадрового предсказания. Выделение I-кадра – это первый этап, на котором степень компрессии еще относительно невелика, но зато восстановленное изображение почти полностью соответствует исходному, а его качество мало зависит от ошибок, возникающих в процессе кодирования и передачи сигнала по каналу связи. Вообще MPEG-кодирование – процесс «возвратно-поступательный». Кодирование *P-кадров* выполняется с помощью алгоритмов компенсации движения и межкадрового предсказания вперед по предшествующим I- или P-кадрам до тех пор, пока в блоке не появится новый объект. После его обнаружения опять происходит переход к алгоритмам, используемым для кодирования I-кадров, т.е. к внутрикадровому предсказанию. Заметим, что степень сжатия P-кадров почти втрое превышает этот показатель для I-кадров.

Определим «иерархию»: I-кадры являются основой для предсказания P- и B-кадров, а P-кадры, в свою очередь, используются для создания последующих P- или B-кадров. Очевидно, что ошибки любого кадра распределяются по всем кадрам, созданным на его основе, поэтому

при декодировании I- и P-кадров требуется обеспечивать высокую точность восстановления исходного изображения.

Алгоритмы кодирования *B-кадров* зависят от характера картинки. В MPEG предусмотрено четыре способа кодирования. Первый, самый простой, – компенсация движения и предсказание вперед по ближайшим предшествующим I- или P-кадрам. При появлении в кодируемом B-кадре новых объектов применяется предсказание назад по ближайшим последующим I- или P-кадрам вместе с компенсацией движения. Третий алгоритм включает в себя компенсацию движения и двунаправленное предсказание по предшествующим и последующим I- или P-кадрам. И, наконец, четвертый основан на внутрикадровом предсказании без компенсации движения (он чаще всего используется при резкой смене плана или высоких скоростях движения отдельных фрагментов картинки).

При кодировании B-кадров обеспечивается наибольший коэффициент сжатия. Однако чем выше степень сжатия, тем ниже точность восстановления исходного изображения. Именно поэтому B-кадры не применяются в качестве опорных, а значит, и ошибки при их декодировании не распределяются по другим кадрам [1].

Метод компенсации движения, определенный в алгоритме MPEG, основан на обработке *макроблоков* (структурных единиц кадра, описывающих квадратные участки изображения размером 16 пикселей на 16 строк). Согласно спецификации MPEG, размеры макроблока согласуются со структурой, используемой для дискретизации изображения ТВ-кадра. При этом в каждом ТВ-кадре должно быть целое число макроблоков. В процесс кодирования входят операции сравнения базового и последующих кадров, поиска идентичных или похожих макроблоков. Макроблоки, не содержащие изменений, игнорируются. В результирующем потоке сохраняются только данные о различиях между кадрами – так называемый *вектор смещения*. Чтобы определить вектор смещения, например, при предсказании вперед, поиск нового положения определенного макроблока первого кадра выполняется в зоне поиска второго кадра. Для всех отсчетов этого макроблока вычисляются межкадровые разности и рассчитываются координаты вектора смещения, описывающего движение макроблока по вертикали и горизонтали относительно его начального положения.

Зона поиска должна быть достаточно большой, чтобы быстро движущийся макроблок изображения первого кадра не вышел из зоны поиска второго кадра. Однако ее размеры ограничены техническими возможностями аппаратуры, так как понятно, что чем больше размер зоны, тем больше и объем вычислений, которые необходимо выполнить в масштабе реального времени. На практике размеры зоны в четыре раза больше размеров макроблока, т.е. она ограничена квадратом изображения 64x64 пикселей.

Повышение эффективности сжатия. К настоящему времени создано множество схем сжатия, по которым выполняется компрессия различной степени – от средней, используемой при профессиональной видеозаписи, до достаточно высокой, реализуемой в любительских магнитофонах и устройствах видеозаписи на компакт-диски. Для цифрового спутникового, наземного и кабельного телевизионного радиовещания цифровая компрессия становится, в значительной мере, гарантией максимально эффективного использования спектра при одновременном сохранении качества. Чем выше эффективность сжатия, тем более экономно расходуется драгоценный ресурс полосы пропускания, что позволяет либо улучшить качество картинки в пределах заданной полосы, либо, за счет уменьшения полосы, понизить стоимость передачи телевизионной программы. Еще одно техническое решение от Philips – кодер DVS 3115/01, разработанный на базе MPEG-2. Для повышения эффективности сжатия в нем реализованы оптимальное подавление шума, обнаружение момента смены плана, двупроходное кодирование и адаптивное кодирование поля/кадра.

Выбор оптимальной эффективности сжатия – задача достаточно сложная. Пропускная способность должна динамически распределяться в соответствии с требованиями отображения исходного материала. При этом необходимо избегать кодирования изображения, которое не воспринимается зрением человека.

Шум заклятый враг всякого телевидения, в том числе цифрового. Он съедает полосу в ущерб эффективности сжатия или качеству изображения. Ясно, что шум повышает сложность видеосигнала. Являясь в значительной степени случайным, он по-разному проявляется в разных кадрах, увеличивая, таким образом, разностную информацию. А поскольку кодируется и передается именно разностная информация, наличие шума приводит к пустым тратам полосы

частот на его тщательное кодирование, что, понятно, не повышает качества воспринимаемого изображения.

Подавление шума на этапе предварительной обработки исключает как сами шумовые составляющие, так и необходимость их кодирования, т.е. позволяет сберечь драгоценный частотный ресурс. Добавленное к эффективному кодированию, шумоподавление обеспечивает выигрыш в скорости передачи до 15% (при передаче сильно зашумленных сигналов). Сохраненная полоса может использоваться либо для добавления новых каналов, либо для повышения качества изображения.

Выравнивание качества. Поскольку при телевизионном вещании качество передаваемого сигнала во многом определяется сложностью изображения, то для обеспечения комфортного просмотра важно поддерживать качество такого сигнала практически постоянным для изображений различной сложности. С этой целью в MPEG-2 предусмотрен буфер, позволяющий избежать переполнения или недостаточного заполнения декодера.

Двупроходное кодирование применяется в качестве дополнительного способа повышения эффективности сжатия. Процедура выполняется в режиме реального времени, при этом каждый кадр «просматривается» дважды. Во время первого прохода анализируется сложность изображения, чтобы обнаружить момент смены плана и выбрать тип структуры, наилучшим образом соответствующей кодированию данного изображения. При втором проходе создается бинарный поток и выполняется оптимизация распределения бит в доступной пропускной способности канала и использования объема буфера.

Статистическое мультиплексирование. Основу системы кодирования составляет видеокодер, рассчитанный на работу с постоянной либо переменной скоростью потока. Говоря о статистическом мультиплексировании, необходимо понимать, что взаимосвязь между скоростью потока и картинкой не описывается фиксированным соотношением бит, а зависит от содержимого изображения, точнее – от показателя, который часто называют его сложностью (X). Например, если для кодирования двух картинок (1 и 2) разной сложности ($X1<X2$) используется одинаковое количество бит, то их качество изображения (PQ) будет различным ($PQ1>PQ2$). Системы с постоянной скоростью потока будут вести себя именно так. Как правило, качество изображения, полученного при использовании таких систем, достаточно хорошее, за исключением случаев, когда степень сложности изображения превышает возможности видеокодера (тогда искажения кодирования становятся заметными). Технология статистического мультиплексирования, задействуемая, например, в системе StatCast (Philips), позволяет получить выигрыш в использовании полосы (за счет шумоподавления) и реализовать его для достижения лучшего качества изображения и/или понижения «удельной» скорости потока (на канал). Система обеспечивает и такое выравнивание (усреднение) качества получаемых телепрограмм, что качество картинки остается постоянным на протяжении всей передачи; при этом появляется возможность перераспределить пропускную способность. При передаче большинства типов картинок StatCast поддерживает необходимый уровень пропускной способности, как бы «запасая» часть полосы для кодирования более сложных фрагментов изображения. Очень быстрые последовательные изменения изображений также требуют больших затрат пропускной способности (хотя они не всегда определяются человеческим глазом). В системе StatCast быстрая смена картинки отслеживается во избежание расточительности при распределении скорости потока.

Сегодня цифровое телевидение немыслимо без стандарта MPEG. Можно сказать, что оно вообще смогло выйти за порог студий лишь благодаря методам компрессии, основанным на «схожести» последовательных изображений и несовершенстве нашего зрения. Для цифрового телевещания алгоритмы сжатия MPEG-2 позволяют без заметной потери качества снизить первоначальную скорость передачи приблизительно в 20 раз. Если же не предъявлять высоких требований к качеству, то скорость можно снизить в 50 и даже 100 раз.

Поскольку основным стандартом, используемым для кодирования и сжатия видеоинформации, является формат MPEG, то большинство способов защиты разработаны именно для этого формата. В них используются особенности кодирования и структуры потока MPEG для сокращения вычислительных ресурсов на защиту видеоданных.

Метод случайной перестановки коэффициентов ДКП. Стандарт MPEG (Moving Picture Experts Group) был создан для сжатия и передачи аудио и видеоданных. Был принят в мае 1988 г. в Ганновере. Стандарт является открытым, он исполь-

зует особенности восприятия человеком визуальной информации для сжатия данных. Кодирование осуществляется на основании дискретного косинусного преобразования (ДКП) данных пространственно-цветовой области в частотную область – строится матрица коэффициентов ДКП. После этого из матрицы отбрасываются данные, которые вносят незначительный вклад в видеоинформацию кадра. Затем информация кодируется без потерь методом статистического кодирования на основе таблиц Хаффмана. Данный метод заключается в использовании преобразования блока коэффициентов ДКП 8x8 в вектор 1x64 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 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 [2].

Метод селективного кодирования. 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. 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 шифровани 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.

Еще один способ выборочного шифрования [4], суть которого заключается в использовании множества таблиц Хаффмана для сжатия без потерь полученной матрицы коэффициентов

дискретного косинусного преобразования. Из множества таблиц случайным образом выбирается одна для кодирования конкретной последовательности значений матрицы. Недостатком такого способа является снижение эффективности сжатия по сравнению с использованием одной таблицы, адаптированной для использования в кодировании MPEG. Однако этот недостаток частично компенсируется путем предварительного отбора таблиц, обеспечивающих максимальное сжатие для шифруемых видеоданных [5].

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 [5]. Необходимо отметить, что такой шифр нельзя назвать стойким. Здесь в качестве критерия для отбора строк и столбцов выбрана мера близости, основанная на метрике:

$$d(a_i, a_j) = \sum_{k=1}^{m} \left| a_{i,k} - a_{j,k} \right|,$$

где a – матрица, соответствующая изображению. Оказалось, что в данной метрике практически не возникает коллизий, и исходное изображение легко восстанавливается, аналогично тому, как восстанавливается текст по анализу биграмм и триграмм [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).

Использование стойких алгоритмов делает зашифрованные данные стойкими к атакам на основе открытого текста, и в то же время из-за частичного шифрования значительно снижаются затраты вычислительных ресурсов (порядка 10 раз по сравнению с полным шифрованием по DES или IDEA).

Выводы. Таким образом, на сегодняшний день существует обширный арсенал средств защиты видеоданных в формате MPEG. Они позволяют в зависимости от задачи − нужны ли высокая защищенность или компромисс между стойкостью и скоростью обработки − выбрать оптимальное решение. Общей особенностью рассмотренных способов защиты является то, что они основаны на принципах классического шифрования − перестановках и заменах − принципах, известных еще с древних времен. Между тем прогресс бросает все новые вызовы специалистам по защите информации, и вполне возможно, что в ближайшем будущем с развитием вычислительной техники (появлением квантовых компьютеров) эти методы станут в принципе неэффективными. А значит необходимо разрабатывать принципиально новые методы и подходы к защите видеоданных.

ЛИТЕРАТУРА

[1]. Алферов А.А., Зубков А.Ю., Кузьмин А.С. Основы криптографии. – М: Гелиос АРВ, 2001.

[2]. Володин А.А. Митько В.Г., Е.Н. Спинько Е.Н. Обработка видео в системах телевизионного наблюдения // Вопросы защиты информации. – М.: 2002. С. 34-47.

[3]. Рябова Л.В., Голембиевская Ю.Г. Базовые операторы для обработки изображений радужной оболочки глаза // Наука і молодь: Зб. наук. пр. – К.: НАУ, 2006. – Вип.6.– С. 45-48.

[4]. Chung-Ping Wu and C.-C. Jay Kuo. Efficient Multimedia Encryption via Entropy Codec Design. In Proceedings of SPIE, Security and Watermarking of Multimedia Contents III, volume 4314, San Jose, CA, USA, 2001.

[5]. C.W. Richardo Identification of three dimensional

using Fourier descriptor objects of the boundary curve. IEEE vol. SMC- 4, Jule 1994.

REFERENCES

[1]. Alferov A.A., Zubkov A.YU., Kuzmin A.S. Cryptography, M.:Gelios ARB, 2001.
[2]. Volodin A.A., Mitko V.G., Spinko E.N. Video processing systems, video surveillance, Information security, M.: 2002. pp.34-47.
[3]. Ryabova L.V., Golembievskaya YU.G. Basic operators for image processing iris, Nauka i molod, K, NAU, 2006., №6. pp. 45-48.
[4]. Chung-Ping Wu and C.-C. Jay Kuo. Efficient Multimedia Encryption via Entropy Codec Design. In Proceedings of SPIE, Security and Watermarking of Multimedia Contents III, volume 4314, San Jose, CA, USA, 2001.
[5]. C.W. Richardo Identification of three dimensional using Fourier descriptor objects of the boundary curve. IEEE vol. SMC- 4, Jule 1994.

ЗАСОБИ ЗАХИСТУ ВІДЕОДАННИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У статті дано огляд існуючих методів її захисту. Наслідком розвитку відеотехнологій стало масове поширення випадків незаконного копіювання та перегляду відеоданих, – виникла проблема захисту відеоінформації. Зокрема, відеодані можуть поширюватися з порушенням авторських прав (піратство), а також до них можуть несанкціоновано звертатися конкуренти чи зловмисники для отримання конфіденційної інформації (шпигунство). Найпростіший підхід до захисту відеоданих – це використання класичного шифрування за схемами з відкритим чи закритим ключем. Файл відеоданих шифрується, після чого передається по незахищеному каналу зв'язку або записується на незахищений носій. Такий спосіб забезпечує досить високий ступінь захисту відеоданих, яка досягається високою стійкістю використовуваного для захисту шифру. Однак, найчастіше обсяг шифрованих даних у порівнянні з текстовими і навіть звуковими даними значно більше, що вимагає значних обчислювальних ресурсів для шифрування такого обсягу даних. Це призводить до обмеження можливості використання класичного шифрування в таких областях, як інтерактивне і кабельне телебачення. Користувач таких сервісів повинен мати потужну систему, здатну в реальному часі, без затримок розшифровувати, а потім і декодувати отримані дані. Оскільки основним стандартом, використовуваним для кодування і стиснення відеоінформації, є формат MPEG, то більшість способів захисту розроблені саме для цього формату. У них використовуються особливості кодування і структури потоку MPEG для скорочення обчислювальних ресурсів на захист відеоданих. Одним з перших способів захисту даних у форматі MPEG був алгоритм перестановки "зигзаг". Суть його полягає в зчитуванні квантованих коефіцієнтів дискретного косинусного перетворення не способом «зигзаг» для подальшого кодування, як це визначено в форматі, а випадковим чином. Розглянуто різні методи захисту відеоданих стосовно до телекомунікаційних систем реального часу. У наш час все більш актуальною стає проблема захисту відеоінформації. У статті запропоновано огляд існуючих методів її захисту.

Ключові слова: відеодані, захист відеоданих, несанкціонований доступ, кодування відеоінформації, шифрування даних, методи захисту відеоданих.

MODES OF PROTECTION OF VIDEO DATA FROM UNAUTHORIZED ACCESS

The paper reviews existing methods of protection of video. A consequence of the mass distribution of video technology has become illegal copying and viewing of video data - a problem of protection of video. In particular, video data can be distributed to copyright infringement (piracy), and these may refer unauthorized competitors or hackers to obtain sensitive information (espionage). The simplest approach to the protection of video data - is the use of classical encryption schemes open or secret key. Image data file is encrypted and then transmitted over the insecure communications channel or recorded on unprotected media. This method provides a very high degree of protection of video data is achieved by a high resistance used for protection cipher. Often, however, the amount of encrypted data over the text and audio data even considerably more, which requires significant computing resources to such encryption of data. This tends to limit the possibility of using classical encryption in areas such as interactive and cable TV. Users of these services should have a powerful system capable of real-time, without delays decoding, and then decode the received data. Since the main standard used to encode and compress video data format is MPEG, then most of the methods of protection designed specifically for this format. They use features and coding structure of MPEG to reduce the computational resources to protect the video data. One way to protect the first data in the MPEG algorithm was permutation «zigzag». Its essence consists in reading the quantized coefficients of discrete cosine transform method is not «zigzag» for subsequent encoding as defined format, randomly. Different methods of protection vidiodannyh applied to telecommunications systems real-time.

Index Terms: video data, the protection of video data, unauthorized access, video encoding, data encryption methods to protect the video data.

Рябова Любовь Владимировна, ассистент кафедры средств защиты информации Национального авиационного университета.
E-mail:ubanau@ukr.net
Рябова Любов Володимирівна, асистент кафедри засобів захисту інформації Національного авіаційного університету.

Lyubov Ryabova, Assistant Professor, Department of information security of the National Aviation University.

Подгорный Евгений Иванович, доцент Национального авиационного университета.
E-mail:ubanau@ukr.net
Подгорний Евгеній Иванович, доцент Національного авіаційного університету.
Evgeniy Podgornyy, Associate Professor, National Aviation University.

Мацуева Карина Андреевна, аспирант кафедры компьютеризованных систем управления Национального авиационного университета.
E-mail: kamatsueva@gmail.com
Мацуєва Карина Андріївна, аспірант кафедри комп'ютеризованих систем управління Національного авіаційного університету.
Karyna Matsueva, postgraduate, Department of Computerized Control Systems, National Aviation University.

УДК 621.327:681.5

МЕТОД КОДИРОВАНИЯ ДИНАМИЧЕСКИХ ИЗОБРАЖЕНИЙ СТАЦИОНАРНОГО ФОНА В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Владимир Баранник, Альберт Леках, Борис Остроумов

С целью повышения производительности инфокоммуникационных систем необходимо совершенствовать технологии сжатия динамических изображений. Поэтому обоснованы основные принципы построения метода сжатия динамических изображений стационарного фона в инфокоммуникационных системах на основе формирования дифференциально-представленного кадра. Для выявления динамической составляющей излагаются условия использования пороговой фильтрации дифференциально-представленного кадра. Разработана технология разбиения дифференциально-представленного кадра на составляющие: динамическую составляющую, двоичную маску стационарного фона и матрицу знаков. Рассмотрена технология обработки динамической составляющей, проводимая на основе одномерного позиционного кодирования с адаптивным выбором основания. Изложены основные этапы способа обработки двоичной маски дифференциально-представленного кадра, осуществляемая на основе кодирования по мощности двух алфавитов длин двоичных серий. Построена технология кодирования матрицы знаков, реализуемая на базе кодирования по мощности алфавита с учетом структурного подобия с матрицей двоичной маски. Показано, что разработанные методы кодирования обеспечивают потенциальные возможности для сокращения объема и дополнительного увеличения степени сжатия динамических изображений стационарного фона, что в целом приводит к сокращению времени на их обработку в инфокоммуникационных системах.

Ключевые слова: *дифференциально-представленный кадр, код мощности алфавита, двоичная маска предсказанного кадра, динамическая составляющая, стационарный фон.*

Введение. В рамках повышения безопасности управления железнодорожным (ЖД) транспортом актуальным является совершенствования технологий объективного контроля. В этой связи расширяется использование видеоинформационных средств видеоконтроля [1-3]. С одной стороны это позволяет повысить качество мониторинга. С другой стороны такое направление сопровождается рядом трудностей. Наиболее проблематичный аспект состоит в ограниченной пропускной способности инфокоммуникационных систем. В связи с чем, передача больших объемов видеоданных сопровождается временными задержками. Для повышения производительности инфокоммуникационных систем необходимо применять методы обработки (кодирования) изображений. Это позволит уменьшить объем данных, которые передаются по каналам связи. Однако существующие технологии компрессии видеопотока не обеспечивают требуемой степени сжатия в условиях повышенной разрешающей способности видеопотока и высоких требований относительно достоверности получаемой информации. Все это усложняется условиями проведения мониторинга железнодорожного транспорта, а именно ростом скоростей ЖД составов. Отсюда дополнительно необходимо повышать частоту кадров. В результате растет нагрузка на каналы связи. Поэтому необходимо совершенствовать технологии сжатия динамических изображений. Вариант такого развития заключается в учете особенностей видеомониторинга на транспорте. Здесь предлагается учитывать то, что видеопоток формируется в