ЗАХИСТ ІНФОРМАЦІЇ

УДК 681.3

А.В. Яковенко,
кандидат технических наук,
старший научный сотрудник,
В.В.Ларин,
кандидат технических наук,
Р.В. Тарнополов

ПОДХОДЫ ДЛЯ ЗАЩИТЫ ВИДЕОИНФОРМАЦИИ НА ОСНОВЕ УСТРАНЕНИЯ ИЗБЫТОЧНОСТИ В ИНФОКОММУНИКАЦИЯХ

У статті запропоновані варіанти позиціонування процесів стиснення і шифрування. Можливі такі стратегії захисту відеоінформації: попереднє шифрування, шифрування в процесі стиснення, шифрування стиснених відеоданих. Був проведений аналіз запропонованих підходів, розкрито їх особливості та недоліки. На основі запропонованих варіантів був введений показник, що характеризує процес захисту зображень на базі стандартів стиснення.

Ключові слова: *захист відеоінформації, стиснення зображень.*

В статье предложены варианты позиционирования процессов сжатия и шифрования. Возможны следующие стратегии защиты видеоинформации: предварительное шифрование, шифрование в процессе сжатия, шифрование сжатых видеоданных. Был проведен анализ предложенных подходов, раскрыты их особенности и недостатки. На основе предложенных вариантов был введен показатель, характеризующий процесс защиты изображений на базе стандартов сжатия.

Ключевые слова: *защита видеоинформации, сжатие изображений.*

Paper suggests the ways of the positioning of compression processes and encryption. The following protection strategies of videoinformation are possible: advanced encryption, encryption in the process of compression, encryption of the compressed video data. Analysis of the proposed approaches was carried out, features and lacks are revealed. On the basis of the proposed options an indicator characterizing the process of the protection based on the image compression standards was introduced.

Keywords: *protection of videoinformation, image compression.*

Введение

Видеоинформация приобретает значение важного ресурса, влияющего на национальную безопасность, безопасность коммерческих структур и соблюдения прав личности, определяет уровень экономического развития государства, его оборонный потенциал, формирование общественного мнения.

Расширяются области приложений, для которых видеоинформация становится информационным ресурсом, не подлежащим обязательному разглашению, и содержащей в себе [2–5]:

– информацию, которая является собственностью государства;

– информацию с ограниченным доступом;

– информацию об оперативной и следственной работе органов прокуратуры, МВД, СБУ;

– информацию, которая касается личной жизни граждан;

– сведения, по которым принимается решение на ведение боевых действий (аэрофотосъемка).

Значит, требуется обеспечить безопасность и защиту видеоинформации от несанкционированного пользователя.

Под безопасностью видеоинформационного ресурса будем понимать обеспечение конфиденциальности, целостности и доступности источников видеоданных.

Однако, в отличие от других информационных ресурсов, видеоинформация обладает рядом характерных свойств, а именно:

– объемы видеоинформации по сравнению с другими видами информации достигают сотен мегабит и более;

– наличие разных типов избыточности;

– восприятие видеоинформации обусловлено психофизическими особенностями зрительной системы человека;

– наличие многомерных связей в обрабатываемых данных.

В связи с этим, при обработке и передаче видеоинформации с использованием инфокоммуникационных систем возникают следующие трудности:

1) повышается нагрузка на информационно-телекоммуникационные сети;

2) увеличивается задержка передачи обработанного информационного ресурса;

3) происходит потеря информационных пакетов в каналах передачи данных.

Поэтому требуется наряду с защитой видеоинформации обеспечить требуемые:

– оперативность доставки видеоинформации;

– достоверность (качество) получаемого видеоинформационного ресурса.

Значит, существует проблема, которая состоит в обеспечении заданного уровня защиты видеоинформации с выполнением требований по оперативности доставки и необходимой достоверности ее восстановления.

Вариантом решения данной проблемы является обеспечение защиты видеоинформации с использованием технологии компрессии [1–7]. Это позволит сократить объем информации, которая поступает на обработку, и повысить качество восстановленных изображений.

Однако существующие подходы для реализации данного направления не систематизированы. Также отсутствует аппарат оценки эффективности таких методов. В связи с этим, цель исследований состоит в разработке методологии оценки эффективности технологий защиты информации на базе стандартов сжатия изображений.

Основная часть

Рассмотрим оценку характеристик процесса защиты видеоинформации для информационно-коммуникационных систем. Для этого введем критерии, характеризующие временные показатели и показатели информационной скрытности обрабатываемой видеоинформации.

Информационная скрытность обрабатываемых изображений вычисляется по следующим показателям:

Безопасное время $T_б$

$$T_б = \min_{1 \le i \le M} \{T_{б_i}\}. \quad (1)$$

Здесь $T_{б_i}$ – безопасное время функционирования алгоритма, реализующего i-й метод криптоанализа, оцениваемое как $T_{б_i} = S_{б_i} / \phi S_{обр}$; $S_{б_i}$ – временная сложность алгоритма, реализующего i-й метод криптоанализа; $S_{обр}$ – производительность вычислительной системы, имеющейся в распоряжении противника.

Мера информационной скрытности, определяемая как вероятность $P_{інф}$ достоверного дешифрирования (распознавания) изображения, состоящая из:

1) вероятности $P_к$ правильного восстановления секретных ключевых данных:

$$P_к = \max_{1 \le i \le M} \{P_{к_i}\}; \quad (2);$$

2) вероятности $P_и$ правильного восстановления открытого текста

$$P_и = \max_{1 \le i \le M} \{P_{и_i}\}. \quad (3).$$

Здесь $P_{к_i}$, $P_{и_i}$ – вероятности правильного восстановления секретной ключевой части и открытой информационной части, в случае использования злоумышленником i-го метода криптоанализа.

Для варианта обработки изображений величина $P_{інф}$ прямо пропорциональна значению $h_н$ пикового отношения сигнал/шум в случае несанкционированного доступа, т.е. $P_{інф} \sim h_н$.

$$h_н = 20\ell g\left(\frac{255}{\sqrt{\sum_{i=1}^{L_{стр}} \sum_{j=1}^{L_{стб}} (a_{ij} \quad a'_{ij})^2 / \; L_{стр} \; L_{стб}}}\right), \quad (4)$$

где a_{ij}, a'_{ij} – соответственно исходное значение и значение (i; j)-го элемента в случае несанкционированного доступа, $L_{стр}$ – размер строки фрагмента изображения, $L_{стб}$ – размер столбца фрагмента изображения.

С учетом ограничений на степень потерь качества восстановленных изображений должно выполняться неравенство $h \geq h_з$, где $h_з$ – заданное значение пикового отношения сигнал/шум.

Показатель оперативности характеризует время обработки видеоданных $T_{обр}$, включающее этапы прямого $T_{шд}$ и обратного $T_{дшд}$ криптографического шифрования. Время шифрования определяется производительностью вычислительной системы и количеством операций, затрачиваемых на шифрование. С учетом шифрования суммарное время T доставки видеоинформации определяется по формуле:

$$T = T_{обр} + T_{пш}, \quad (5)$$

где $T_{обр}$ – время обработки, содержащая

$$T_{обр} = T_{шд} + T_{дшд}. \quad (6).$$

Здесь $T_{пш}$ – передача шифрованных данных по информационно- коммуникационной системе.

Суммарное время T обработки и передачи данных находится по формуле:

$$T = T_{сд} + T_{вд} + T_{шсд} + T_{дсд} + T_{псш}, \quad (7)$$

где $T_{д}$ – время сжатия данных; $T_{вд}$ – время восстановления данных; $T_{шсд}$ – время на шифрование сжатых данных; $T_{дсд}$ – время дешифрования компактно представленных данных; $T_{псш}$ – время на передачу данных.

$T_{дсд}$ и $T_{вд}$ зависит от колличества операций необходимых для выполнения полного цикла и производительности вычислительной системы.

Одним из основных параметров, влияющих на время выполнения любого преобразования, является количество элементарных операций, необходимых для выполнения этих преобразований.

В общем случае время выполнения любого преобразования $T_{преобр}$ определяется отношением общего объема обрабатываемых данных $W_д$ к быстродействию этого преобразования $V_{преобр}$ по формуле:

$$T_{преоб} = \frac{W_{сд}}{V_{преоб}}, \quad (8)$$

где $V_{преобр}$ – скорость выполнения преобразования, которая определяется по формуле:

$$V_{преоб} = \frac{V_{проц}}{Q} W_{блока}, \quad (9)$$

где $V_{преобр}$ – производительность вычислительной системы (тактовая частота процессора);

Q – количество элементарных операций (инструкций), необходимых для выполнения преобразования;

$W_{блока}$ – размерность блока, обрабатываемых преобразованием данных.

Производительность вычислительной системы (тактовая частота процессора) $V_{проц}$ расчитывается по формуле:

$$V_{проц} = R_р = F_р n_р n_{такт} 10^{-6}, \quad (10)$$

где $R_р$ – пиковая производительность; $F_р$ – частота процессора (ядра процессора), МГц; $n_р$ – количество процессоров или ядер в процессоре; $n_{такт}$ – количество инструкций (команд) процессора, выполняющихся за один такт.

Пиковая производительность измеряется в терафлопсах (TFLOPS) и показывает, сколько операций в секунду выполняет данная вычислительная система.

Время передачи данных $T_{псш}$ зависит от характеристик изображения, от применяемого метода компрессии, от возможностей инфокоммуникационных систем, в которых происходит обработка видеоинформации.

В результате использования технологий компрессии объем $W_{сд}$ шифруемых данных и время передачи $T_{псш}$ по каналам связи уменьшается на величину коэффициента сжатия k, а именно:

$$W_{сд} = W_{ид} / k; \quad (11)$$

$$T_{псш} = T_{пш} / k. \quad (12)$$

Однако в процессе защиты видеоинформации изображения изменяют свои структурные характеристики вплоть до их утраты. Это приводит к снижению степени сжатия. Вследствие этого происходит увеличение нагрузки на сеть передачи данных из-за неуменьшения исходных объемов, увеличения времени на обработку и передачу информации. Поэтому важным показателем, характеризующим процесс защиты изображений на базе стандартов сжатия, является показатель, оценивающий потери степени сжатия, а именно: коэффициент потери степени сжатия в обрабатываемых данных, который расчитывается по формуле:

$$k_{пот} = \frac{k}{k'}, \quad (13)$$

k – показатель, характеризующий степень устранения избыточности без ее шифрования, то есть без изменения свойств изображений.

k' – показатель, характеризующий степень устранения избыточности в условиях возможных изменений характера выявленных закономерностей изображений по причине ее шифрования.

Этот коэффициент показывает степень нарушения закономерностей в обрабатываемых данных в связи с использованием криптографических средств защиты в процессе сжатия. Также он характеризует степень повышения неопределенности видеоинформации вследствие процесса шифрования.

В зависимости от вариантов позиционирования процессов сжатия и шифрования, возможны следующие стратегии, представленные на рисунке 1.

Рисунок 1. Стратегии защиты видеоинформации

Рассмотрим стратегию защиты видеоинформации на основе предварительного шифрования данных. Структурная схема представлена на рисунке 2.

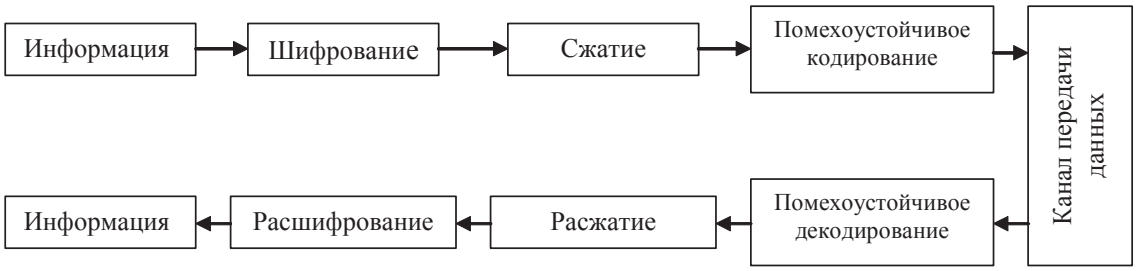

Рис. 2. Структурно-функциональная схема составляющих процесса защиты видеоинформации до сжатия

При предварительном шифровании возникает ряд трудностей, а именно:

– наличие значительного количества избыточности изображений, что дает дополнительную информацию криптоаналитику;

– большой объем информации поступает на шифрование, а значит, растет время обработки;

– в процессе сжатия вносятся безвозвратные потери информации, это разрушает используемые шифры;

– резко снижается эффективность сжатия вследствие разрушения характерных для исходного изображения закономерностей. Это приводит к снижению оперативности передачи данных в информационно-коммуникационных сетях.

Следующим подходом защиты видеоинформации является шифрование сжатых видеоданных. В этом случае информацией, поступающей на шифрование, будут компактно представленные изображения (рис. 3).

К положительным сторонам защиты видеоинформации после сжатия можно отнести:

– исходный объем обрабатываемой информации уменьшается вследствие сжатия;

– большое количество избыточности видеоданных устранено;

– информация, которая используется для стегоанализа, уменьшена.

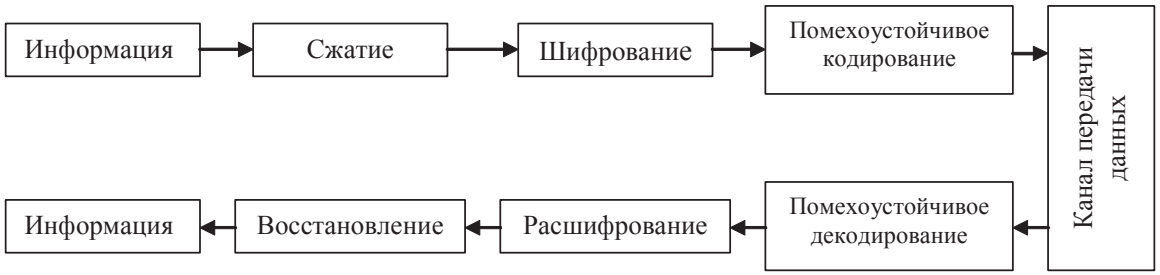

Рис. 3. Структурно-функциональная схема составляющих процесса защиты видеоинформации после сжатия

Рассмотрим особенности использования механизмов защиты видеоинформации после сжатия. К таковым относятся:

а) сжатые видеоданные, содержащие большое количество остаточной избыточности разных видов (в первую очередь, психовизуальную и структурную избыточности), а их структура и содержание сохраняет значительную информацию об исходных изображениях, что создает дополнительные возможности для проведения криптоанализа;

б) временные затраты на доведение конфиденциальных видеоданных, представленных в компактном виде, с заданным качеством реконструкции , достигают нескольких десятков секунд. При этом до 80 % от общего времени доведения отводится на обработку изображений.

Но суммарное время на обработку достигает десятков секунд и не всегда существующие вычислительные мощности позволяют выполнять обработку и доведение оперативной видеоинформации с заданным уровнем конфиденциальности.

Поэтому для устранения описанных недостатков предлагается третий вариант – шифрование в процессе сжатия.

Шифрование в процессе сжатия – это процесс использования методов защиты на разных этапах сжатия во временной и спектральной областях.

Выводы

Таким образом, были рассмотрены варианты позиционирования процессов сжатия и шифрования. Возможны следующие стратегии защиты видеоинформации: предварительное шифрование, шифрование в процессе сжатия, шифрование сжатых видеоданных.

На сегодняшний день существует множество способов защиты цифровых изображений в формате JPEG. Они, в зависимости от поставленной задачи (нужны ли высокая защищенность или компромисс между стойкостью и скоростью обработки), позволяют выбрать оптимальное решение. Общей особенностью рассмотренных способов защиты является то, что они основаны на принципах классического шифрования – перестановках и заменах. В связи с развитием вычислительной техники эти методы становятся неэффективными вследствие увеличения времени на обработку, снижения коэффициента сжатия и недостаточной стойкости защищенных данных. Отсюда следует: необходимо разрабатывать принципиально новые методы и подходы к защите цифровых данных в процессе сжатия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Баранник В.В.* Модель лавинно-связывающего эффекта в процессе реконструкции изображений в комбинированных криптосемантических системах на базе полиадического представления / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2010. – № 4(23). – С. 45–51.

2. *Ларин В.В.* Обоснование проблемных недостатков систем сжатия относительно построения сложностно-дешифрируемых преобразований / В.В. Ларин, С.А. Сидченко, В.В. Баранник // Современные проблемы математического моделирования, прогнозирования и оптимизации : 4 междунар. науч. конф. (Каменец-Подольск, 18–20 мая 2010 г.) / Каменец-Подольск : Каменец-Подольский национальный университет имени Ивана Огиенко. – 2010. – С. 248.

3. *Ватолин В.И.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В.И. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. – М. : ДИАЛОГ – МИФИ, 2002. – 384 с.

4. *Ахмед Н.* Ортогональные преобразования при обработке цифровых сигналов / Н. Ахмед, К.Р. Рао; пер. с англ. под ред. И.Б. Фоменко. – М. : Связь, 1980. – 248 с.

5. *Баранник В.В.* Метод маскування відеоінформації на основі систем компресії / С.А. Сидченко, В.В. Ларин // Інформаційні технології : Наука, техніка, технологія, освіта, здоров'я (MicroCAD-2011) : XIX міжнар. наук.-практ. конф. (Харків, 2011 р.) / Харків : Харківський національний технічний університет "ХПІ", 2011. – С. 58.

6. *Володин А.А.* Обработка видео в системах телевизионного наблюдения / А.А. Володин, В.Г. Митько, Е.Н. Спинко // Вопросы защиты информации. – М. : 2002. – С. 34–47.

Отримано 30.04.2014