УДК 681.3

МЕТОДОЛОГИЧЕСКАЯ БАЗА КРИПТОКОМПРЕССИОННОГО ПРЕДСТАВЛЕНИЯ ВИДЕОИНФОРМАЦИОННЫХ РЕСУРСОВ

Владимир Баранник, Сергей Сидченко, Владимир Ларин

Развитие технологий представления видеоинформационного обеспечения и его интеграция в разные сферы деятельности общества требует повышения эффективности защиты видеоданных, доведение которых необходимо в реальном времени. Существующие технологии защиты видеоданных от несанкционированного доступа основаны на последовательном выполнении операций сжатия и шифрования или схеме так называемого выборочного шифрования, использующие особенности кодирования и структуры потока MPEG для сокращения вычислительных ресурсов на защиту видеоданных. Недостатком последовательной схемы является потребность в значительных вычислительных ресурсах или временные задержки при обработке и передачи, а недостатком выборочного шифрования – более низкая защищенность данных. Рассмотрены потенциальные возможности защиты оперативной видеоинформации в направлении построения стойких к несанкционированной дешифровки (распознавания) изображений на базе систем компактного представления, т.е. обеспечение скрытности видеоинформации на уровне кодирования ее источников. Излагаются основные компоненты разработки методологической базы криптокомпрессионного представления видеоинформационных ресурсов. Приводятся базовые определения криптокомпрессионного представления, вводится новое научно-прикладное направление – "Теория криптокомпрессии". Даются основные направления научно-прикладных исследований, проводимых в данной области знаний. Формируется методологическая база составляющих криптокомпрессионного построения видеоданных.

Ключевые слова: *криптокомпрессионное представление, защита видеоинформации, компактное представление, видеоинформационный ресурс, методологические основы.*

Введение. Развитие технологий представления видеоинформационного обеспечения и его интеграция в разные сферы деятельности общества выводит такую составляющую, как видеоинформационный ресурс, на новый уровень значимости. В связи с чем становится актуальным вопрос об организации безопасности видеоинформации. В тоже время, как показано в роботах [1–3] существующие информационные технологии не справляются с увеличенными объемами видеоданных относительно ее своевременной доставки, защиты в условиях обеспечения гарантированной целостности информации. Поэтому актуальным есть направления развития технологий защиты видеоинформации с использованием методов цифровой обработки изображений.

Для повышения эффективности защиты видеоинформации, доведение которой необходимо в реальном времени, возможны два направлений, а именно [1]:

1. Проводить модификацию существующих технологий компрессии и криптографических преобразований с позиции последовательного выполнения операция сжатия и шифрования.

2. Разработать принципиально новый подход, который заключается в создании технологий, которые одновременно обеспечивают повышение оперативности доведения и защиты видеоинформации на основе методов семантической и синтаксической обработки изображений.

Первое направление с позиции последовательного выполнения операция сжатия и шифрования широко изучено и используется на практике [4]. При этом исходят из позиции, что видеоданные ничем не отличаются от других данных. Их рассматривают как определенным образом структурированный набор битов. И как следствие, для защиты видеоданных используют классическое шифрование по схемам с открытым или закрытым ключом. На шифрование подаются либо исходные видеоданные, либо их сжатое представление. Этот подход с одной стороны обеспечивает высокую степень защиты видеоданных, а с другой – требует значительные вычислительные ресурсы для шифрования, поскольку объем видеоданных значительно больше других типов данных.

Для снижения требований к вычислительным ресурсам была предложена схема так называемого выборочного шифрования, имеющая много модификаций [4, 5]. Этот класс методов защиты заключается в шифровании только ключевых битов или блоков битов видеоданных. 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. Не-

достатком метода является более низкая защищенность данных, однако скорость шифрования/дешифрирования данных значительно увеличивается по сравнению с полным шифрованием.

Второе направление повышения защиты оперативной видеоинформации является принципиально новым и заключается в создании систем информационной скрытности путем построения методов стойких к несанкционированной дешифровке (распознаванию) изображений на базе систем их цифровой обработки.

В пользу выбора данного направления указывает наличие следующих потенциальных преимуществ:

– обеспечивается сокращение объемов видеоданных, передаваемых с использованием инфотелекоммуникационных систем;

– разработка процессов сжатия и шифрования рассматривается как единый этап обработки, что исключает необходимость в организации их совместимости и согласованности;

– исключается возможность несанкционированного доступа к видеоинформации после этапа компрессии;

– существует возможность учитывать для обеспечения информационной скрытности особенности семантического содержания изображений и психовизуального восприятия их зрительной системой. В том числе учитывать и тот факт, что шифрование осуществляется одинаково для всех частей фрагмента изображения, т.е. затрачивается одинаковое количество операций для всех блоков изображения. В то время как разные блоки несут различное количество семантической нагрузки, т.е. разные блоки изображения имеют различную важность и ценность информации. Учет такой семантической неоднородности блоков изображения позволяет сократить вычислительные затраты. Это можно сделать с помощью методов кодирования источников изображений;

– сокращается время обработки за счет слияния двух этапов в один.

Потому целью статьи будет рассмотрение потенциальной возможности защиты оперативной видеоинформации в направлении построения стойких к несанкционированной дешифровки (распознавания) изображений на базе систем компактного представления, т.е. обеспечение скрытности видеоинформации на уровне кодирования ее источников.

Основной материал. Такой подход предполагает создание технологий, обеспечивающих одновременно и сокращение избыточности и защиту видеоинформации. Это делает создание стойкие к несанкционированной дешифровке – представления изображений на базе систем компрессии на уровне кодирования их источника одним из ключевых вариантов организации защиты видеоинформации [2–3]. В связи с чем, введем понятие «Криптокомпрессионного представления».

Определение 1. Криптокомпрессионным представлением видеоданных называется такое криптосемантическое представление, для которого семантически маскирующие преобразования строятся на базе технологий и методов сжатия изображений.

Процессы сжатия позиционируются на уровне кодирования источников. Основной теоретической базой для создания таких методов являются теоретические положения теории информации и кодирования. С другой стороны положения теории криптографии формируют базовую составляющую относительно обеспечения скрытия видеоданных. Поэтому применительно криптокомпрессии допускается использование таких терминов как кодирование и шифрование.

Криптокомпрессионным преобразованием (кодированием, шифрованием) являются такие сжимающие преобразования (кодирование, шифрование), которые обеспечивают гарантированную стойкость относительно несанкционированного доступа к скрытым изображениям.

Методами криптосемантического преобразования являются методы, одновременно обеспечивающие маскировку семантического содержания изображений и их компактное представление для повышения уровня конфиденциальности видеоинформации и оперативности ее доставки в инфокоммуникационных системах.

Рассмотрим более подробно основные определения относительно криптокомпрессионного кодирования (шифрования).

Пусть заданы два конечных множества $A=\{a_1,a_2,...,a_M\}$ и $C=\{c_1,c_2,...,c_g\}$, где, как правило $M>g=2$. Из элементов $a_k\in A$, где $k=\overline{1,M}$ составим последовательности $a'_j=\{a_1^{(j)};a_2^{(j)};...;a_{m_j}^{(j)}\}$, $j=\overline{1,N}$ длиной m_j, образующих множества последовательностей $A'=\{a'_1,a'_2,...,a'_N\}$. В частном случае $m_j=1$.

Из элементов $c_l\in C$, $l=\overline{1,g}$ составим последовательности $c'_j=\{c_1^{(j)};c_2^{(j)};...;c_{q_j}^{(j)}\}$ длиной q_j, образующие множество последовательностей $C'=\{c'_1,c'_2,...,c'_N\}$.

Определение 2. Правило ϕ задающее однозначное отображение множества последовательностей $A'=\{a'_1, a'_2,\dots,a'_N\}$ на множество последовательностей $C'=\{c'_1, c'_2,\dots,c'_N\}$ называется кодированием.

Определение 3. Если кодовая комбинация $c'_j \in C'$ ставится в соответствие исходной последовательности $a'_j \in A'$, так, что достигается уменьшение объема цифрового представления, т.е. $W(c'_j) \le W(a'_j)$, то такое кодирование называется сжимающим кодированием.

Соответственно правило φ такого отображения называется оператором сжимающего кодирования.

Определение 4. Когда кодовая комбинация $c'_j \in C'$ ставится в соответствие исходной видеопоследовательности $a'_j \in A'$ на основе правила сжимающего кодирования φ, так, что достигается уменьшение объема цифрового представления, и обеспечивается гарантированная конфиденциальность видеоинформации, то такое сжимающее кодирование называется криптокомпрессионным кодированием (шифрованием).

Соответственно отображение φ называется криптокомпрессионным.

Последовательности a'_j называют открытыми видеосообщениями или криптокомпрессируемыми последовательностями, а c'_j – криптокомпрессионными кодовыми последовательностями или криптокомпрессиограммами. При этом если исходная последовательность $a'_j \in A'$ отображается в последовательность c'_j, $c'_j \in C'$, то c'_j называется криптокомпрессионным кодом последовательности a'_j, $a'_j \in A'$. Элементы $a_k \in A$ называют элементами видеосообщений, а элементы $c_l \in C$ – элементами криптокомпрессионного представления.

Создание криптокомпрессионного представления видеоизображений можно трактовать как обеспечение устойчивости защиты относительно несанкционированного дешифрирования информативных семантических признаков изображений в пространстве компрессионных кодов.

Кодограммами криптокомпрессионного описания являются такие кодовые конструкции, которые формируются в результате криптокомпрессионного кодирования, и обеспечивают скрытие семантического содержания или дешифровочных признаков компактно-представленных изображений.

При построении криптокомпрессионного представления необходимо обеспечить следующее:

– стойкость к несанкционированному дешифрированию;

– заданный уровень компрессии изображений с различной степенью насыщенности мелкими деталями и контурами;

– механизмы семантического маскирования не должны снижать степень сжатия изображений;

– требуемое качество восстановленных изображений;

– приемлемую вычислительную сложность реализации, т.е. количество шагов или арифметико-логических операций, необходимых для прямого и обратного криптокомпрессионного преобразований;

– заданную пропускную способность криптокомпрессионного канала;

– требуемую скорость битового потока с учетом задержек на формирование криптокомпрессионного представления;

– подлинность и целостность скрываемой видеоинформации для авторизованного пользователя.

Теория криптокомпрессии как новое научно-прикладное направление является составной составляющей теории криптосемантики, и строится на стыке положений следующих теорий, а именно (рис. 1):

– теории криптографической защиты информации;

– теории информации и кодирования;

– теории сжатия цифровых видеоизображений;

– теория фильтрации, локализации и детектирования объектов;

– теории дешифрирования видеоизображений.

Методологические основы построения теории криптокомпрессионного представления видеоизображений на основе положений базовых теорий рассматриваются на рис. 2.

Криптокомпрессионные преобразования должны включать в себя следующие направления:

– скрытие семантического содержания изображения с целью обеспечения гарантированной конфиденциальности;

– повышение оперативности обработки и передачи скрытых изображений;

– установление факта модификации кодовой конструкции;

– компрессию изображений без внесения дополнительных потерь информации.

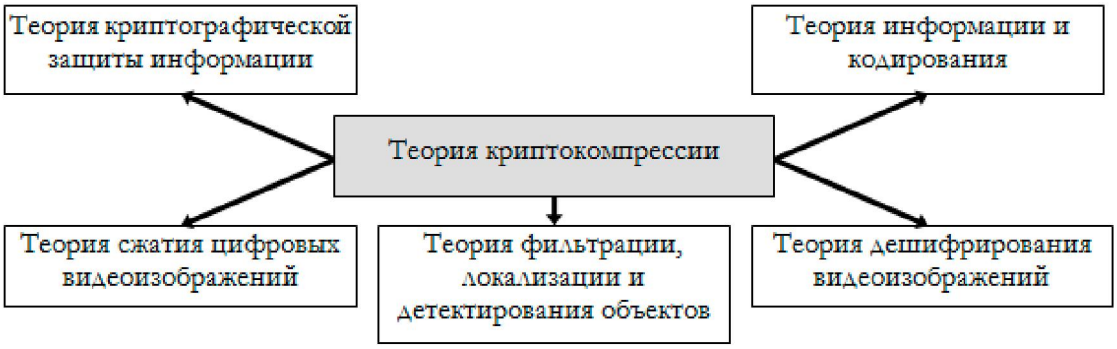

Рис. 1. Структура строения теории криптокомпрессии

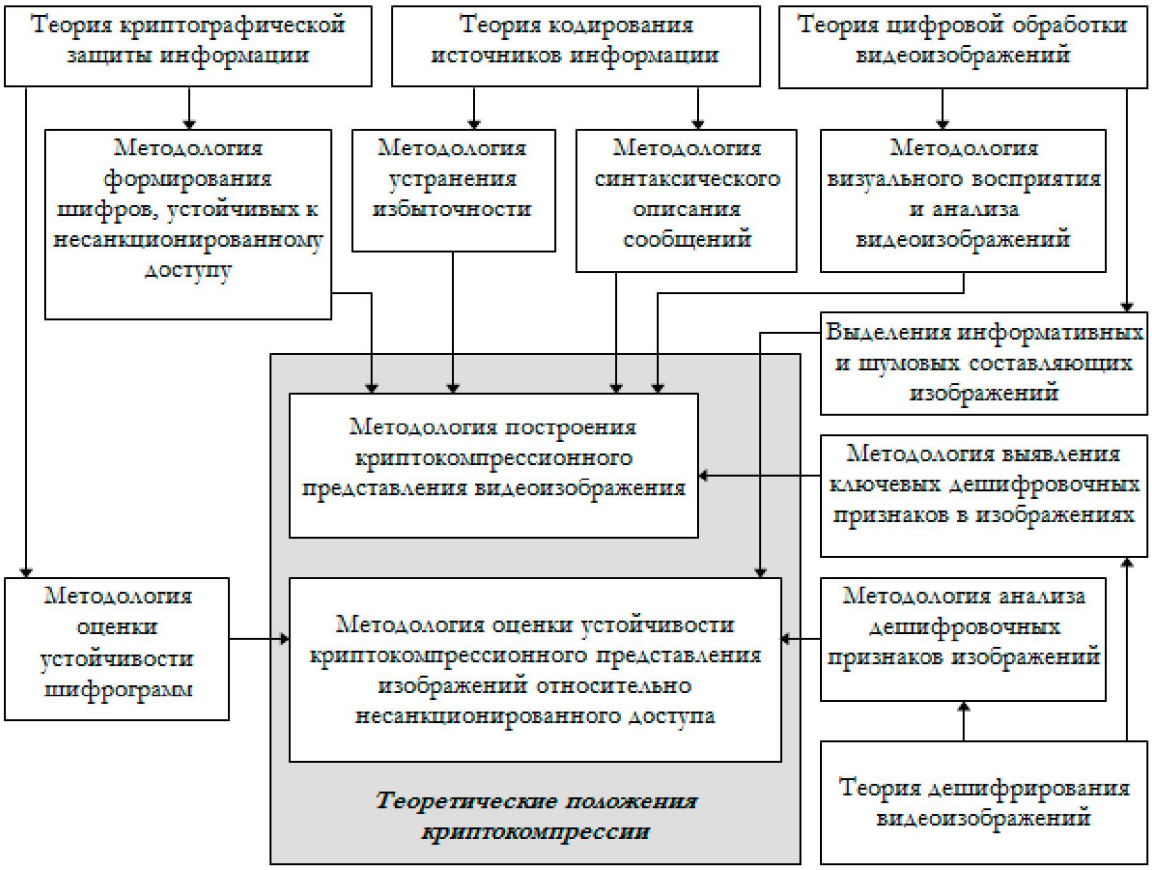

Рис. 2. Схема построения методологических основ криптокомпрессии видеоизображений

В зависимости от сферы использования методов криптокомпрессионного представления для них могут добавляться дополнительные требования. Например, связанные с обеспечением устойчивости к ошибкам в процессе передачи данных по каналам связи, устойчивость к потере пакетов, экономия энергозатрат, ограниченными вычислительными возможностями.

В соответствии с чем, криптокомпрессия применяется для решения таких важных проблем, как:

– обеспечение безопасности видеоинформационных ресурсов, в том числе в отличии от классической криптографии дополнительного обеспечения целостности относительно угроз, связанных с ошибками канала связи, сжатия, потерями пакетов и данных;

– повышение оперативности обработки и доставки видеоинформации с использованием инфокоммуникационных систем;

– увеличение уровня достоверности видеоинформации;

– локализация и идентификация семантически значимых признаков изображений.

В случае доставки видеоинформационных ресурсов с использованием беспроводных технологий их скрытие на основе криптокомпрессионного представления достигается на следующих уровнях (рис. 3):

1. Энергетическая скрытность – выполняется комплекс мероприятий, направленных на исключение или существенное затруднение выявления сигналов систем беспроводной связи приемником злоумышленника.

С использованием криптокомпрессии энергетическая скрытность обеспечивается за счет того, что:

– сокращается битовое описание, а следовательно снижаются энергетические затраты на передачу сигнала;

– в случае попытки несанкционированной реконструкции видеофрагмента может осуществляться эффект пропадания значительной части кадра.

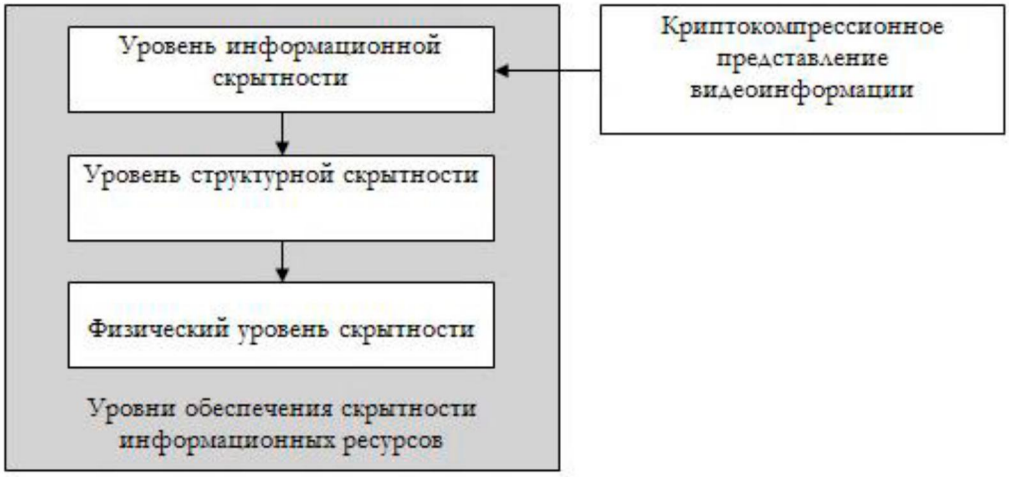

Рис. 3. Позиционирование криптокомпрессионной системы в системе скрытия видеоинформации

2. Структурная скрытность. Здесь подразумевается исключение или существенное осложнение распознавания структуры и параметров сигналов систем беспроводной связи. Структура сигнала определяется видом модуляции, которая используется в системе и типом кодировки сигналов. Показателем эффективности структурной скрытности является достоверность распознавания структуры сигнала при условии, что он обнаружен. Количественным параметром, который оценивает структурную скрытность, есть число измерений, которые необходимо провести, чтобы раскрыть структуру сигнала. Такой тип скрытности для криптокомпрессионного представления достигается за счет:

– изменения структуры первоначального видеосигнала в результате нелинейных преобразований. Даже используя обычную кодировку импульсов цифрового сигнала за счет предварительных нелинейных преобразований достигается изменение структуры первоначального сигнала;

– методы, лежащий в основе построения криптокомпрессионных технологий могут быть универсальными, в том смысле, что допускают свое использование для произвольных типов информации. В случае использования криптокомпрессии для сформированного видеосигнала сжатого образа (например, для JPEG-сжатого образа) происходит изменение его структуры;

– разделение исходного сигнала на шифрованную низкочастотную составляющую и высокочастотную интегрированную составляющую, распознавание которой зависит от знания зашифрованной низкочастотной составляющей.

Данные механизмы обеспечивают повышение сложности распознавания сигнала в случае, когда он обнаружен.

3. Информационная скрытность, определяется способностью систем беспроводной связи противостоять мероприятиям, направленным на раскрытие передаваемой с ее помощью информации. Мерой информационной скрытности является достоверность распознавания сообщения, которое передается. Информационная скрытность путем использования криптокомпрессионного представления обеспечивается на уровне скрытия как синтаксиса кодовых конструкций (количественная сторона информации), так и скрытия семантического содержания (качественной сторона информации) изображения.

4. Скрытность по времени. Здесь подразумевается тот факт, что чем большим временным ресурсом располагает злоумышленник относительно доступа к сигналу, тем большее количество шифрограмм закрытых фрагментов будет накоплено. Отсюда более успешным будет криптоанализ. В то же время в результате криптокомпрессии достигается сокращения объема видеоданных, следовательно, сокращается количество

закрытых кодовых конструкций. Поэтому за фиксированный временной ресурс будут перехвачено меньшее количество шифрограмм.

С другой стороны для криптокомпрессионных преобразований за счет уменьшения объемов сокращается количество видеоданных, закрытых одним ключом. Это снижает возможность проведения успешного криптоанализа, базирующегося на накоплении критического объема закрытых сообщений [3].

Для оценки семантической скрытности изображений в случае использования подхода, базирующегося на компрессии видеоданных на уровне источника информации, требуется задействовать факт наличия влияния синтаксического описания изображения на вероятность правильного распознавания объектов и сцен изображения, т.е. на вероятность правильного дешифрирования семантической составляющей

$$P(A_{сем};\ N(A_{син}))_{дш} \to 0, \qquad (1)$$

и будет трактоваться как то, что вероятность правильного дешифрирования семантического содержания открытого фрагмента $A_{сем}$ по преобразованному на синтаксическом уровне формату $N(A_{син})$ должна стремиться к нулю. Очевидно также то, что

$$P(A_{сем};\ A_{син})_{дш} = 1, \text{ и}$$
$$P(A_{сем};\ N(A_{син}) |\ V(N(A_{син})) = 0)_{дш} = 0,$$

где $V(N(A_{син}))$ – количество информации в преобразованном фрагменте $N(A_{син})$.

Причем для варианта реализации функционала $f_{ск}(A_{син})$ на основе систем кодирования источника изображений может выполняться условие, когда количество информации преобразованного фрагмента будет меньше, чем количество информации исходного (открытого) фрагмента, т.е.

$$V(N(A_{син})) \le V(A_{син}). \qquad (2)$$

Предложенный подход допускает использование для оценивания меры различия семантических содержаний открытого и преобразованного фрагмента, количественных показателей относительно степени расхождения соответствующих форматов описания на синтаксическом уровне фрагмента. Такими мерами расхождения могут быть:

1) среднеквадратический показатель $\delta(A_{син};\ N(A_{син}))$ отклонения преобразованного (скрытого) изображения от исходного (открытого)

$$\delta(A_{син};\ N(A_{син})) = \sqrt{\frac{\sum_{i=1}^{L_{стр}}\sum_{j=1}^{L_{стб}} (a_{i,j} - [b]_{10}^{(d)})^2}{L_{стр}\ L_{стб}}}, \qquad (3)$$

где $a_{i,j}$ – элемент исходного изображения (цветовой плоскости); b_{ξ} – значение двоичного разряда преобразованного формата $N(A_{син})$; $[b]_{10}^{d}$ – десятичное отображение значения, содержащегося в двоичной последовательности длиной d бит, $[b]_{10}^{d} = [b_1, \ldots, b_{\xi}, \ldots, b_d]_{10}$. Обычно $d=8$ бит.

2) пиковое отношение $h(A_{син};\ N(A_{син}))$ сигнал/относительное расхождение, как для всего изображения, так и для локализованной информативной области

$$h(A_{син};\ N(A_{син})) = 20\,\ell g \sqrt{\frac{\sum_{i=1}^{L_{стр}}\sum_{j=1}^{L_{стб}} a_{i,j} / |a_{i,j} - [b]_{10}^{(d)}|}{L_{стр}\ L_{стб}}}. \qquad (4)$$

Чем меньше величина $h(A_{син};\ N(A_{син}))$, тем выше степень скрытности преобразованного фрагмента;

3) количество информации в преобразованном формате $N(A_{син})$ об открытом (исходном) фрагменте $A_{син}$.

Выводы:

1. Описан процесс криптокомпрессионного кодирования (шифрования). Представлено его математическое описание.

2. Введено новое научно-прикладное направление – "Теория криптокомпрессии". Описаны уровни скрытности видеоинформационных ресурсов.

3. Предложены меры различия семантических содержаний открытого и преобразованного участка изображения, количественных показателей относительно степени расхождения соответствующих форматов описания на синтаксическом уровне фрагмента изображения.

ЛИТЕРАТУРА

[1]. Баранник В.В. Метод криптосемантического представления изображений на основе комбинированного подхода / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – К., 2010. – № 3(22). – С. 33-38.

[2]. Баранник В.В. Метод дешифрируемо-стойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – К., 2011. – № 1(24). – С. 22-28.
[3]. Бараннік В.В. Методологічні основи криптосемантичного представлення відеозображень в інформаційних комунікаціях / В.В. Бараннік, С.О. Сідченко, В.В. Ларін // Наукоємні технології. – К., 2012. – № 3(15). – С. 78-82.
[4]. Нагорных И.М. Способы защиты видеоданных от несанкционированного доступа / И.М. Нагорных // Спецтехника и связь // http://www.st-s.su/index.htm.
[5]. Uhl A. Image and Video Encryption From Digital Rights Management to Secured Personal Communication / A. Uhl, A. Pommer. – Springer 2005, ISBN: 978-0-387-23402-1.

REFERENCES

[1]. Barannik V.V., Sidchenko S.A., Larin V.V. Method of cryptosemantic presentation of images on the basis of the combined approach, Modern special technique, 2010, № 3(22), pp. 33–38.
[2]. Barannik V.V., Sidchenko S.A., Larin V.V. Method of the combined decoded-firm presentation of images, Modern special technique, 2011, № 1(24), pp. 22-28.
[3]. Barannik V.V., Sidchenko S.A., Larin V.V. Methodological bases of cryptosemantic presentation of video-images in the informative communications, Science-Based Technologies, 2012, № 3(15), pp. 78-82.
[4]. Nagornyh I.M. Methods of defense of videoinformation from the unauthorized division, Specialtechnique and connection, http:www.st-s.su/index.htm.
[5]. Uhl A., Pommer A. Image and Video Encryption From Digital Rights Management to Secured Personal Communication, Springer 2005, ISBN: 978-0-387-23402-1.

МЕТОДОЛОГІЧНА БАЗА КРІПТОКОМПРЕСІЙНОГО ПРЕДСТАВЛЕННЯ ВІДЕОІНФОРМАЦІЙНИХ РЕСУРСІВ

Розвиток технологій представлення відеоінформаційного забезпечення та його інтеграція в різні сфери діяльності суспільства вимагає підвищення ефективності захисту відеоданих, доведення яких необхідно в реальному часі. Існуючі технології захисту відеоданих від несанкціонованого доступу засновані на послідовному виконанні операцій стиску й шифрування або схемі так званого вибіркового шифрування, що використовує особливості кодування й структури потоку MPEG для скорочення обчислювальних ресурсів на захист відеоданих. Недоліком послідовної схеми є потреба в значних обчислювальних ресурсах або часові затримки при обробці й передачі, а недоліком вибіркового шифрування – більш низька захищеність даних. Розглянуто потенційні можливості захисту оперативної відеоінформації в напрямку побудови стійких до несанкціонованого дешифрування (розпізнавання) зображень на базі систем компактного представлення, тобто забезпечення скритності відеоінформації на рівні кодування її джерел. Висловлюються основні компоненти розробки методологічної бази криптокомпресійного представлення відеоінформаційних ресурсів. Приводяться базові визначення криптокомпресійного представлення, вводиться новий науково-прикладний напрямок – "Теорія криптокомпресії". Даються основні напрямки науково-прикладних досліджень, проведених у даній області знань. Формується методологічна база складових криптокомпресійної побудови відеоданих.

Ключові слова: криптокомпресійне представлення, захист відеоінформації, компактне представлення, відеоінформаційний ресурс, методологічні основи.

METHODOLOGICAL BASE OF CRYPTOCOMPRESSION PRESENTATION OF VIDEOINFORMATION RESOURCES

Development of the technologies presentation of the videoinformation providing and its integration in the different spheres of activity of the society requires the increase of efficiency of defence the videodate, leading of which is need in real time. Existent technologies of defence of the videoinformation from unauthorized division are based on step-by-step implementation of the operations compression and encipherement or schemes of the so called selective encipherement, uses the features of encoding and structure of stream of MPEG for reduction of calculable resources for defence of videoinformation. The lack of successive scheme appear is requirement in considerable calculable resources or dwells at treatment and transmissions, but by the lack of selective encipherement is more low defend of information. Potential possibilities of defence of operative videoinformation are considered in the direction of construction proof to unauthorized decoding (recognitions) of images on the base of the systems of compact presentation, i.e. providing of secrecy of videoinformation at the level of coding its sources. Sets out the principal components of the methodological base development of the cryptocompression presentation videoinformation resources. Basic definitions cryptocompression presentation are provides, also is introduce a new scientific and practical direction – "Theory of cryptocompression". The main directions of scientific-applied research are conducted in this field of knowledge. The methodological base of the cryptocompression building of the videodata components is formed.

Index Terms: cryptocompression presentation, defence of the videoinformation, compact presentation, videoinformation resource, methodological base.

Бараннік Володимир Вікторович, доктор технічних наук, професор, начальник кафедри, Харківський університет Повітряних Сил імені Івана Кожедуба.
E-mail: Barannik_V_V@mail.ru.