УДК 621.327:681.5

С.А. Сидченко,
кандидат технических наук,
старший научный сотрудник
В.В. Ларин,
кандидат технических наук
Д.В. Баранник

МЕТОД КРИПТОКОМПРЕССИОННЫХ ПРЕОБРАЗОВАНИЙ С КЛЮЧОМ

Излагаются основные компоненты разработки метода криптокомпрессионных преобразований с ключом видовых изображений. Приводятся базовые варианты защиты ключа в процессе компрессии видеоинформации, дана классификация по временному пространству действия. Выделены основные направления научно-прикладных исследований, проводимых в данной области знаний. Формируются базовые составляющие процесса построения криптокомпрессионных преобразований с ключом.

Ключевые слова: *криптокомпрессионное представление изображений; механизмы криптографического преобразования, стойкие к несанкционированной дешифровке (СНД) системы.*

Викладено основні компоненти розробки методу криптокомпресійних перетворень із ключем видових зображень. Наведено базові варіанти захисту ключа в процесі компресії відеоінформації, дана класифікація за часовим простором дії. Виокремлено основні напрями науково-прикладних досліджень, що проводяться в цій галузі знань. Формуються базові складові процесу побудови криптокомпресійних перетворень із ключем.

Ключові слова: *криптокомпресійне представлення зображень, механізми криптографічного перетворення, стійкі до несанкціонованої дешифровки (СНД) системи.*

Basic components of the development of a method cryptocompressive transformations with a key of specific images are stated. Basic variants of a key protection in the course of a video information compression are resulted; classification by time space of an action is given. Basic directions of scientifically-applied researches, spent in the given field of knowledge, are highlighted. Basic components of the process of the construction cryptocompressive transformations with a key are formed.

Keywords: *cryptocompressive representation of images; mechanisms of the cryptographic transformation, resistant to unauthorized decryption (RUD) system.*

С широким распространением медиаконтента, остро встал вопрос его защиты от хищения, искажения и незаконного использования. Повсеместное использование высокоскоростного Интернета, локальных вычислительных сетей, беспроводных сетевых технологий делает данную проблему еще более актуальной. Видеоконференции, видеосвязь, видеонаблюдение, цифровое наземное, кабельное и спутни-

ковое ТВ – это далеко не полный перечень актуальных приложений, которые не могут быть конфиденциальны без применения в том или ином виде защиты в связи с тем, что большинство такого рода приложений использует сети общего назначения для передачи данных. Соблюдение авторских прав также является одной из задач конфиденциальности передачи видеоинформации [1].

Важным подходом относительно дополнительной обработки, направленной на изменение стандартного процесса сжатия и создания стойких к несанкционированной дешифровке (СНД) систем с ключом, является интегрирование криптографического преобразования (шифрования), как представлено на рис. 1. Для такого подхода возможны следующие варианты (классификация по временному пространству действия) (рис. 2) [2–3]:

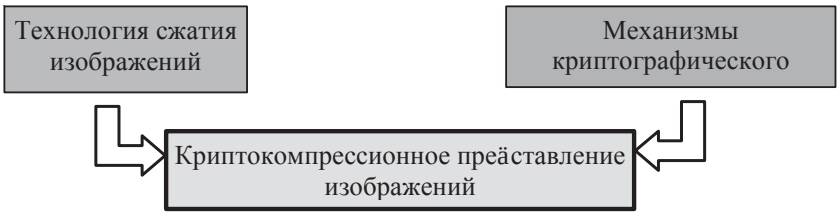

Рис. 1. Схема подхода для создания криптокомпрессионного представления с ключом

1) использовать ключ в процессе сжатия, т.е. сжатие с ключом. Криптографические преобразования осуществляются в процессе формирования сжатого представления изображения;

2) использовать ключ после сжатия информации, т.е. сжатие с последействием. Вначале используется процесс сжатия, и формируются информационная и служебная составляющие компактного представления. После чего используются специальные механизмы криптографического трансформирования. Например, криптографическая шифровка служебных данных и/или информационной части кодовой конструкции;

3) комбинированный подход, когда оба варианта используются в одном процессе обработки изображения.

Наибольшая степень стойкости к несанкционированной дешифровке будет достигаться для третьего варианта обработки.

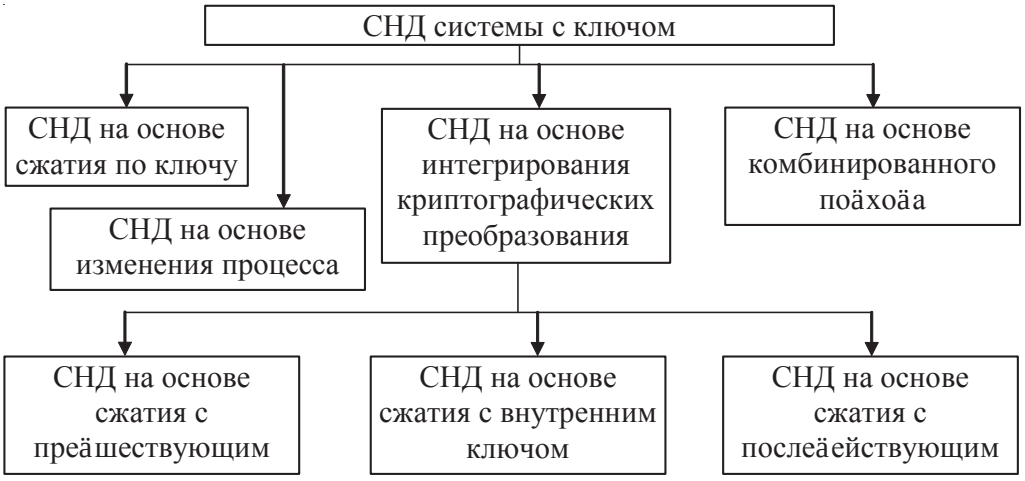

Рис. 2. Классификация вариантов систем СНД представления с ключом

Схематично такой процесс обработки представлен на рис. 3.

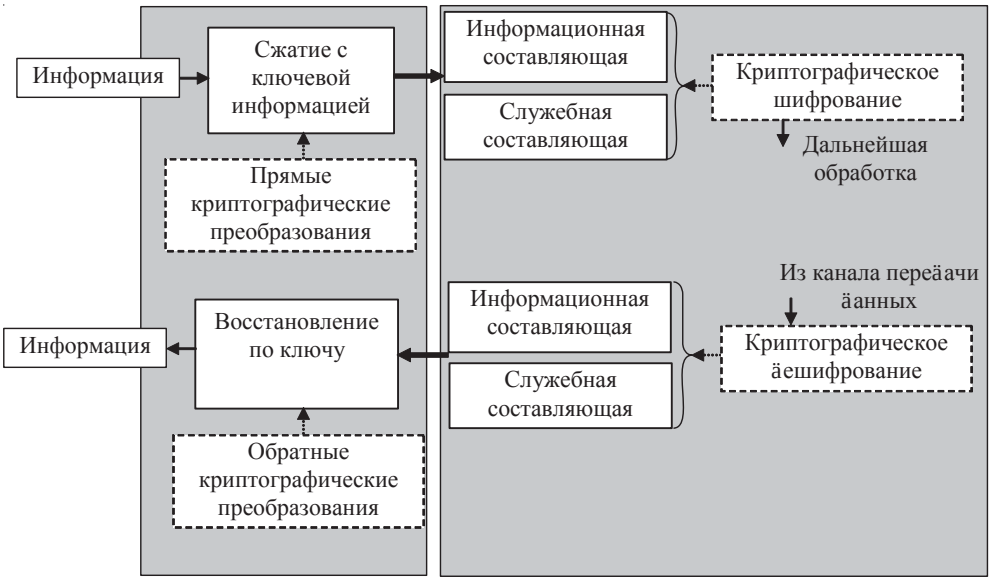

Рис. 3. Схема вариантов задействования криптографических преобразований в процессе формирования СНД представления изображений

Рассмотрим первый вариант, а именно ***систему с СНД на основе сжатия по ключу*** [3]. Для таких систем скрытие (маскирование) видеоинформации обеспечивается в процессе компактного представления по ключу S. В этом случае ключ S является составной частью процесса кодирования, т.е. представляет собой вектор параметров, влияющих на структуру или на процесс функционирования алгоритма сжатия. В основе данного подхода лежит предположение о возможности выделения из изображения той его составляющей, которая имеет наибольшее семантическое значение с позиции достоверного дешифрирования. Другими словами требуется преобразовать изображение к структуре, в которой достигается его разделение на составляющие, имеющие различную семантическую нагрузку. Например, выделить в процессе кодирования ключевые данные, несущие основную информацию о полном представлении изображения, в том числе выделить данные несущие интегрированную информацию о контурах и деталях блоков видеоданных. Такими данными могут быть низкочастотные составляющие, содержащие преобладающее количество семантической информации об изображении. Причем такое выделение необходимо сделать как можно в меньшем количестве данных по сравнению с количеством данных в исходном блоке.

Тогда искажения семантически значимой составляющей приведет к лавинному разрушению исходного изображения. Будут разрушены дешифровочные признаки открытого изображения, т.е. скрытие будет достигнуто на качественном уровне информации. В этом случае использовать функцию маскирования с учетом особенностей восприятия изображений зрительной системой не представляется возможным. Поэтому оценку степени такого разрушения можно будет осуществлять с использованием среднеквадратических показателей степени отклонения.

Представление стойкого к несанкционированному дешифрированию (СНД) [4] на базе компрессионного преобразования $f_{кпк}(A_{син}; P_{син}; S)$ по ключу S задается следующим образом:

$$N(A_{син}; S) = \underset{Âèäåî èí îôîðì àöèÿ}{f_{кпк}}(A_{син}; P_{син}; S), \quad (1)$$

где $A_{син}$ – фрагмент исходного (открытого) фрагмента изображения, $P_{син}$ – система количественных признаков изображений, характеризующих особенности источника видеоинформации, $N(A_{син}; S)$ – стойкое к дешифрированию по ключу представление открытого фрагмента изображения.

На выходе компрессирующего преобразования по ключу формируется две составляющих $\{N(A_{син}; S), S\}$, а именно собственно СДШП представление $N(A_{син}; S)$ и ключевая информация S.

Определение. Системой с СНД (криптокомпрессионной системой) на основе сжатия по ключу называется система, задаваемая следующим вектором (рис. 4):

$$\{N(A_{син}; S);\ S;\ f_{кпк}(A_{син}; P_{син}; S);\ f_{кпк}^{(-1)}(N(A_{син}; S); P_{син}; S)\},$$

где $f_{кпк}(A_{син}; P_{син}; S)$ – прямое криптокомпрессионное преобразование открытого фрагмента $A_{син}$ с ключом сжатия S; $f_{кпк}^{(-1)}(N(A_{син}; S); P_{син}; S)$ – обратное криптокомпрессионное преобразование на основе скрытого представления $N(A_{син}; S)$, системы служебных данных $P_{син}$ и ключа сжатия S.

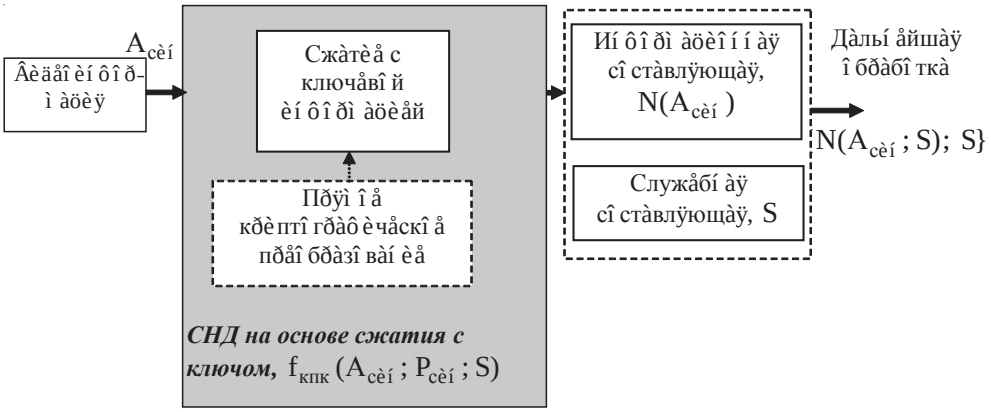

Рис. 4. Структурная схема системы с СНД на основе сжатия с ключом

Под служебными данными $P_{син}$ будем понимать систему количественных параметров закономерностей, на основе которых устраняется избыточность в изображениях. Обязательным условием для системы служебных данных является наличие их влияния на процесс восстановления изображений.

Относительно преобразования $f_{кпк}(A_{син}; P_{син}; S)$ в системе с СНД [4] выдвигаются следующие требования (обеспечение оперативности и безопасности доставки видеоинформации):

1. Функционал $f_{кпк}(A_{син}; P_{син}; S)$ преобразования должен быть взаимообратимым. Показатель потерь, как среднеквадратическое отклонение декомпрессированного фрагмента $A'_{син}$ относительно исходного $A_{син}$ фрагмента, в случае санкционированного доступа должен быть равным нулю, т.е. $\delta(A_{син}; A'_{син}) = 0$. Для реконструируемого фрагмента $A'_{син}$ должно обеспечиваться условие $(A'_{син} | (A_{сем} \cap A'_{сем} = A_{сем}))$, когда семантическая составляющая $A'_{сем}$, соответствующая реконструируемому фрагменту, полностью соответствует семантической составляющей $A_{сем}$ исходного

(открытого) фрагмента. Данное требование можно записать в виде необходимого условия

$$V(A_{\text{сèí}}) = V(A'_{\text{сèí}}; S') \text{ для } \quad S' = S; \tag{2}$$

и достаточного условия

$$P(A_{\text{сâì}}; A'_{\text{сèí}}; S')_{\text{äш}} = 1 \quad \text{для} \quad S' = S, \tag{3}$$

т.е. вероятность правильного дешифрирования полного семантического содержания исходного фрагмента по синтаксическому описанию $A'_{\text{сèí}}$ декомпрессированного фрагмента равна единице. Здесь $V(A_{\text{сèí}})$ – количество информации, определяемое для синтаксического уровня исходного фрагмента изображения; $V(A'_{\text{сèí}}; S')$ – количество информации для синтаксического уровня описания декомпрессионного фрагмента на основе использования ключа S'. Величина $V(A'_{\text{сèí}}; S')$ является условным количеством информации в $A'_{\text{сèí}}$ об $A_{\text{сèí}}$ в зависимости от ключа S'.

2. Не должно существовать других методов вскрытия семантического содержания открытого фрагмента $A_{\text{сâì}}$ по известному представлению $N(A_{\text{сèí}}; S)$, кроме как полного перебора ключей S.

В том числе должно выполняться следующее, если $S' \neq S$, то:

– не найдется таких параметров преобразований $P'_{\text{сèí}}$ для текущей функции $f_{\text{кпк}}(A_{\text{сèí}}; P_{\text{сèí}}; S')$ и $f^{(-1)}_{\text{кпк}}(N(A_{\text{сèí}}; S); P_{\text{сèí}}; S')$, при которой раскрывалось бы содержание исходного фрагмента;

– не найдется такого видоизменения прямого и обратного преобразований $f'_{\text{кпк}}(A_{\text{сèí}}; P_{\text{сèí}}; S')$ и $f'^{(-1)}_{\text{кпк}}(N(A_{\text{сèí}}; S); P_{\text{сèí}}; S')$ функции $f_{\text{кпк}}$, для которого раскрывалось бы содержание исходного фрагмента;

– не найдется одновременно видоизменения функции и ее параметров, т.е. $f'_{\text{кпк}}(A_{\text{сèí}}; P'_{\text{сèí}}; S')$ и $f'^{(-1)}_{\text{кпк}}(N(A_{\text{сèí}}; S); P'_{\text{сèí}}; S')$, при которой раскрывалось бы содержание исходного фрагмента.

Другими словами, когда $S' \neq S$, тогда количество информации в $A'_{\text{сâì}}$ об $A_{\text{сâì}}$ должно равняться нулю, т.е. $P(A_{\text{сâì}}; A'_{\text{сèí}}; S')_{\text{äш}} = 0$ для $S' = S$.

3. Не должно существовать других методов определения, каким ключом было осуществлено преобразование открытого фрагмента $A_{\text{сâì}}$ в криптокомпрессионное представление $N(A_{\text{сèí}}; S)$ со скрытым семантическим содержанием, кроме как полным перебором ключей. Функционал не должен иметь уязвимых мест, позволяющих выявить ключевую последовательность в случае, когда известны скрытое преобразование фрагмента, параметры алгоритмов преобразования и сами алгоритмы прямого и обратного преобразования.

4. Обеспечивать сокращение объема открытого фрагмента изображения в результате его компактного представления на основе сокращения избыточности, т.е. $V(N(A_{\text{сèí}}; S)) + V(P_{\text{сèí}}) + V(S) \leq V(A_{\text{сèí}})$, где $V(N(A_{\text{сèí}}; S))$ – объем цифрового описания преобразованного представления, $V(P_{\text{сèí}})$ – объем цифрового описания системы количественных признаков, характеризующих особенности

источника видеоинформации, V(S) – количество двоичных разрядов на представление ключа S.

5. Должна обеспечиваться допустимая сложность реализации. Формирование скрытого представления исходного фрагмента изображения должно требовать приемлемых затрат машинных операций, и допускать как программную, так и аппаратную реализации для универсальных и дистанционных вычислительных комплексов в условиях энергоэффективных систем.

В целом же для систем с СНД [5] на основе ключа в процессе компрессии выдвигаются следующие требования:

1. Кодограммы $[N(A_{сжí}; S)]_2$ криптокомпрессионного представления должны поддаваться раскрытию только при наличии ключа S. Алгоритмы прямого $f_{кпк}$ и обратного $f_{кпк}^{(-1)}$ преобразований, а также вектор параметров $P_{сжí}$ считаются известными. Для злоумышленника не известной остается только ключевая информация S. Данное требование записывается следующим видом:

$$(A'_{сжí} \mid (A_{сåì} \cap A'_{сåì} = \varnothing)) \text{ или } P(A_{сåì}; A'_{сжí}; S')_{äø} = 0 \text{ для } S' \neq S.$$

Здесь величина $P(A_{сåì}; A'_{сжí}; S')_{äø}$ означает вероятность правильного дешифрирования семантического содержания $A_{сåì}$ исходного фрагмента по декомпрессированному синтаксическому представлению $A'_{сжí}$,

$$A'_{сжí} = f_{кпк}^{(-1)}(N(A_{сжí}; S); P_{сжí}; S'),$$

полученного на основе обратного преобразования $f_{кпк}^{(-1)}(N(A_{сжí}; S); P_{сжí}; S')$ по ключу S', где $S' \neq S$. Здесь S, S' – соответственно истинная (верная) и неверная ключевые последовательности.

2. Должно обеспечиваться существенное изменение скрытого представления $N(A_{сжí}; S)$ в случаях незначительного изменения:

– ключа S. В общем случае ключ S может представляться набором количественных параметров и условий, $S = \{s_1, \ldots, s_u, \ldots, s_U\}$. Тогда под изменением ключа понимается событие, когда хотя бы для одного параметра выполняется условие $s'_u \neq s_u$;

– исходного (открытого) $A_{сжí}$ фрагмента изображения на синтаксическом уровне описания.

Для первого случая ключевая последовательность должна оказывать значимое влияние на представление $N(A_{сжí}; S)$. Изменение даже одного элемента ключевой последовательности должно приводить к существенному изменению выходной последовательности сжатого (скрытого) представления. Данное требование можно записать как то, что

$$N(A_{сжí}; S_1) - N(A_{сжí}; S_2) \to \max \text{ и } |S_1| = |S_2|,$$

где $|S_{1,2}|$ – количество двоичных разрядов, значения которых совпадают для ключевых последовательностей S_1 и S_2; $|S_1|$, $|S_2|$ – длина соответственно ключа S_1 и S_2.

3. Количество операций, необходимых для определения ключа S, по скрытому представлению $N(A_{\text{сні}}; S)$, и соответствующего ему открытому фрагменту $A_{\text{сні}}$, должно быть не меньше общего количества возможных ключей.

4. Количество операций, необходимых для расшифровки $N(A_{\text{сні}}; S)$ путем перебора всех возможных ключей S (лобовая атака), должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных и перспективных компьютерных систем и сетей;

5. Ключевая информация, используемая для систем с СНД на основе сжатия с ключом, не должна быть одинаковой для разных фрагментов изображения.

6. Структурные элементы алгоритма, стойкого к дешифрированию преобразования на основе технологий компрессии, должны быть неизменными.

7. Не должно быть простых и легко устанавливаемых зависимостей между ключами S, которые используются в процессе стойких к дешифрированию преобразований.

8. Изменение длины ключа S не должно вести к качественному ухудшению алгоритма криптокомпрессии, в том числе к изменению скорости кодирования и декодирования.

Выводы

1. Показана необходимость обеспечения безопасности видеоинформационных ресурсов, с использованием метода криптокомпрессионных преобразований с ключом.

2. Разработаны требования обеспечения оперативности и безопасности доставки видеоинформации. Приводятся базовые требования системы со стойкими к несанкционированной дешифровки преобразованиями. Даются основные направления научно-прикладных исследований, которые проводятся в данной области знаний. Формируются базовые составляющие построения криптокомпрессионных преобразований с ключом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Кашкин В.Б.* Цифровая обработка аэрокосмических изображений : Конспект лекций / В.Б. Кашкин. – Красноярск : ИПК СФУ, 2008. – 121 с.

2. *Баранник В.В.* Методология создания криптографических преобразований на базе методов, исключающих избыточность / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2009. – Вип. 4 (19). – С. 24–30.

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

4. *Баранник В.В.* Метод дешифрируемостойкого представления изображений / В.В. Баранник, С.А. Сидченко, В.В. Ларин // Сучасна спеціальна техніка. – 2011. – № 1 (24). – С. 22–28.

5. *Баранник В.В.* Методологічні основи криптосемантичного представлення відеозображень в інфокомунікаціях / В.В. Баранник, С.А. Сідченко, В.В. Ларін // Наукоємні технології. –2012. – № 3 (15). – С. 78–82.

Отримано 29.03.2013