Алгоритм защиты видео в формате H.264 полухрупкими цифровыми водяными знаками

А.А. Егорова[1], В.А. Федосеев[1,2]

[1]Самарский национальный исследовательский университет им. академика С.П. Королева, Московское шоссе 34А, Самара, Россия, 443086
[2]Институт систем обработки изображений РАН - филиал ФНИЦ «Кристаллография и фотоника» РАН, Молодогвардейская 151, Самара, Россия, 443001

Аннотация. В работе представлена полухрупкая ЦВЗ-система, предназначенная для аутентификации видеоданных формата H.264. Внедрение полухрупкого ЦВЗ производится в коэффициенты целочисленного ДКП каждого ключевого кадра видеопоследовательности на этапе квантования. Важной отличительной особенностью этой системы является возможность встраивания более одного бита на блок размера 4×4, что способно повысить точность локализации искажённых фрагментов. В экспериментальной части работы представлены результаты исследования зависимости визуального качества видеоданных, защищаемых при помощи предложенной системы, а также погрешность извлечения ЦВЗ при различных степенях сжатия защищаемой информации.

1. Введение

В современном мире крайне важную роль играет задача обеспечения защиты видеоданных от преднамеренных правок, вносимых с целью искажения её содержания. Во-первых, это обусловлено всё возрастающим объёмом трафика видео и ролью мультимедийных данных в современном обществе. Так, согласно отчёту сетевой компании Sandvine [1], среднемировая доля видео в мобильном входящем трафике в 2020 году достигла 65%. Следует также отметить стабильно растущий рынок систем видеонаблюдения (около 22% в год, согласно отчёту аналитиков компании MarketsandMarkets [2]) и их повсеместное внедрение не только крупными бизнес-структурами и органами власти, но и небольшими частными компаниями. Во-вторых, необходимость защиты видеоданных вызвана технической простотой искажения мультимедийной информации злоумышленниками и участившимися примерами подобных искажений. Так, создание фейковых видео уже давно не является сложной технической задачей, а прогресс в области многослойных искусственных нейронных сетей и глубокого обучения привёл к автоматизации этих процессов и, как следствие, к возникновению термина «deepfake» и появлению многочисленных готовых архитектур для создания фальшивых видео [3].

По этой причине большую важность представляет разработка современных методов активной аутентификации видеоданных посредством встраивания в них полухрупких или хрупких цифровых водяных знаков (ЦВЗ) [4, 5]. Хрупкие ЦВЗ удаляются после выполнения любых модификаций над защищённым видео, содержащим встроенный ЦВЗ. Однако если существует некий набор допустимых операций (таких как сжатие, изменение битрейта и пр.),

применяются полухрупкие ЦВЗ, являющиеся стойкими к «разрешённым» преобразованиям и разрушающимися под воздействием всех других. Отсутствие ЦВЗ на этапе проверки подлинности говорит о наличии несанкционированных изменений.

Видеоданные, как правило, хранятся и передаются в сжатом виде, поэтому к числу «разрешённых» преобразований зачастую относят искажения, возникающие вследствие сжатия. Для того, чтобы обеспечить защиту сжатых видеоданных необходимо, чтобы используемая ЦВЗ-система (под этим термином мы будем понимать совокупность методов и средств, образующих единое решение для встраивания ЦВЗ [4, 6]) обладала стойкостью к таким искажениям, то есть встраиваемый ЦВЗ должен с высокой точностью извлекаться из защищаемых сжатых данных.

Одним из наиболее распространённых современных форматов сжатия видеоданных является H.264 [7]. Он отличается от аналогов высоким качеством и степенью сжатия видео, а также гибкостью (в стандарте представлено 7 профилей, задающих наборы параметров кодирования, и 11 уровней, определяющих требования к пропускной способности канала, памяти и т.д.), в связи с чем он широко применяется в DVD высокой чёткости, видеотрансляциях, продуктах компании Apple, онлайн-хранилищах видеоматериалов, игровых видеоприставках и т.д. [8].

В настоящее время известно несколько ЦВЗ-систем, предназначенных для защиты видео в формате H.264. Так, в работах [9, 10, 11] описаны три стойкие системы, предназначенные для защиты авторских прав. Первые две основанные на методе расширения спектра [12], а третья – на методе изменения позиции последнего ненулевого элемента. Подробный обзор систем защиты видеоданных в формате H.264 представлен в статье [13]. В ней описаны системы, реализующие метод встраивания информации в наименее значимые биты (НЗБ-метод), метод расширения спектра, метод на основе табличного отображения (Mapping Table) и др. Однако в данном обзоре не упомянуто ни одной системы на основе метода управляемого переквантования (QIM) [14], несмотря на то, что он является основным при проектировании полухрупких ЦВЗ-систем для других форматов мультимедиа, в частности, JPEG [15]. Кроме того, большая часть систем, представленных в обзоре [13] также не предназначена для аутентификации видео.

Для решения задачи проверки подлинности предложена гибридная система [16], в которой встраивание полухрупкого ЦВЗ реализуется при помощи НЗБ-встраивания, а также системы полухрупкого встраивания [17, 18, 19], из которых [17] и [18] используют метод изменения позиции последнего ненулевого элемента, и лишь система [19] реализует подход на основе переквантования, а именно адаптацию алгоритма DM-QIM [14]. При этом все вышеперечисленные системы [16-19] встраивают 1 бит ЦВЗ в один блок размером 4×4, или один макроблок размером 16×16. Это приводит к тому, что при построении маски изменений велика вероятность ложноположительных обнаружений ЦВЗ в изменившихся блоках.

В настоящей работе предлагается полухрупкая ЦВЗ-система, предназначенная для аутентификации видеоданных формата H.264, и использующая встраивание на базе QIM (а именно, модификацию разработанного нами ранее алгоритма Sign-QIM [15]) с возможностью встраивания более одного бита в один блок. Встраивание ЦВЗ производится одновременно с процессом кодирования ключевых кадров на этапе квантования коэффициентов целочисленного дискретного косинусного преобразования (ДКП), а извлечение происходит совместно с декодированием битовой последовательности, сгенерированной кодером H.264. В работе основное внимание уделяется именно разработке способа внедрения защитной информации в частотную область видеоданных с учётом особенностей стандарта сжатия H.264, при этом вопрос выбора кадров для встраивания опускается. Однако, отметим, что встраивание предложенной системой может быть осуществлено не только в ключевые кадры, но и в кадры других типов, определённые в стандарте H.264. В экспериментальной части работы представлен результат исследования уровня визуальных искажений, вносимых при встраивании информации предложенной системой, а также погрешность извлечения ЦВЗ при различных значениях параметра сжатия видеоданных.

2. Краткая информация о стандарте H.264

В стандарте H.264 [7] перечислены следующие типы кадров, различаемые кодером:

- I-кадры (ключевые кадры) – кодируются и декодируются без привязки к другим кадрам видеопоследовательности;
- P-кадры – содержат ссылки для своего кодирования на части предшествующих I-кадров и/или P-кадров;
- B-кадры – содержат в себе ссылки и на предыдущий, и на последующий ссылочные кадры [8].

Каждый из семи профилей стандарта H.264 определяет какой именно набор параметров использует кодер, в том числе и то, какие типы кадров используются при кодировании. Далее будет рассматриваться и применяться базовый профиль H.264, в котором используются только I- и P-кадры.

Поскольку предлгаемая нами ЦВЗ-система производит встраивание защитной информации на этапе квантования коэффициентов целочисленного ДКП при кодировании ключевых кадров, рассмотрим кратко алгоритмы кодирования и декодирования H.264 ключевых полутоновых кадров, уделяя особое внимание этапам перехода в частотную область, квантованию и соответствующим обратным операциям [8].

2.1. Краткая схема кодирования ключевых кадров в стандарте H.264

При кодировании ключевой кадр разбивается на макроблоки размера 16×16. Затем осуществляется так называемое предсказание либо по всему макроблоку 16×16, либо по непересекающимся блокам 4×4, входящим в него. Суть предсказания заключается в вычислении разницы между исходными значениями блока в каждом отсчёте и значениями, рассчитанными предсказателем. Далее будем рассматривать только кодирование на уровне 4×4. Для него в стандарте определено 9 режимов предсказателя, которые отличаются друг от друга позициями используемых значений (соседей) при расчёте.

Пусть I – это ключевой кадр размера $N_1 \times N_2$, который необходимо закодировать. Обозначим каждый блок ключевого кадра размера 4×4 как I_i, а соответствующий ему блок ошибки предсказаний как X_i, где $i = 1,..,N$ – номер блока, а $N = N_1 N_2/16$ – число непересекающихся блоков в макроблоке. После того, как блок ошибок X_i получен, он переводится в частотную область при помощи прямого целочисленного ДКП по формуле (1) и квантуется по формуле (2) [8]:

$$B_i = \left[C_{f4}\right] \bullet [X_i] \bullet \left[C_{f4}^T\right] \cdot M_{f4}(QP), \quad (1)$$

где • – операция матричного умножения; · – операция поэлементного умножения; $\left[C_{f4}\right]$ – матрица для расчёта прямого целочисленного ДКП, определённая в стандарте H.264; $\left[C_{f4}^T\right]$ – транспонированная матрица $\left[C_{f4}\right]$; $M_{f4}(QP)$ – матрица весов компонент ДКП, соответствующих их значимости, значения которой вычисляются на основе значения *QP*; *QP* – параметр качества, определяющий степень сжатия данных.

$$Y_i = round\left(\frac{B_i}{2^{15+floor(QP/6)}}\right). \quad (2)$$

Чем выше значение *QP*, тем больше шаг квантования и, следовательно, сильнее сжатие. Диапазон изменяемых значений параметра – [0, 51], при этом рекомендуемыми являются значения [20, 40], поскольку значения выше 40 приводят к чрезмерной деградации содержимого, а значения ниже 20 – к неоправданному увеличению объёма сжатого видео [7].

Вслед за операциями (1)-(2) производится статистическое кодирование блока квантованных ДКП коэффициентов Y_i. Этот этап не представляет интерес в рамках настоящей работы, поскольку встраивание ЦВЗ осуществляется до него.

2.2. Краткая схема декодирования ключевых кадров в стандарте H.264

Декодирование квантованного блока Y_i производится по формуле:

$$Z_i = round\left(\left[C_{i4}^T\right] \bullet [Y_i \cdot V_{i4}(QP)] \bullet [C_{i4}] \cdot \frac{1}{2^6}\right), \quad (3)$$

где $[C_{i4}]$ – матрица для расчёта обратного целочисленного ДКП, определённая в стандарте H.264; $[C_{i4}^T]$ – транспонированная матрица $[C_{i4}]$; V_{i4} – матрица весов компонент ДКП, связанная с матрицей $M_{f4}(QP)$, используемой при кодировании.

3. Предлагаемая полухрупкая к сжатию H.264 ЦВЗ-система

Встраивание информации в предлагаемой ЦВЗ-системе выполняется в ключевые кадры данных H.264 методом Sign-QIM, относящимся к классу методов встраивания информации на основе переквантования (QIM) [14]. Sign-QIM был разработан авторами настоящей работы для встраивания информации в коэффициенты ДКП при сжатии JPEG [15]. Его особенностью является различная обработка положительных и отрицательных значений при встраивании информации. В настоящей работе метод Sign-QIM адаптирован под стандарт H.264, он учитывает особенности этапов преобразования и квантования этого стандарта. Для повышения стойкости ЦВЗ-системы ко сжатию, встраивание информации производится в низкочастотную область каждого блока, поскольку погрешность квантования коэффициентов этой области минимальна.

Обозначим ЦВЗ, который необходимо встроить в i-ый блок кодируемого макроблока ключевого кадра W_i, а позиции коэффициентов ДКП в зигзагообразной развёртке, в которые будет производиться встраивание, j_k, где $k = 0, \dots, N_w - 1$, а $N_w -$ количество встраиваемых бит ЦВЗ в один блок 4×4. Тогда формула для встраивания информации в один блок ключевого кадра выглядит следующим образом:

$$B_i^W(j_k) = Br_i(j_k) + S_i(j_k) \cdot W_{i,k} \cdot 2^{15+floor(QP/6)}, \quad (4)$$

где $W_{i,k}$ - k-ый бит ЦВЗ, встраиваемый в i-ый блок;

$$Br_i(j_k) = round\left(\frac{B_i(j_k)}{2 \cdot 2^{15+floor(QP/6)}}\right) \times 2 \cdot 2^{15+floor(QP/6)}, \quad (5)$$

$$S_i(j_k) = \begin{cases} 1, & B_i(j_k) \geq Br_i(j_k), \\ -1, & \text{иначе.} \end{cases} \quad (6)$$

Извлечение производится по формуле (7):

$$\widetilde{W}_{i,k} = mod\left(round\left(\frac{B_i^W(j_k)}{2^{15+floor(QP/6)}}\right), 2\right). \quad (7)$$

4. Экспериментальные исследования

Все эксперименты выполнялись на наборе данных, состоящем из четырёх видеопоследовательностей: *IndianCooking*, *PrimitiveCooking, LutGaya, RealBarca*. В таблице 1 отражены их основные особенности. Различные видео были выбраны для того, чтобы показать работу предложенной системы в различных ситуациях. В экспериментах для встраивания информации использовались яркостные компоненты каждого из видео, а на рисунке 1 приведены примеры кадров из каждого видео.

Во всех экспериментах число встраиваемых бит на блок 4×4 принималось равным 2, а длина защищённой последовательности формировалась таким образом, чтобы содержать 80 ключевых кадров.

Таблица 1. Особенности тестовых видеопоследовательностей.

Видеопосле-довательность	Тип видео	Основные особенности
IndianCooking	Кулинарное видео	Крупные планы ингредиентов; частые монтажные склейки
PrimitiveCooking	Документальный фильм	Продолжительные сцены без монтажа; наличие надписей
LutGaya	Комедийный фильм	Короткие сцены; преимущественно неподвижная камера
RealBarca	Трансляция футбольного матча	Продолжительные сцены без переключения на другую камеру; съёмка закреплёнными, но вращающимися камерами, однородный фон

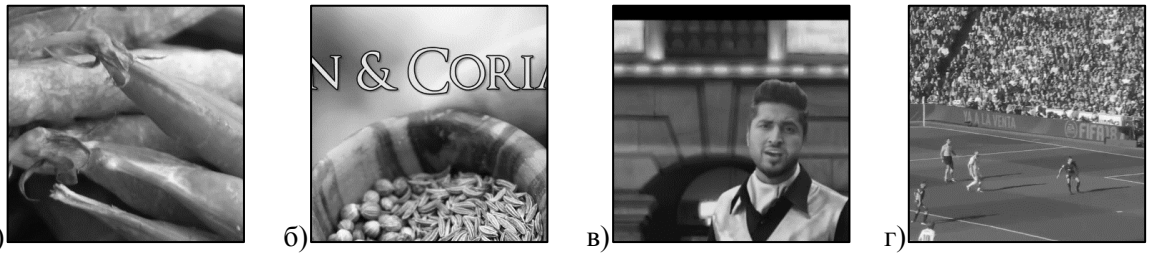

Рисунок 1. Примеры кадров тестового видео: а) *IndianCooking*, б) *PrimitiveCooking*, в) *LutGaya*, г) *RealBarca*.

4.1. Исследование влияния предложенной ЦВЗ-системы на визуальное качество видео формата H.264

Прежде всего, для того, чтобы оценить применимость предложенной ЦВЗ-системы для решения задачи аутентификации данных формата H.264, была проведена оценка визуального качества защищаемых видеоданных при помощи показателя *PSNR* (Peak Signal-To-Noise Measure) [20] при различных значениях параметра сжатия *QP*: от 2 до 40 с шагом 2. На рисунке 2 представлено сравнение значений *PSNR* сжатых видеоданных при различных значениях *QP* в случаях, когда выполнялось только кодирование H.264 и, когда выполнялось и кодирование H.264, и встраивание ЦВЗ. Отметим, что расчёт значений показателя качества в обоих случаях производился только по ключевым кадрам тестовых видеозаписей.

В рамках данного исследования, будем считать допустимыми те значения *PSNR*, которые превышают 35 дБ [20]. По графикам на рисунке 2 видно, что в видеоданных, представленных в формате H.264, данное требование обеспечивается при значениях параметра сжатия $QP \leq 35$. После встраивания ЦВЗ качество защищаемых данных незначительно падает и $PSNR \geq 35$ дБ обеспечивается при $QP \leq 28$. Таким образом, можно заключить, что диапазон значений параметра сжатия, при которых предложенная система встраивания ЦВЗ обеспечивает хорошее визуальное качество, составляет от 1 до 28.

Рисунок 3 иллюстрирует характер искажений данных H.264, возникающих в результате встраивания ЦВЗ предложенной системой. На нём представлен увеличенный фрагмент ключевого кадра видеопоследовательности *LutGaya* с ЦВЗ.

4.2. Исследование стойкости ЦВЗ ко сжатию H.264

В следующем эксперименте исследовалась стойкость встроенного ЦВЗ ко сжатию H.264. В качестве меры стойкости использовался показатель *BER* (Bit Error Rate), характеризующий ошибку при извлечении ЦВЗ и равный отношению числа неверно извлечённых бит к длине ЦВЗ. Если значение *BER* близко к нулю после некоторого искажения, то можно говорить о стойкости ЦВЗ по отношению к нему. При полном разрушении ЦВЗ значение *BER* должно быть близким к 0,5.

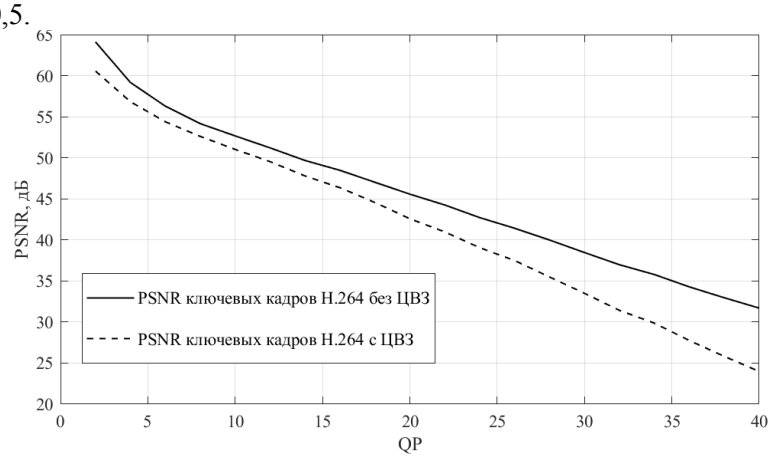

Рисунок 2. График зависимости визуального качества ключевых кадров видеопоследовательности формата H.264 от значения параметра сжатия *QP*.

а) *QP*=8, *PSNR*=52,74 б) *QP*=14, *PSNR*=48,04 в) *QP*=20, *PSNR*=42,93

г) *QP*=26, *PSNR*=37,96 д) *QP* =32, *PSNR*=31,72 е) *QP* =38, *PSNR*=26,01

Рисунок 3. Фрагмент ключевого кадра тестового видео *LutGaya* с ЦВЗ.

В таблице 2 представлены рассчитанные значения *BER* для разработанной системы в случае, когда встраивание производилось при различных *QP* от 2 до 20. При *QP*>20 *BER*=0. Полученные ошибки при малых значениях *QP*, по-видимому, вызваны тем, что при высоком качестве видео значительную роль при извлечении ЦВЗ играют мелкие детали, и даже погрешности, возникающие при восстановлении кадров из архива, играют большую роль. В то же время при больших *QP*, которым соответствуют большие шаги квантования, ЦВЗ более стоек к таким небольшим погрешностям. Отметим, что поскольку рекомендуемые к использованию значения *QP* находятся в диапазоне от 20 до 40, ошибки при малых *QP* не играют серьёзной роли.

Таблица 2. Ошибка *BER* извлечения ЦВЗ после сохранения в формате H.264.

QP	*BER*
2	0,23
4	0,11
6	0,06
8	0,03
10	0,02
12	0,01
14	0
16	0
18	0
20	0

Далее был произведён другой эксперимент: встраивание ЦВЗ производилось с использованием параметра сжатия *QP*, после чего защищённые видеоданные повторно сжимались с параметром *QP**, как большим, так и меньшим, чем *QP*, и исследовалась точность последующего извлечения информации. Встраивание ЦВЗ производилось при нескольких значениях параметра сжатия *QP*=8, 14, 20, 26, 32, 38. Затем в каждом случае производилось повторное сжатие H.264 защищённых видеозаписей с QP^* от 2 до 50 с шагом 2. Декодирование

производилось с QP^*, а извлечение ЦВЗ производилось совместно с декодированием с параметром QP.

На рисунке 4 представлен график влияния уровня сжатия H.264 на ошибку извлечения ЦВЗ. Полученные результаты показывают, что при $QP^* > QP$ точность извлечения резко падает и уже при $QP^* \approx QP+6$ $BER \approx 0{,}5$, что соответствует разрушению ЦВЗ. При $QP^* < QP$ BER сначала наблюдается резкое увеличение ошибки (чем меньше QP, тем больше величина скачка), а затем ошибка уменьшается до значений меньших 0,1, если $QP<32$. Такая картина свидетельствует о том, что разработанная система обеспечивает свойство полухрупкости ЦВЗ по отношению сжатию H.264 с изменяющимся параметром QP.

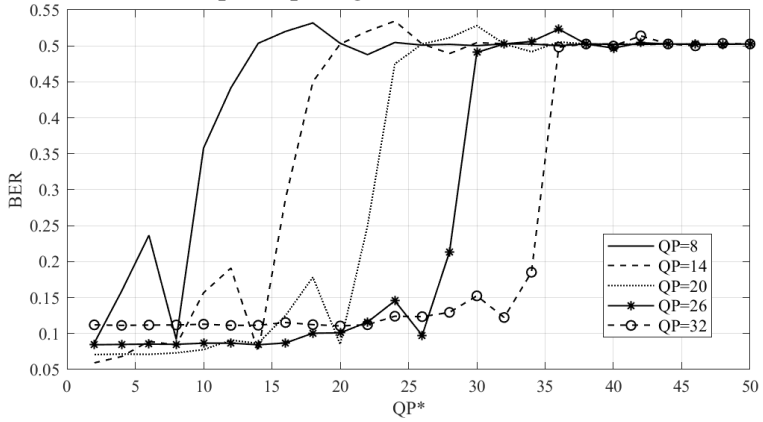

Рисунок 4. Влияние уровня сжатия H.264 на ошибку извлечения ЦВЗ.

5. Заключение

В работе представлена полухрупкая ЦВЗ-система, предназначенная для аутентификации видеоданных формата H.264. Важной отличительной особенностью этой системы является возможность встраивания более одного бита на блок размера 4×4, что способно повысить точность восстановления маски несанкционированных изменений. Другой её особенностью является использование метода встраивания информации на основе управляемого переквантования (QIM), который имеет высокий потенциал в смысле минимизации искажений и повышенной защищённости, как показано в работе [15] на примере встраивания в изображения в формате JPEG.

Экспериментальные исследования, проведённые при встраивании двух бит на блок, показали, что по визуальному качеству встраивание приводит к допустимым результатам при значениях показателя качества $QP \leq 28$. Последующее за встраиванием ЦВЗ сжатие в формате H.264, приводит к различным результатам: при использовании параметра сжатия $QP^* > QP+5$ ЦВЗ разрушается, а при $QP^* \leq QP$ он в целом сохраняется с некоторыми искажениями. Таким образом, система реализует полухрупкое встраивание по отношению к сжатию H.264.

В дальнейших исследованиях планируется уделить внимание на задачи локализации искажений, исследование влияния несанкционированных изменений другого вида на точность извлечения ЦВЗ, а также сравнение с немногочисленными существующими аналогами (в первую очередь, [17, 19]). Кроме того, как отмечалось выше, ещё одним направлением работы является использование не только I-кадров для встраивания информации.

6. Благодарности

Исследование выполнено за счёт гранта Российского научного фонда (проект № 18-71-00052).

7. Литература

[1] Global Internet Phenomena / Sandvine [Electronic resource]. – Access mode: http://www.sandvine.com/phenomena (30.03.2020).

[2] Video Surveillance as a Service Market - Global Forecast to 2022 Phenomena / MarketsAndMarkets [Electronic resource]. – Access mode: https://www.

marketsandmarkets.com/Market-Reports/video-surveillance-as-a-service-market-773.html (30.03.2020).
[3] Westerlund, M. The Emergence of Deepfake Technology: A Review // Technology Innovation Management Review. – 2019. – Vol. 9(11). – P. 39-52. DOI: 10.22215/timreview/1282.
[4] Cox, I. Digital Watermarking and Steganography / I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker – Elsevier, 2008. – 624 p.
[5] Asikuzzaman, Md. An Overview of Digital Video Watermarking / Md. Asikuzzaman, M.R. Pickering // IEEE Transactions on Circuits and Systems for Video Technology. – 2018. – Vol. 28(9). – P. 2131-2153. DOI: 10.1109/TCSVT.2017.2712162.
[6] Федосеев, В.А. Унифицированная модель систем встраивания информации в цифровые сигналы // Компьютерная оптика. – 2016. – Т. 40, № 1. – С. 87-98. DOI: 10.18287/2412-6179-2016-40-1-87-98.
[7] ITU-T H.264 [Electronic resource]. – Access mode: https://www.itu.int/rec/T-REC-H.264-201704-I (01.12.2019).
[8] Richardson, I.E. The H.264 Advanced Video Compression Standard – JohnWiley&Sons, Ltd, 2010. – 346 p.
[9] Su, P.-C. A Content-Adaptive Digital Watermarking Scheme in H.264/AVC Compressed Videos / P.-C. Su, M.-L. Li, I.-F. Chen // International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. – P. 849-852. DOI: 10.1109/IIH-MSP. 2008.305.
[10] Masoumi, M. Content Protection in Video Data Based on Robust Digital Watermarking Resistant to Intentional and Unintentional Attacks / M. Masoumi, S. Amiri // International Arab Journal of Information Technology. – 2014. – Vol. 11(2). – P. 204-212.
[11] Mansouri, A. A Low Complexity Video Watermarking in H.264 Compressed Domain / A. Mansouri, A.M. Aznaveh, F. Torkamani-Azar, F. Kurugollu // IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5(4). – P. 649-657. DOI: 10.1109/ TIFS.2010.2076280.
[12] Cox, I.J. Secure spread spectrum watermarking for multimedia / I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon // IEEE Transactions on Image Processing. – 1997. – Vol. 6(12). – P. 1673-1687. DOI: 10.1109/83.650120.
[13] Tew, Y. An Overview of Information Hiding in H.264/AVC Compressed Video / Y. Tew, K. Wong // IEEE Transactions on Circuits and Systems for Video Technology. – 2014. – Vol. 24(2). – P. 305-319. DOI: 10.1109/TCSVT.2013.2276710.
[14] Chen, B. Quantization Index Modulation: A class of provably good methods for digital watermarking and information embedding / B. Chen, G. Wornell // IEEE Transaction on Information Theory. – 2001. – Vol. 47(4). – P. 1423-1443.
[15] Егорова, А.А. Классификация и сравнительное исследование систем аутентификации JPEG-изображений, основанных на встраивании полухрупких водяных знаков / А.А. Егорова, В.А. Федосеев // Компьютерная оптика. – 2019. – Т. 43, № 3. – С. 419-433. DOI: 10.18287/2412-6179-2019-43-3-419-433.
[16] Park, S.-W. Authentication and Copyright Protection Scheme for H. 264/AVC and SVC / S.-W. Park, S.-U. Shin // J. Inf. Sci. Eng. – 2011. – Vol. 27(1). – P. 129-142.
[17] Chen, T.Y. H.264 Video Authentication Based on Semi-fragile Watermarking / Tsong-Yi Chen, Thou-Ho Chen, Yin-Ting Lin, Yin-Chan Chang, Da-Jinn Wang // International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. – P. 659-662. DOI: 10.1109/IIH-MSP.2008.332.
[18] Farfoura, M.E. Low complexity semi-fragile watermarking scheme for H.264/AVC authentication / M.E. Farfoura, S.-J. Horng, J.-M. Guo, A. Al-Haj // Multimedia Tools and Applications. – 2016. – Vol. 75(13). – P. 7465-7493. DOI: 10.1007/s11042-015-2672-8.
[19] Zhang, Y. Quantization based semi-fragile watermarking scheme for H. 264 video / Y. Zhang, Z.-M. Lu, D.-N. Zhao // Information Technology Journal. – 2010. – Vol. 9(7). – P. 1476-1482.
[20] Сэломон, Д. Сжатие данных, изображений и звука – Москва: Техносфера, 2004. – 368 с.

Semi-fragile watermarking algorithm for H.264 video protection

A.A. Egorova[1], V.A. Fedoseev[1,2]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086
[2]Image Processing Systems Institute of RAS - Branch of the FSRC "Crystallography and Photonics" RAS, Molodogvardejskaya street 151, Samara, Russia, 443001

Abstract. The paper presents a semi-fragile watermarking system designed for authentication of H.264 video. Watermark embedding is performed into integer DCT coefficients of each key frame of a video sequence at the quantization stage. An important distinguishing feature of this system is the ability to embed more than one bit into a 4×4 subblock, which can increase the accuracy of distortion localization. The experimental part presents the results of studies of the dependence of visual quality on protected video using the proposed system, and the watermark extraction error for various H.264 quantization parameter values.