МЕТОД ВСТРАИВАНИЯ ИНФОРМАЦИИ В ВИДЕО, СТОЙКИЙ К ОШИБКАМ ПОТЕРИ СИНХРОНИЗАЦИИ

Митекин В.А., Федосеев В.А.
Институт систем обработки изображений РАН,
Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ)

Аннотация

В работе представлен новый метод стеганографического встраивания информации в цифровые видеопоследовательности. Отличительной особенностью предлагаемого метода является тот факт, что для извлечения информации не требуется временная (по номерам кадров) синхронизация исходной видеопоследовательности и видеопоследовательности со встроенной информацией, что обусловливает высокую устойчивость метода к ошибкам пропуска и замены кадров. Кроме того, данный метод обладает более высокой, по сравнению с другими методами данного класса, информационной ёмкостью. На основе предложенного метода разработана система встраивания информации в видео, использующая методы модуляции с расширением спектра. Приведены результаты экспериментальных исследований данной системы, показавшие её стойкость к атаке с приближённым вычислением ЦВЗ и к искажениям видеопоследовательности (сжатие с потерями, кадрирование и др.), а также высокую кодовую скорость в сравнении с наиболее известным методом данного класса (метод Дэйви и МакКея).

Ключевые слова: сокрытие информации, цифровой водяной знак (ЦВЗ), ЦВЗ для видео, стойкий ЦВЗ, ошибка потери синхронизации.

Введение

Методы встраивания скрытой информации в цифровые видеопоследовательности и в особенности методы защиты видео от несанкционированного копирования при помощи встроенного ЦВЗ получили значительное распространение в последние два десятилетия. Согласно [6] и [8], большинство существующих алгоритмов встраивания ЦВЗ в видеопоследовательности основано на покадровом подходе к встраиванию ЦВЗ. Данный подход предполагает, что и при встраивании, и при извлечении ЦВЗ каждый кадр видеопоследовательности обрабатывается независимо от других кадров. Таким образом, данный подход рассматривает видеопоследовательность как упорядоченный набор изображений, в каждое из которых встраивается один и тот же ЦВЗ малого объёма (до 30–50 бит). Как было показано в работе [2], подобный «покадровый» подход к встраиванию ЦВЗ в видео имеет ряд уязвимостей, которые могут быть использованы для обнаружения и/или удаления встроенного ЦВЗ без знания ключа встраивания.

Во-первых, если один и тот же стеганографический ключ K использовался для встраивания ЦВЗ во все кадры видеопоследовательности, то становится возможной достаточно тривиальная атака, направленная на извлечение встроенного ЦВЗ. Атакующий, используя метод главных компонент (PCA) или схожий с ним метод независимых компонент (ICA) [1], может приближённо вычислить «шумоподобную» компоненту $D'(n,m)$, присутствующую в каждом кадре и кодирующую встроенный ЦВЗ. Далее атакующий может и обнаружить присутствие встроенной информации без знания ключа, и извлечь её полностью или частично, если известен способ кодирования. Данная атака становится возможной именно в том случае, когда значение ЦВЗ (а значит, и соответствующее ему значение $D'(n,m)$) одинаково для всех кадров видеопоследовательности. Кроме того, с целью удаления или искажения встроенного ЦВЗ при минимальных искажениях видео атакующий может применить так называемую атаку с «приближённым вычислением ЦВЗ» (“watermark estimation attack”) [2], используя приближённое значение $D'(n,m)$.

Во-вторых, рассмотрим случай, когда для покадрового встраивания используется не один ключ K, а серия независимо сгенерированных ключей K_t, $t \in [0, T-1]$, где T – количество кадров в видеопоследовательности, а t – номер кадра. То есть при встраивании информации в кадр с номером t выбирается ключ K_t.

Использование индивидуальных ключей встраивания для каждого кадра видеопоследовательности делает невозможной рассмотренную выше атаку, основанную на вычислении статичной «шумоподобной» составляющей $D'(n,m)$. Но в то же время данный подход делает необходимой временну́ю (т.е. по номеру кадра) синхронизацию процедур встраивания и извлечения информации. Действительно, для извлечения ЦВЗ из каждого кадра видеопоследовательности необходимо знать номер этого кадра на момент встраивания. В ряде же случаев, например, в случае пропуска отдельных кадров при передаче и/или кодировании видеоданных, номера кадров в искажённой видеопоследовательности не будут соответствовать номерам, использованным при встраивании ЦВЗ.

Ранее были предложены несколько алгоритмов, позволяющих избежать ошибок извлечения, связанных с потерей синхронизации. Так, в работах [3] и [4] авторами предложено генерировать ключ K_t на осно-

ве статистических характеристик t-го кадра, таких как средняя яркость кадра и пр. Таким образом, непосредственно номер текущего кадра не требуется ни при встраивании, ни при извлечении ЦВЗ. Необходимая для генерации ключа K_t информация может быть получена путём анализа только текущего кадра, что обеспечивает устойчивость всей схемы к ошибкам потери синхронизации, включая ошибки пропуска и замены кадров видеопоследовательности. Тем не менее, представленный в работах [3] и [4] подход к генерации ключа обладает рядом недостатков. Во-первых, если видеопоследовательность содержит большое число идентичных или визуально схожих кадров, то для всех этих кадров будет сгенерирован одинаковый ключ встраивания и встроенный ЦВЗ окажется уязвимым к рассмотренной ранее атаке приближённого вычисления ЦВЗ. Во-вторых, после встраивания ЦВЗ видеопоследовательность может быть подвергнута преднамеренным или непреднамеренным искажениям, что приведёт к изменению именно тех статистических характеристик кадра, которые используются при определении ключа K_t. Подобное изменение может привести к полной невозможности извлечения ЦВЗ из всех кадров искажённого видео, так как генерируемый при извлечении ЦВЗ ключ будет отличаться от исходного.

Ещё один подход к генерации ключей встраивания, описанный в работах [2], [5–6], основан на использовании фиксированного набора заранее сгенерированных ключей K_j, где $j \in [0, J-1]$ и $J \ll T$. Индекс ключа для каждого кадра определяется как $j = t \pmod J$. При потере синхронизации извлечение информации возможно путём перебора всех ключей сформированного набора. Однако если принцип выбора ключа K_j в зависимости от номера текущего кадра становится известен атакующему, тот может выбрать из видеопоследовательности только кадры с заданным значением j (т.е. фактически кадры, у которых шумоподобная составляющая $D'(n,m)$ совпадает) и использовать их для проведения рассмотренной выше атаки.

Кроме того, в работах [7] и [8] рассматриваются способы обеспечения временно́й синхронизации, основанные на встраивании в видеопоследовательность дополнительных (помимо основного ЦВЗ) «меток синхронизации». Данные метки, в роли которых обычно выступают M-последовательности или последовательности Голда, аддитивно встраиваются в фиксированные области кадра и позволяют независимо от ключа встраивания основного ЦВЗ встроить в текущий кадр информацию о номере текущего кадра в исходной видеопоследовательности. Таким образом, встроенная дополнительная «метка синхронизации» позволяет для каждого кадра определить, какой именно ключ K_j нужно использовать для извлечения основного ЦВЗ. Подобное решение обеспечивает высокую устойчивость ЦВЗ как к непреднамеренным искажениям кадра (фильтрация, кадрирование, сжатие с потерями и т.д.), так и к ошибкам потери синхронизации. Но, как показано в [9], в случае преднамеренных атак, направленных на удаление ЦВЗ без знания ключа, «метки синхронизации» сами по себе могут стать объектом таких атак (это так называемые атаки с шаблоном ЦВЗ, “watermark template attack”). Действительно, поскольку при встраивании «меток синхронизации» не используется ключ K_j, эти метки могут быть легко обнаружены и удалены атакующим. В результате удаления «меток синхронизации» извлечение информации также становится невозможным, т.к. становится недоступной информация о выборе ключа K_j, необходимая для корректного извлечения ЦВЗ.

Ещё один класс алгоритмов встраивания информации образуют методы, в которых встраиваемый ЦВЗ формируется путём модуляции шумоподобного шаблона ЦВЗ во временной области. Эти алгоритмы позволяют существенно повысить информационную ёмкость ЦВЗ путём увеличения длины обрабатываемого временно́го фрагмента, но они являются чувствительными к непреднамеренным пропускам кадров и потере синхронизации.

В настоящей работе предложен новый метод встраивания в видео информации, устойчивый к преднамеренным и непреднамеренным ошибкам потери синхронизации (потеря отдельных кадров, изменение порядка следования кадров). Предлагаемый метод встраивания, в отличие от существующих методов покадрового встраивания информации, не требует временно́й синхронизации видеопоследовательности на этапе извлечения. Кроме того, предложенный метод встраивания обеспечивает псевдослучайное распределение встраиваемой информации между кадрами видеопоследовательности, что позволило достигнуть высокой информационной ёмкости по сравнению с существующими методами, которые предполагают встраивание одной последовательности бит ЦВЗ во все кадры.

Работа организована следующим образом. В разделе 1 описан метод предварительного кодирования и встраивания ЦВЗ в видеопоследовательности, устойчивый к преднамеренным и непреднамеренным ошибкам потери синхронизации. В разделе 2 уточняются алгоритмы встраивания и извлечения информации, применяемые в рамках предлагаемого метода и основанные на модуляции с расширением спектра. В разделе 3 предложены способы снижения визуальной различимости ЦВЗ при встраивании информации в видеопоследовательности, а в разделе 4 представлены результаты экспериментальных исследований предложенного метода.

1. Метод предварительного кодирования и встраивания информации в видео

Предлагаемый метод предназначен для встраивания ЦВЗ повышенной информационной ёмкости в цифровые видеопоследовательности. Как утверждается в [6] и [10], метод встраивания скрытой инфор-

мации является уязвимым к атаке с приближённым вычислением ЦВЗ в том случае, если встраиваемая информационная последовательность и ключ встраивания одинаковы для всех кадров видеопоследовательности. Существующие алгоритмы встраивания ЦВЗ в видеопоследовательности, рассмотренные в предыдущем разделе, для защиты от подобных атак используют набор из различных ключей K_t. В то же время как альтернатива схемам с динамически генерируемыми ключами для защиты от атаки с приближённым вычислением ЦВЗ может быть использован подход, при котором ключ встраивания остаётся постоянным для всех кадров, но сам встраиваемый ЦВЗ изменяется некоторым псевдослучайным образом для каждого кадра видеопоследовательности. Такой подход обеспечивает отсутствие статичной шумоподобной составляющей во всех кадрах видеопоследовательности, тем самым обеспечивая стойкость ЦВЗ к упомянутой выше атаке.

Рассмотрим более подробно способ предварительного кодирования встраиваемой информации, основанный на указанном подходе.

Пусть H – последовательность бит встраиваемой информации, состоящая из L непересекающихся фрагментов длиной B_H бит каждый. j-й бит i-го фрагмента H мы будем обозначать как $H_{i,j}$, $i \in [0, L-1]$, $j \in [0, B_H - 1]$. В каждый кадр исходного видео встраивается один из L независимых фрагментов $S_0, S_1, ..., S_{L-1}$, каждый из которых состоит из

$$B = B_I + B_H$$

бит, где

$$B_I = \lceil \log_2 L \rceil + 1,$$

где $\lceil \cdot \rceil$ – это операция округления в бóльшую сторону. Фрагменты S_i формируются по следующему правилу:

$$S_i = i_0 i_1 ... i_{B_I - 1} H_{i,0} H_{i,1} ... H_{i,B_H - 1}, \quad (1)$$

где $i_0 i_1 ... i_{B_I - 1}$ – бинарное представление индекса i, а $H_{i,0} H_{i,1} ... H_{i,B_H - 1}$ – i-й фрагмент H. Например, если $L=8$ и $B_H = 1$, то для $H_7 = 0$ S_7 будет равен *1110*, где *111* – это двоичное представление числа 7. Ниже в тексте $i_0 i_1 ... i_{B_I - 1}$ мы будем именовать *индексной частью* S_i, а $H_{i,0} H_{i,1} ... H_{i,B_H - 1}$ – *информационной частью* S_i.

Далее при встраивании информации для каждого кадра псевдослучайным образом выбирается один фрагмент из набора $S_0, S_1, ..., S_{L-1}$. После этого выбранный фрагмент встраивается в изображение-кадр любым алгоритмом встраивания информации в цифровые изображения. Единственным требованием к используемому алгоритму в данном случае является возможность встраивания и *слепого* (без знания исходного фрагмента ЦВЗ или его части) извлечения не менее чем B бит информации.

Таким образом, предлагаемый подход позволяет избежать статической или периодически повторяющейся структуры встраиваемой информации, не требуя динамически изменяемого ключа встраивания. Используя структуру фрагмента ЦВЗ, указанную в (1), декодер ЦВЗ может извлечь исходную информационную последовательность H, не используя никакую дополнительную информацию об исходной нумерации кадров. Фактически предложенная избыточная структура фрагмента позволяет сделать ЦВЗ устойчивым как к преднамеренным, так и к случайным (например, связанным со сбоями передающего оборудования) ошибкам потери синхронизации.

2. Алгоритмы встраивания и извлечения информации для видео на основе расширения спектра

В данном разделе описана реализация предложенного метода псевдослучайного распределения информации по кадрам видео на основе предложенного ранее одним из авторов [16] алгоритма встраивания стойких ЦВЗ в изображения.

2.1. Алгоритм встраивания информации

Пусть $I_t(m,n)$ – t-й кадр исходного видео размером $N \times M$ пикселей, а T – длина всей видеопоследовательности, предназначенной для встраивания информации; $t \in [0, T-1]$. Для упрощения обозначений будем считать, что информационная последовательность H, введённая в предыдущем разделе, представляется в виде бинарного изображения $W(n,m)$ размерами $N' \times M'$, где $N' < N, M < M'$ и $N'M' = L$.

Пусть также $B_H = 1$, то есть встраивание производится таким образом, что каждый кадр содержит только один информационный бит.

На первом шаге встраивания производится генерация на основе ключа K двух различных двумерных массивов Q_1 и Q_2 размерами $N \times M$, состоящих из значений $\{-1, 1\}$, причём максимальное значение циклической свёртки этих последовательностей близко к нулю.

Далее происходит встраивание информации в t-й кадр по следующему правилу:

$$I_t'(m,n) = I_t(m,n) + \alpha \cdot \xi_W(m,n), \quad (2)$$

где α – коэффициент усиления ЦВЗ, а $\xi_t^W(m,n)$ – шумоподобная аддитивная компонента, зависящая от W и t и вычисляемая по формуле

$$\xi_t^W(m,n) = \begin{cases} \widehat{S}_{x',y'}(Q_2(m,n)) - \widehat{S}_{x,y}(Q_1(m,n)), \\ \quad \textit{если } W(x-x', y-y') = 1; \\ \widehat{S}_{x',y'}(Q_1(m,n)) - \widehat{S}_{x,y}(Q_2(m,n)), \\ \quad \textit{если } W(x-x', y-y') = 0; \end{cases} \quad (3)$$

где $\widehat{S}_{x,y}$ – операция циклического сдвига двумерного массива на x ячеек по горизонтали и y ячеек по верти-

кали, $I_t'(m,n)$ - t-й кадр видеопоследовательности после встраивания ЦВЗ. Положительные целые x, y, $x-x'$, $y-y'$ выбираются псевдослучайным образом для каждого кадра с учётом следующих ограничений:

$$\begin{aligned} &x\in[0,M-1],\\ &y\in[0,N-1],\\ &(x-x')\in[0,M'-1],\\ &(y-y')\in[0,N'-1]. \end{aligned} \quad (4)$$

Как следует из (2)–(3), в результате встраивания каждый кадр видео содержит ровно один бит (пиксель) бинарного изображения $W(n,m)$. Порядок распределения отдельных бит изображения $W(n,m)$ между отдельными кадрами является случайным и определяется только величинами x, y, x', y', генерируемыми независимо для каждого кадра видеопоследовательности. Таким образом, индексная часть фрагмента встраиваемой информации определяется значениями $x-x'$ и $y-y'$, которые встраиваются в текущий кадр путём модуляции циклического сдвига массивов Q_1 и Q_2.

Отметим, что процедура встраивания информации (2)–(3), которая обычно является наиболее критичной в плане вычислительной сложности, в данном случае реализуется на основе простейших операций попиксельного сложения изображений и циклического сдвига. Кроме того, предлагаемый метод также не требует буферизации, т.е. хранения некоторого подмножества кадров в оперативной памяти.

2.2. Алгоритм извлечения информации

Для извлечения изображения $W'(n,m)$ используется быстрый алгоритм вычисления взаимной корреляционной функции (ВКФ) [11, 12] между текущим кадром видеопоследовательности $I_t'(m,n)$ и двумерными массивами Q_1 и Q_2. Пусть C_1 – максимум ВКФ между $I_t'(m,n)$ и Q_1; а неотрицательные целые p и q – это значения циклического сдвига Q_1 по вертикали и горизонтали, при которых достигается этот максимум. Аналогично C_2 – максимум ВКФ между $I_t'(m,n)$ и Q_2; а неотрицательные целые p' и q' – значения циклического сдвига Q_2 по вертикали и горизонтали, при которых достигается этот максимум.

Фрагмент встроенной информации считается обнаруженным в текущем кадре видеопоследовательности, если

$$F=\left[(C_1<-\tau)\wedge(C_2>\tau)\right]\vee\left[(C_1>\tau)\wedge(C_2<-\tau)\right] \quad (5)$$

является истинным. В формуле (5) $\tau\in(0;1)$ – экспериментально выбираемый порог обнаружения.

Значения n и m, составляющие индексную часть встроенного фрагмента, определяются по формуле

$$\begin{aligned} n&=p-p',\\ m&=q-q'. \end{aligned} \quad (6)$$

Наконец, информационная составляющая находится как

$$W'(n,m)=\begin{cases}1, & if\ (C_1<-\tau)\wedge(C_2>\tau),\\ 0, & if\ (C_1>\tau)\wedge(C_2<-\tau).\end{cases} \quad (7)$$

Если число кадров в видеопоследовательности значительно превышает $N'\cdot M'$, то для определения значения каждого бита используется метод «голосования большинства». Это означает, что предложенный метод псевдослучайного распределения бит встраиваемой информации обеспечивает дополнительную избыточность при встраивании, при этом атакующий не может предположить, какие именно кадры содержат выбранный бит ЦВЗ.

3. Снижение визуальных искажений при встраивании информации

3.1. Покадровое маскирование шумоподобной компоненты

Традиционно в системах встраивания ЦВЗ в изображения для снижения визуальных искажений ЦВЗ используется адаптивное изменение амплитуды встраиваемого шумоподобного сигнала в зависимости от локальных особенностей контейнера, то есть вместо формулы (2) при встраивании используется следующее соотношение

$$I_t'(m,n)=I_t(m,n)+\alpha\cdot\beta(m,n)\cdot\xi_t^W(m,n). \quad (8)$$

Одним из простых и наиболее распространённых способов является выбор в качестве $\beta(m,n)$ поля локальной дисперсии контейнера [13]. В данной работе предлагается ограничивать значение $\beta(m,n)$ на отрезке $\left[\sigma^2_{\min},\sigma^2_{\max}\right]$:

$$\beta(m,n)=\min\left\{\max\left\{\sigma^2_{\min},\sigma^2_{8\times8}(m,n)\right\},\sigma^2_{\max}\right\},$$

где $\sigma^2_{8\times8}(\mathrm{m},\mathrm{n})$ – локальная дисперсия $I_t(m,n)$ в окне 8×8 пикселей. В ходе исследований использовались $\sigma^2_{\min}$ и $\sigma^2_{\max}$, равные соответственно 1 и 4.

3.2. Пропуск кадров при встраивании информации

Для некоторых типов видеофрагментов рассмотренный выше способ не способен обеспечить низкую визуальную различимость встроенной информации даже при $\alpha=1$. К таким видеопоследовательностям относятся фрагменты, в которых бóльшая часть кадра имеет постоянную яркость (т.е. значение локальной дисперсии для большинства пикселей кадра близка к нулю). Это могут быть пустые фрагменты (затемнения или осветления экрана между сценами), экраны с титрами, сцены на постоянном фоне и пр. Для таких фрагментов встраивание информации не производится, то есть используется $\alpha=0$.

Пропуск кадра может также осуществляться на основе анализа локальной дисперсии:

$$\frac{1}{MN}\sum_{m,n}\sigma^2_{8\times 8}(m,n) \le \alpha D_{skip},$$

то есть кадр пропускается, если средняя по кадру локальная дисперсия не превышает αD_{skip}.

Данное правило является эвристическим и требует дополнительного исследования, в том числе для уточнения значения D_{skip}. При проведении исследования стойкости предложенного метода (раздел 4) пропуск кадров при встраивании ЦВЗ не проводился.

3.3. «Замораживание» встраиваемой информации в статичных сценах

Рассмотренный выше случай абсолютно постоянной области экрана встречается нечасто, зато нередко возникает ситуация, когда отдельные кадры являются неоднородными по яркости (т.е. обладают высокой локальной дисперсией для большинства пикселей кадров), но при этом видеофрагмент содержит ряд последовательных идентичных кадров. Такая ситуация характерна для статичных сцен, которые в изобилии присутствуют в фильмах любых жанров.

Для таких сцен встроенная информация может быть неразличима при анализе отдельных кадров, но она становится заметной при просмотре всей сцены ввиду того, что шумоподобная компонента $\xi_t^W(m,n)$ псевдослучайно меняется от кадра к кадру. Во избежание подобной ситуации следует применять «замораживание» $\xi_t^W(m,n)$ (то есть фиксацию бита встраиваемой информации) на протяжении всей статичной сцены. В качестве простого критерия необходимости «замораживания» $\xi_t^W(m,n)$ может использоваться выражение

$$\Delta_t = \sum_{m=1}^{M}\sum_{n=1}^{N}\left|I_t(m,n) - I_{t-1}(m,n)\right| \le \tau_\Delta. \qquad (9)$$

Если неравенство (9) выполняется, то $\xi_t^W(m,n) = \xi_{t-1}^W(m,n)$.

4. Экспериментальные исследования разработанного алгоритма

4.1. Стойкость к атакам, основанным на оценке встроенной информации

В целях проверки стойкости разработанного метода к рассмотренным во введении видам атак была проведена серия экспериментов, направленная на выявление наличия статической шупомодобной компоненты $D'(n,m)$, вносимой в исходную видеопоследовательность при аддитивном встраивании ЦВЗ.

В первом из этих экспериментов оценивалось среднее значение коэффициента корреляции между значениями $D'(n,m)$, вычисление которой проводилось в два этапа. Сначала оценивались шумоподобные компоненты каждого кадра по формуле

$$D'_t(n,m) = I_t(m,n) - I'_t(m,n). \qquad (10)$$

Затем для всех t вычислялось максимальное значение ВКФ $C_{\max}(t)$ между $D'_t(n,m)$ и $D'_{t+1}(n,m)$. Полученное значение характеризует схожесть шумоподобных компонент, вносимых при встраивании информации в соседние кадры видеопоследовательности, и позволяет оценить статичность этих компонент.

Если для любого t значение $C_{\max}(t)$ близко к нулю, то можно предполагать, что нарушитель не сможет приближённо вычислить шумоподобную компоненту $D'(n,m)$ (общую для всех кадров), используя только набор последовательных кадров видео, содержащего встроенную информацию. С другой стороны, если значение $C_{\max}(t)$ близко к 1 для достаточно широкого диапазона t (т.е. одно и то же значение $D'(n,m)$ повторяется для всех кадров из заданного диапазона), то атакующий сможет полностью или частично извлечь ЦВЗ.

В ходе эксперимента среднее значение $C_{\max}(t)$, рассчитанное по видео длиной $T = 1000$ кадров, составило 0,0221, в то время как минимальное и максимальное значения составили –0,034 и 0,03 соответственно. Полученные результаты позволяют заключить, что метод устойчив к атакам с приближённым вычислением ЦВЗ, т.к. значения $D'_t(n,m)$ для соседних кадров являются практически некоррелированными.

Кроме того, если значения x, y, $x-x'$, $y-y'$ (4) выбираются случайно и независимо для каждого кадра видеопоследовательности, то можно утверждать, что процедура встраивания ЦВЗ не порождает никаких периодически повторяющихся шумоподобных компонент видеопоследовательности ни во временной, ни в пространственной области. В отличие от методов, предложенных в [2, 5, 6], подобных результатов удаётся добиться даже при использовании постоянного ключа встраивания для всех кадров видеопоследовательности.

4.2. Исследование работоспособности предложенной системы на неискажённом видео

В следующем эксперименте исследовалось количество кадров, необходимое для полностью корректного извлечения скрытой информации из неискажённых видео различного характера и при различных $\alpha \in [2;8]$. Использовались 5 типов видео:

1) «артхаусный фильм» – видеопоследовательность, содержащая длительные фрагменты, снятые неподвижной или медленно движущейся камерой;
2) «дорожное видео» – видео с непрерывно меняющимся пейзажем, снятое из движущегося транспортного средства;
3) «семейный фильм» – видео, содержащее часто сменяющиеся сцены средней активности, преимущественно диалоги;
4) «остросюжетный фильм» – видео, содержащее часто сменяющиеся сцены с высокой активностью;
5) «футбольная трансляция».

В каждое видео (с размером кадра 640×480) встраивался 64-битный ЦВЗ: $N'=M'=8$; при извлечении использовался порог $\tau = 0{,}02$. На рис. 1 показаны результаты проведённого исследования.

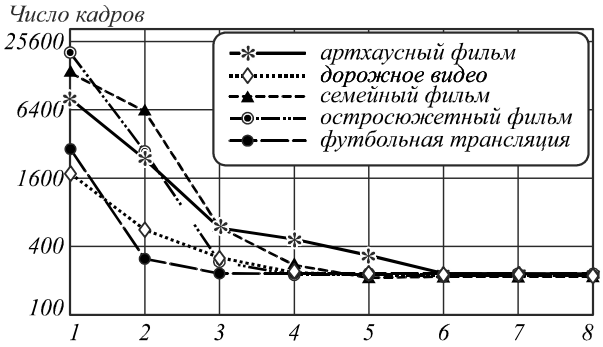


Рис. 1. Количество кадров, достаточное для безошибочного извлечения встроенной информации для разных типов видео и при различных α

Как видно, искомое минимальное число кадров уменьшается с увеличением α; для всех типов видео безошибочное извлечение встроенной информации возможно осуществить за разумное время (в худшем случае – менее, чем за две минуты видео при 30 кадрах в секунду). Таким образом, полученные результаты подтверждают работоспособность предложенной системы для всех типов видео.

На рис. 2 показаны усреднённые показатели визуального качества видеопоследовательностей после встраивания информации при различных значениях α, использовавшихся в ходе данного эксперимента. Последний является основанной на *PSNR* мерой, разработанной с учётом особенностей зрительной системы человека [14]. Значения показателей, представленные на рис. 2, усреднялись по 1000 кадров анализируемых видеопоследовательностей. Как показывает график, для всех рассмотренных α показатели качества принимают допустимые значения, однако практически неразличимым водяной знак становится при $\alpha \leq 3$.

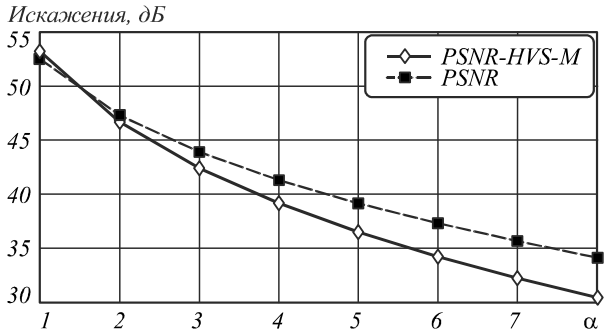


Рис. 2. Усреднённое качество видео после встраивания информации при различных α

На рис. 3 показаны примеры одного и того же кадра из видеопоследовательности «артхаусный фильм» без ЦВЗ и с ЦВЗ при различных α.

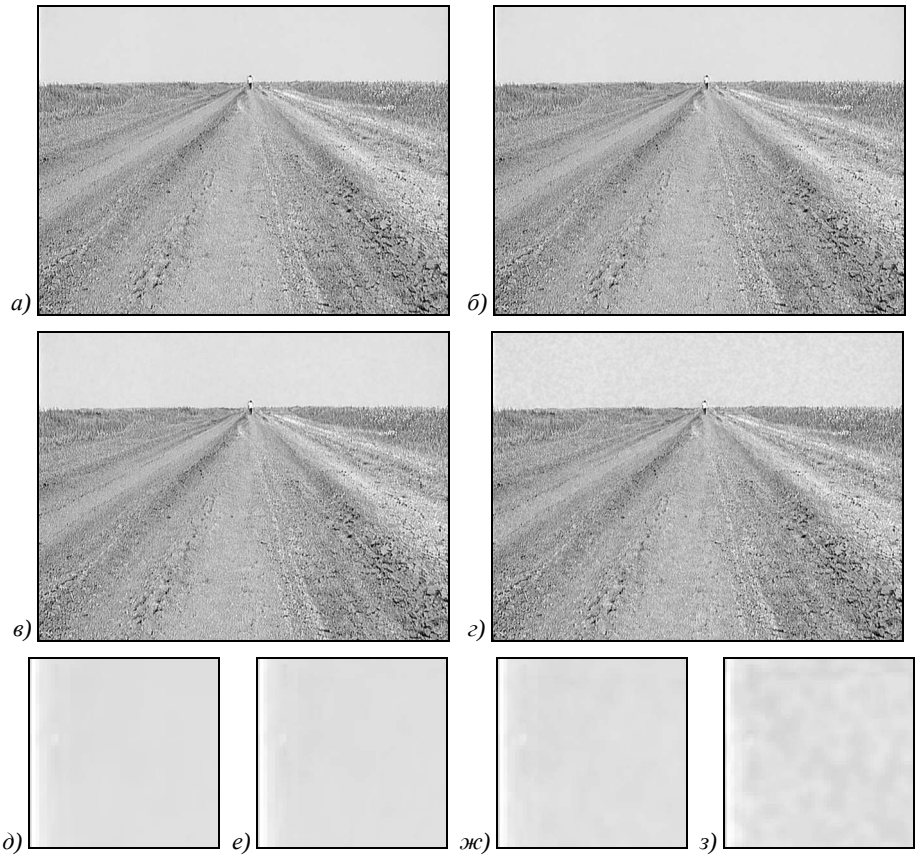


Рис. 3. Кадр видео до встраивания ЦВЗ (а) и после встраивания с параметрами α = 1, α = 3, α = 8 (б)–(г), а также увеличенные фрагменты однородной области кадра (д)–(з)

4.3. Устойчивость к потере кадров и попиксельным искажениям

Далее было проведено исследование стойкости предложенной системы к искажениям видео и потере данных. В эксперименте использовался видеофрагмент «артхаусный фильм»; параметры ЦВЗ и значение порога идентичны предыдущему эксперименту.

После встраивания информации случайным образом были удалены 10 % кадров. Полученный в результате набор кадров обозначим *Set 0*. Далее на основе *Set 0* были сформированы ещё три набора видео:

1. *Set A*: результат обрезки кадров Set 0 на 5 % площади кадра.

2. *Set B*: результат покадрового JPEG-сжатия с параметром качества $Q = 75$.

3. *Set C*: результат сжатия видео в MPEG-4 с кодеком H.264 и параметром качества $Q = 75$.

Как и в предыдущем эксперименте, эти 4 набора формировались для различных α, и далее оценивалось количество кадров, достаточное для полностью корректного извлечения ЦВЗ. Результаты исследования приведённые на рис. 4, показывают, что даже в худшем случае для точного извлечения достаточно не более 6500 кадров (менее четырёх минут) видеопоследовательности.

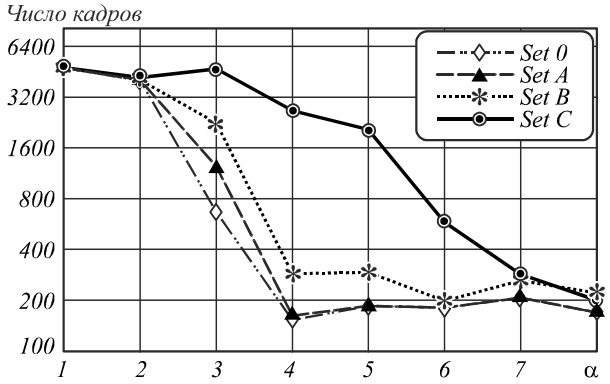


Рис. 4. Количество кадров, достаточное для безошибочного извлечения встроенной информации из множеств кадров Set 0, Set A, Set B, Set C искажённого видео при различных α

4.4. Исследование кодовой скорости в сравнении со схемой Дэйви и МакКея

Также в ходе исследования предложенного метода было проведено его сравнение с существующим методом избыточного кодирования (Дэйви и МакКей, [15]), позволяющим обеспечить целостность встроенного ЦВЗ в условиях возможного пропуска отдельных кадров видеопоследовательности.

В ходе проводимого сравнения методов схема встраивания, предложенная в разделах 1 и 2, была использована для встраивания ЦВЗ во все кадры тестовой видеопоследовательности, при этом каждый кадр видеопоследовательности после встраивания содержал 17-битный фрагмент ЦВЗ, сформированный согласно (1). Для встраивания 17-битного фрагмента S_i использовались два типа модуляции, рассмотренные ранее в подразделе 2.1. Во-первых, один из бит встраивался путём выбора одной из двух шумоподобных последовательностей Q_1 and Q_2. Во-вторых, по 8 бит информации встраивались путём выбора значений смещений $x - x'$ и $y - y'$ из диапазона [0,255] (согласно (4)).

Таким образом, используя указанные способы модуляции, можно встраивать в видеопоследовательность ЦВЗ различного объёма, варьируя при этом значения B_I и B_H (при этом следует учитывать ограничение, накладываемое на общий объём фрагмента S_i: $B_I + B_H = 17$).

В то же время ЦВЗ, устойчивый к пропуску отдельных кадров видеопоследовательности, мог быть встроен в тестовую видеопоследовательность с использованием схемы избыточного кодирования Дейви и МакКея [15]. Действительно, информационная последовательность *H*, используемая в качестве ЦВЗ, может быть подвергнута избыточному кодированию согласно [15], после чего разбита на 17-битные фрагменты и встроена в видеопоследовательность. При этом в процессе встраивания ЦВЗ используются те же способы модуляции, что и для формирования 17-битных фрагментов ЦВЗ S_i, но при этом разбиение ЦВЗ на фрагменты (согласно разделу 2) не производится.

Предложенный метод и метод кодирования Дейви и МакКея сравнивались по значению *кодовой скорости R*, равной отношению количества бит ЦВЗ к общему количеству встроенной информации [15]. Таким образом, с точки зрения максимизации объёма встраиваемого ЦВЗ наилучшим будет метод с более высоким значением *R*. Для предложенного в разделах 2 и 3 метода встраивания объём встроенного ЦВЗ равен объёму информационной последовательности *H*, а общий объем встроенной информации равен $17 \cdot T$, где T, как и прежде, количество кадров видео, в которые производилось встраивание 17-битных фрагментов ЦВЗ. Данные о кодовой скорости метода Дэйви и МакКея были почерпнуты из первоисточника [15].

Экспериментальное сравнение кодовой скорости методов осуществлялось при следующих условиях. Для различных значений вероятности пропуска (удаления) кадра $P_{skip} = \{0,1; 0,2; 0,3\}$ видеопоследовательности со встроенным фрагментом ЦВЗ экспериментальным путём были найдены параметры метода встраивания, обеспечивающие вероятность корректного извлечения полного ЦВЗ из повреждённой видеопоследовательности не менее $P_{ext} = 0,999$. Аналогично выбор параметров кодирования ЦВЗ производился для метода Дейви и МакКея. Далее с учётом найденных параметров обоих методов был произведён расчёт показателя кодовой скорости *R*. Результаты исследования приведены в табл. 1.

Проведённый эксперимент показал, что метод Дейви и МакКея обладает лучшей кодовой скоростью при $P_{skip} = 0,1$ для кодирования ЦВЗ объёмом более

704 бит. В то же время для объёма ЦВЗ до 704 бит предложенный метод встраивания обеспечивает более высокую кодовую скорость и позволяет восстанавливать исходную информационную последовательность H при значениях P_{skip} до 0,3 включительно. Кроме того, метод Дэйви и МакКея, согласно [15], обладает высокой вычислительной сложностью (процедура декодирования 5000-битного ЦВЗ требует до 200 секунд машинного времени), в то время как предложенный в разделах 1-2 метод разделения ЦВЗ основан на простейшей операции генерации псевдослучайного бинарного вектора заданной длины.

Таблица. 1. Сравнение кодовых скоростей, достаточных для достижения P_{ext}=0,999, для разных схем

Схема модуляции или кодирования ЦВЗ (λ – длина информационной последовательности H в битах)	Кодовая скорость R, достаточная для достижения P_{ext}=0,999		
	$P_{skip}=0,1$	$P_{skip}=0,2$	$P_{skip}=0,3$
Предложенный метод, $B_I=3$, $B_H=14$, λ =112	0,085	0,075	0,066
Предлагаемая система, $B_I=4$, $B_H=13$, λ =208	0,061	0,054	0,047
Предлагаемая система, $B_I=5$, $B_H=12$, λ=384	0,057	0,050	0,043
Предлагаемая система, $B_I=6$, $B_H=11$, λ=704	0,052	0,046	0,040
Предлагаемая система, $B_I=7$, $B_H=10$, λ=1280	0,044	0,039	0,034
Метод Дэйви и МакКея [15] (L – произвольное)	0,05	нет данных	нет данных

Заключение

В работе предложены новый метод псевдослучайного распределения информации при сокрытии её в видеосигнале, а также система встраивания информации в видео, в которой реализован данный метод. Показано, что данная система обладает повышенной информационной ёмкостью, устойчива к ошибкам потери синхронизации (пропуск отдельных кадров и изменение порядка следования кадров) и обладает высокой стойкостью к атакам с приближённым вычислением ЦВЗ. Проведённые эксперименты показали, что система обладает высокой стойкостью к искажающим преобразованиям, таким как кадрирование и сжатие с потерями, и позволяет корректно восстанавливать встроенный ЦВЗ при удалении до 30 % кадров видеопоследовательности (согласно данным в табл. 1). Кроме того, экспериментально доказано, что предложенный алгоритм встраивания позволяет достичь более высокой кодовой скорости, нежели известный алгоритм Дэйви и МакКея [15], для информационных сообщений, не превышающих 704 бита.

Благодарности

Работа выполнена при поддержке РФФИ (гранты 12-01-00822, 12-07-00021, 12-07-31056, 13-01-12080, 13-01-97007), гранта президента РФ МК-3863.2013.9. и Минобрнауки РФ в рамках реализации мероприятий Программы повышения конкурентоспособности СГАУ среди ведущих мировых научно-образовательных центров на 2013-2020 годы.

Литература

1. **Pavel, G.** Embedding, Extraction and Detection of Digital Watermark in Spectral Images: PhD Thesis / G. Pavel. – Lappeenranta: Lappeenranta University of Technology, 2005.
2. **Doërr, G.** Security pitfalls of frame-by-frame approaches to video watermarking / G. Doërr, J.L. Dugelay // IEEE Transactions on Signal Processing. – 2004. – V. 52(10). – P. 2955-2964.
3. **Chen, C.** Temporal statistic based video watermarking scheme robust against geometric attacks and frame dropping / C. Chen, J. Ni, J. Huang // Digital Watermarking. – Springer, 2009. – P. 81-95.
4. **Sun, S.W.** Video watermarking synchronization based on profile statistics / S.W. Sun, P.C. Chang // Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology. – 2003. – P. 410-413.
5. **Holliman, M.J.** Robust frame-dependent video watermarking / M.J. Holliman, W.W. Macy, M.M. Yeung // Proceedings of SPIE 3971, Security and Watermarking of Multimedia Contents II. – 2000. – P. 186-197.
6. **Lin, E.T.** Temporal synchronization in video watermarking / E.T. Lin, E.J. Delp // IEEE Transactions on Signal Processing. – 2004. – V. 52(10). – P. 3007-3022.
7. **Delannay, D.** Classification of watermarking schemes robust against loss of synchronization / D. Delannay, B. Macq // Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – P. 581-591.
8. **Delannay, D.** Digital watermarking algorithms robust against loss of synchronization. PhD Thesis / D. Delannay. – Louvain: Universite catholique de Louvain, 2004.
9. **Herrigel, A.** Watermark template attack / A. Herrigel, S.V. Voloshynovskiy, Y.B. Rytsar // Proceedings of SPIE 4314, Security and Watermarking of Multimedia Contents III. – 2001. – P. 394–405.
10. **Lin, E.T.** Spatial synchronization using watermark key structure / E.T. Lin, E.J. Delp // Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – P. 536-547.
11. **Tsai, D.M.** Fast normalized cross correlation for defect detection / D.M. Tsai, C.T. Lin // Pattern Recognition Letters. – V. 24(15). – 2003. – P. 2625-2631.
12. **O'Ruanaidh, J.J.K.** Rotation, scale and translation invariant digital image watermarking / J.J.K. O'Ruanaidh, T. Pun // Proceedings of International Conference on Image Processing. – V. 1. – 1997. – P. 536-539.
13. **Barni, M.** Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications / M. Barni, F. Bartolini. – Marcel Dekker, 2004.
14. **Ponomarenko, N.** On between-coefficient contrast masking of DCT basis functions / N. Ponomarenko, F. Silvestri, K. Egiazarian, M. Carli, J. Astola, V. Lukin // Proceedings of the Third International Workshop on Video Processing and Quality Metrics. – 2007. – V. 4. – 4 p.

15. **Davey, M.C.** Reliable communication over channels with insertions, deletions, and substitutions / M.C. Davey, D.J.C. MacKay // IEEE Transactions on Information Theory. – V. 47(2). – 2001. – P. 687-698.
16. **Глумов, Н.И.** Модифицированный метод защиты цифровых изображений с помощью стойких ЦВЗ с повышенными информационной емкостью и устойчивостью к искажениям изображений / Н.И. Глумов, В.А. Митекин // Доклады 9-й Международной конференции «Интеллектуализация обработки информации». – 2012. – С. 320-323.

References

1. **Pavel, G.** Embedding, Extraction and Detection of Digital Watermark in Spectral Images: PhD Thesis / G. Pavel. – Lappeenranta: Lappeenranta University of Technology, 2005.
2. **Doërr, G.** Security pitfalls of frame-by-frame approaches to video watermarking / G. Doërr, J.L. Dugelay // IEEE Transactions on Signal Processing. – 2004. – V. 52(10). – P. 2955-2964.
3. **Chen, C.** Temporal statistic based video watermarking scheme robust against geometric attacks and frame dropping / C. Chen, J. Ni, J. Huang // Digital Watermarking. – Springer, 2009. – P. 81-95.
4. **Sun, S.W.** Video watermarking synchronization based on profile statistics / S.W. Sun, P.C. Chang // Proceedings of IEEE 37th Annual 2003 International Carnahan Conference on Security Technology. – 2003. – P. 410-413.
5. **Holliman, M.J.** Robust frame-dependent video watermarking / M.J. Holliman, W.W. Macy, M.M. Yeung // Proceedings of SPIE 3971, Security and Watermarking of Multimedia Contents II. – 2000. – P. 186-197.
6. **Lin, E.T.** Temporal synchronization in video watermarking / E.T. Lin, E.J. Delp // IEEE Transactions on Signal Processing. – 2004. – V. 52(10). – P. 3007-3022.
7. **Delannay, D.** Classification of watermarking schemes robust against loss of synchronization / D. Delannay, B. Macq // Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – P. 581-591.
8. **Delannay, D.** Digital watermarking algorithms robust against loss of synchronization. PhD Thesis / D. Delannay. Louvain: Universite catholique de Louvain, 2004.
9. **Herrigel, A.** Watermark template attack / A. Herrigel, S.V. Voloshynovskiy, Y.B. Rytsar // Proceedings of SPIE 4314, Security and Watermarking of Multimedia Contents III. – 2001. – P. 394–405.
10. **Lin, E.T.** Spatial synchronization using watermark key structure / E.T. Lin, E.J. Delp // Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2004. – P. 536-547.
11. **Tsai, D.M.** Fast normalized cross correlation for defect detection / D.M. Tsai, C.T. Lin // Pattern Recognition Letters. – V. 24(15). – 2003. – P. 2625-2631.
12. **O'Ruanaidh, J.J.K.** Rotation, scale and translation invariant digital image watermarking / J.J.K. O'Ruanaidh, T. Pun // Proceedings of International Conference on Image Processing. – V. 1. – 1997. – P. 536-539.
13. **Barni, M.** Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications / M. Barni, F. Bartolini. – Marcel Dekker, 2004.
14. **Ponomarenko, N.** On between-coefficient contrast masking of DCT basis functions / N. Ponomarenko, F. Silvestri, K. Egiazarian, M. Carli, J. Astola, V. Lukin // Proceedings of the Third International Workshop on Video Processing and Quality Metrics. – 2007. – V. 4. – 4 p.
15. **Davey, M.C.** Reliable communication over channels with insertions, deletions, and substitutions / M.C. Davey, D.J.C. MacKay // IEEE Transactions on Information Theory. – V. 47(2). – 2001. – P. 687-698.
16. **Glumov, N.I.** Modified high-capacity digital image watermarking algorithm with robust to image distortions / N.I. Glumov, V.A. Mitekin // Proceedings of the 9th International Conference “Intelligent Information Processing”. – 2012. – P. 320-323. – (In Russian).

A NEW ROBUST INFORMATION HIDING METHOD FOR VIDEO

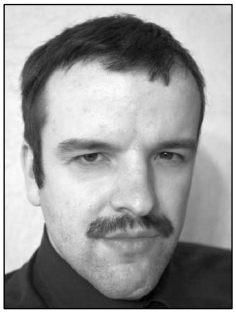
V.A. Mitekin, V.A. Fedoseev
Image Processing Systems Institute, Russian Academy of Sciences,
S.P. Korolyov Samara State Aerospace University

Abstract

A new method for information hiding in digital video is presented in this paper. The proposed method is based on multi-bit frame-by-frame information hiding technique and does not require a temporal synchronization during blind information extraction. This means, proposed method provides hidden information robustness against both malicious and non-malicious frame dropping (temporal desynchronization). A new approach to randomized distribution of hidden information bits across the video frames was implemented to increase method’s embedding capacity compared to known video watermarking and information hiding techinques, robust again temporal desynchronization. Provided experimental results shows that proposed method provides hidden information robustness against frame cropping, frame loss and lossy compression using MPEG-4 and MJPEG algorithms. The proposed method is also highly robust against known “watermark estimation” attack aimed at estimation of hidden information without knowing the embedding key or non-watermarked video. Proposed information hiding method was also compared with Davey - MacKay “watermark code” redundand coding algorithm, which is also aimed at “frame loss” error correction. As a result, proposed method showed better code rates when used for small (up to 704 bits) message length.

Key words: information hiding, video watermarking, watermark synchronization, spread spectrum watermarking, robust watermark.

Сведения об авторах



Митекин Виталий Анатольевич, 1983 года рождения. В 2006 году окончил Самарский государственный аэрокосмический университет (СГАУ) по специальности «Прикладная математика и информатика», кандидат технических наук (2009). В настоящее время работает научным сотрудником в Институте систем обработки изображений РАН и ассистентом кафедры геоинформатики и информационной безопасности СГАУ. Круг научных интересов включает обработку изображений и распознавание образов, стеганографию и стегоанализ, криптографию.

E-mail: *mitekin@smr.ru* .

Vitaly Anatolyevich Mitekin (b. 1983) graduated from S.P. Korolyov Samara State Aerospace University (SSAU), in 2006 majoring in Applied Mathematics and Informatics. He received his Candidate in Technical Sciences degree from Samara State Aerospace University in 2009. Currently he is a research scientist in the Image Processing Systems Institute of the Russian Academy of Sciences and assistant professor at the Geoinformatics and Information Security department at SSAU. His scientific interests include image processing and recognition, steganography and steganalysis, cryptography.

*Сведения об авторе **Федосеев Виктор Андреевич** – см. стр. 563 этого номера.*

Поступила в редакцию 27 мая 2014 г.