АЛГОРИТМ ГЕНЕРАЦИИ СТОЙКОГО ЦИФРОВОГО ВОДЯНОГО ЗНАКА ДЛЯ ЗАЩИТЫ ГИПЕРСПЕКТРАЛЬНЫХ ИЗОБРАЖЕНИЙ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

В.А. Митекин

Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет) (СГАУ), Самара, Россия,
Институт систем обработки изображений РАН, Самара, Россия

Аннотация

В работе представлены новые алгоритмы генерации, встраивания и извлечения стойкого цифрового водяного знака в гиперспектральные изображения дистанционного зондирования Земли. Предлагаемый алгоритм генерации ЦВЗ предполагает генерацию двумерного шумоподобного изображения (шаблона встраивания), кодирующего ЦВЗ, на основе пароля (секретного ключа) пользователя. Предложенные алгоритмы обладают рядом преимуществ по сравнению с существующими аналогами. В частности, предложенный алгоритм генерации шаблонов встраивания на основе пароля обеспечивает высокую устойчивость встроенного цифрового водяного знака к атакам прямого перебора ключа (сложность атаки подбора ключа составляет 10^{14} попыток извлечения по сравнению с $10^4 – 10^5$ попытками для существующих аналогов).

Ключевые слова: цифровой водяной знак, стеганографическая стойкость, стеганографическая атака, информированный детектор ЦВЗ.

Цитирование: **Митекин, В.А.** Алгоритм генерации стойкого цифрового водяного знака для защиты гиперспектральных изображений дистанционного зондирования Земли // Компьютерная оптика. – 2015. – Т. 39, № 5. – С. 808-817. – DOI: 10.18287/0134-2452-2015-39-5-808-817.

Введение

Методы встраивания скрытой информации в цифровые мульти- и гиперспектральные изображения, а также в видеопоследовательности получили распространение в последние два десятилетия в задачах защиты от несанкционированного копирования при помощи встроенного ЦВЗ. Согласно [1] и [2], большинство существующих алгоритмов встраивания ЦВЗ в видеопоследовательности и в мультиспектральные изображения основаны на «покадровом» (поканальном) подходе к встраиванию ЦВЗ. Данный подход предполагает, что и при встраивании, и при извлечении ЦВЗ каждый спектральный канал изображения обрабатывается независимо от других каналов.

Как было показано в работе [3], подобный «покадровый» (поканальный) подход к встраиванию ЦВЗ имеет ряд уязвимостей, которые могут быть использованы для обнаружения и/или удаления встроенного ЦВЗ без знания ключа встраивания.

Так, если один и тот же стеганографический ключ K использовался для встраивания ЦВЗ во все спектральные каналы (или кадры в случае 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) [4], может приближённо вычислить «шумоподобную» компоненту $D'(n,m)$, присутствующую в каждом спектральном канале защищённого гиперспектрального изображения и кодирующую встроенный ЦВЗ. Данная атака становится возможной именно в том случае, когда значение ЦВЗ (а значит, и соответствующее ему значение $D'(n,m)$) одинаково для спектральных каналов. Следует отметить, что в большинстве алгоритмов встраивания стойкого ЦВЗ в видеопоследовательности и последовательности изображений ([5–11]) используется именно «покадровый» (поканальный) подход, следовательно, знание «шумоподобной» компоненты $D'(n,m)$ позволяет атакующему извлечь или удалить ЦВЗ сразу из всех кадров (каналов) защищённого изображения.

Кроме упомянутой атаки на ЦВЗ, водяной знак может быть извлечён или удалён с использованием стратегии т.н. «прямого перебора ключа». В данном случае атакующий пытается последовательно использовать все возможные ключи встраивания ЦВЗ и выбирает в качестве «истинного» тот ключ, который позволил обнаружить и извлечь. В дальнейшем, зная «истинный» ключ встраивания, атакующий может и извлекать, и удалять все ЦВЗ, встроенные с использованием данного ключа.

В качестве примера рассмотрим некоторые алгоритмы встраивания стойкого ЦВЗ, основанные на кодировании с расширением спектра ([12–15]). Данные алгоритмы используют секретный стеганографический ключ для выбора (генерации) М-последовательности или последовательности Касами и далее используют выбранные последовательности для модуляции и кодирования встраиваемого бинарного ЦВЗ. Фактически в данных алгоритмах единственной секретной информацией, требуемой для извлечения ЦВЗ, является использованная для модуляции М-последовательность. При подобном подходе длина используемой М-последовательности приблизительно равна числу пикселей изображения-контейнера: так, для изображения размером 640×480 пикселей необходимо использовать М-последовательность длиной примерно 2^{18} бит. Известно, что число различных последовательностей данной длины ограничено сверху значением функции Эйлера; для М-последовательности длиной 2^{18} бит число разных последовательностей может быть оцене-

но (согласно [16]) как ≈5×10^4. Следовательно, атакующий, знающий об использовании М-последовательностей для модуляции ЦВЗ, может попытаться извлечь ЦВЗ, просто перебирая все различные М-последовательности данной длины. В результате атакующий, используя найденную исходную М-последовательность, может применить атаку с «приближённым вычислением ЦВЗ» (“watermark estimation attack”) [3] и удалить встроенный ЦВЗ с минимальной потерей качества изображения-контейнера.

В данной работе предложены алгоритмы генерации, встраивания и извлечения стойкого цифрового водяного знака в гиперспектральные изображения, стойкие к рассмотренным выше преднамеренным атакам на встроенный ЦВЗ.

В параграфе 1 рассмотрен непосредственно алгоритм встраивания и извлечения ЦВЗ, использующий для кодирования ЦВЗ набор двумерных шумоподобных шаблонов с гарантированно большим значением минимального циклического расстояния Хэмминга. В параграфе 2 рассмотрен алгоритм генерации подобных двумерных шумоподобных шаблонов большого объёма (до нескольких миллионов пикселей) на основе пароля пользователя. В параграфе 3 приведены результаты экспериментального исследования стойкости разработанных алгоритмов к различным видам атак и искажающих преобразований. Как экспериментально показано в параграфе 3, использование подобных шаблонов позволяет практически полностью избежать возникновения коллизий при извлечении ЦВЗ (в ходе эксперимента не было обнаружено ни одной коллизии). Предложенный алгоритм генерации двумерных шаблонов также позволяет повысить сложность атаки подбора ключа до 10^{14} попыток извлечения ЦВЗ атакующим.

1. Алгоритмы встраивания и извлечения ЦВЗ

Предлагаемые алгоритмы предназначены для встраивания и извлечения ЦВЗ повышенной информационной ёмкости в цифровые видеопоследовательности и наборы изображений (в том числе гиперспектральные изображения). Как утверждается в [1] и [4], метод встраивания скрытой информации является уязвимым к атаке с приближённым вычислением ЦВЗ в том случае, если встраиваемая информационная последовательность и ключ встраивания одинаковы для всех кадров (спектральных каналов). 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 (спектрального канала). Такой подход обеспечивает отсутствие статичной шумоподобной составляющей во всех спектральных каналах изображения, тем самым обеспечивая стойкость ЦВЗ к упомянутой выше атаке. Кроме того, как будет показано ниже, такое распределение бит ЦВЗ между спектральными каналами позволяет повысить объём встраиваемой информации.

Рассмотрим более подробно способ предварительного кодирования встраиваемой информации, основанный на указанном подходе, изложенный ранее в работе [17]. 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 спектральный канал изображения 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:

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

Здесь $i_0 i_1 ... i_{B_I - 1}$ – 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 в отдельный кадр.

Алгоритм встраивания отдельного фрагмента S_i в изображение (отдельный спектральный канал) основан на модуляции с расширением спектра встраиваемой битовой последовательности и предполагает кодирование бит информационной части фрагмента S_i за счёт выбора модулирующей двумерной последовательности, а кодирование индексной части фрагмента – за счёт циклического сдвига выбранной модулирующей последовательности. Пусть $I_t(n, m)$ – t-й спектральный канал изображения, при этом размер изображения составляет $N \times M$ пикселей, а общее число спектральных каналов известно и равно T: $t \in [0, T-1]$. Пусть информационная последовательность H, рассмотренная ранее, представляет собой бинарное изображение $W(x,y)$ размером $N' \times M'$ пикселей, где $N' < N$, $M < M'$ и $N' \times M' = L$.

Перед непосредственным выполнением алгоритма встраивания ЦВЗ секретный ключ встраивания используется для генерации двух двумерных шумоподобных шаблонов встраивания с гарантированно

большим значением минимума циклического расстояния Хэмминга (примером таких одномерных шаблонов являются М-последовательности или оптические ортогональные коды). Полученные в результате генерации двумерные массивы M_1 и M_0 имеют размер $N \times M$ (т.е. их размер равен размеру изображения-контейнера). Более подробно алгоритм генерации рассмотрен в параграфе 3.

Далее информационный бит $W(x, y)$ фрагмента S_t встраивается в t-й спектральный канал по следующему правилу:

$$I_t^{'}(n,m)=\begin{cases} I_t(n,m)-\alpha\cdot\widehat{S}_{x,y}(M_1), & \text{если } W(x,y)=1, \\ I_t(n,m)-\alpha\cdot\widehat{S}_{x,y}(M_0), & \text{если } W(x,y)=0, \end{cases} \quad (2)$$

где $\widehat{S}_{x,y}$ – операция двумерного циклического сдвига массива (M_1 или M_0) на x столбцов и y строк, $I'_t(n,m)$ – t-й кадр видеопоследовательности после встраивания фрагмента ЦВЗ. Значения $x \in [0, M-1]$ и $y \in [0, N-1]$ выбираются случайным образом независимо для каждого кадра видеопоследовательности.

В результате предыдущей операции каждый спектральный канал изображения содержит ровно один бит исходного ЦВЗ $W(x,y)$, т.е. информационная часть встроенного фрагмента S_t состоит из одного бита. Последовательность, в которой биты $W(x,y)$ встроены в каналы изображения-контейнера, является случайной и полностью определяется значениями x и y. Таким образом, индексная часть фрагмента S_t представлена именно значениями x и y , и эти значения также встраиваются в изображение путём модуляции циклического сдвига массивов M_1 и M_0.

Описанная выше схема встраивания обуславливает также свойство избыточности ЦВЗ – один и тот же бит $W(x, y)$ может быть встроен в несколько случайно выбранных спектральных каналов.

Выражение (2) показывает, что процедура встраивания ЦВЗ, обычно самая вычислительно затратная в схемах защиты с помощью ЦВЗ, в данном случае представляет собой короткую последовательность простых операций: двумерного циклического сдвига и попиксельного сложения двух изображений. Кроме того, процедура встраивания не требует загрузки всего гиперспектрального изображения, а позволяет работать с его отдельным спектральным каналом.

Алгоритм извлечения изображения-ЦВЗ $W'(x, y)$ из отдельного спектрального канала $I'_t(n,m)$ может быть построен на основе быстрой процедуры вычисления взаимной корреляционной функции $C_t(\Delta n, \Delta m)$ [18], где $\Delta n \in [0, N-1], \Delta m \in [0, M-1]$ – значения циклического сдвига (в пикселях) изображения $I_t^{'}(n,m)$ по вертикали и горизонтали соответственно. Аналогично вычисляется взаимная корреляционная функция $\hat{C}_t(\Delta n, \Delta m)$ между изображением $I_t^{'}(n,m)$ и массивом M_1. Далее значения $\hat{C}_t(\Delta n, \Delta m)$ и $C_t(\Delta n, \Delta m)$ усредняются по всем спектральным каналам:

$$\begin{aligned} C_{mean}(\Delta n, \Delta m) &= \frac{1}{T}\sum_{1}^{t=T} C_t(\Delta n, \Delta m), \\ \hat{C}_{mean}(\Delta n, \Delta m) &= \frac{1}{T}\sum_{1}^{t=T} \hat{C}_t(\Delta n, \Delta m). \end{aligned} \quad (3)$$

После вычисления усреднённых значений извлечённое изображение-ЦВЗ $W'(x, y)$ может быть вычислено согласно следующему выражению:

$$W'(x,y)\begin{cases} 1, \text{если } C_{mean}(x,y) > T_w \\ \qquad AND\ (-T_w) < \hat{C}_{mean}(x,y) < T_w \\ 0, \text{если } \hat{C}_{mean}(x,y) > T_w \\ \qquad AND\ (-T_w) < C_{mean}(x,y) < T_w \\ \text{не определен, иначе} \end{cases}, \quad (4)$$

где $Th \in (0;1)$ – порог обнаружения.

2. Генерация двумерных шумоподобных шаблонов для встраивания ЦВЗ

В данном параграфе описан алгоритм генерации двумерных шумоподобных шаблонов с гарантированно большим значением минимального циклического расстояния Хэмминга. Предложенный алгоритм основан на алгоритме генерации ортогональных оптических кодов с кодовыми словами большой битовой длины [20]. Также в данном параграфе исследуются ключевые свойства генерируемых двумерных шаблонов, такие как число возможных различных шаблонов заданного размера, максимальные значения взаимно-корреляционной функции и автокорреляционной функции.

Одномерные последовательности и двумерные шаблоны для встраивания ЦВЗ, генерируемые на основе секретного ключа, широко применяются на этапе модуляции и кодирования стойкого ЦВЗ. В частности, такие последовательности применяются при встраивании ЦВЗ с «информированным» детектором водяного знака («информированный» детектор лишь подтверждает наличие в сигнале встроенной заранее известной последовательности). Выбор алгоритма генерации подобных последовательностей может оказать значительное влияние и на устойчивость встроенного ЦВЗ к искажениям, и на его стойкость к преднамеренным атакам, и на вероятность коллизии (вероятность успешного извлечения ЦВЗ с неправильным секретным ключом).

В работах [21] и [22] подробно формулируются требования к одномерным и двумерным ключевым (т.е. генерируемым на основе секретного ключа встраивания) последовательностям, используемым при встраивании ЦВЗ. Так, предполагается, что минимальное циклическое расстояние Хэмминга ([23]) между двумя любыми ключевыми последовательностями заданного размера должно быть пропорционально длине ключевой последовательности в битах и не может быть равно нулю. В работе [15] показано, что именно это требование позволяет обеспечить устойчивость ЦВЗ к преднамеренным и случайным коллизиям при

извлечении ЦВЗ. Под коллизией в данном случае понимается ситуация, когда встраивание ЦВЗ производится с использованием одного секретного ключа встраивания, а извлечение может быть произведено несколькими «ложными» ключами, близкими к исходному по критерию расстояния Хэмминга.

В качестве примера можно рассмотреть тривиальный случай, когда в качестве ключевой последовательности используется пароль пользователя, приведённый к виду битовой строки. В данном случае минимальное циклическое расстояние Хэмминга между двумя произвольными ключевыми последовательностями равно 0; вероятность коллизии при извлечении ЦВЗ при этом максимальна (среди всех типов ключевых последовательностей заданной длины).

Для большинства алгоритмов встраивания ЦВЗ в изображения необходимо использование не одномерных, а двумерных ключевых последовательностей. В данном случае ключевая последовательность предварительно преобразуется в двумерное шумоподобное изображение-«шаблон», аддитивно встраиваемое – в изображение-контейнер.

Предложенный в работе алгоритм генерации ключевых последовательностей позволяет, с одной стороны, обеспечить низкую (по сравнению с тривиальным случаем, рассмотренным выше) вероятность коллизий за счёт регулируемого минимального циклического расстояния Хэмминга ([23]). С другой стороны, по числу различных ключевых последовательностей заданной длины (а значит, и по устойчивости к атакам прямого перебора ключа) предложенный алгоритм значительно превосходит существующие аналоги. В пункте 2.1 рассматривается первый этап алгоритма, результатом которого является генерация одномерной ключевой последовательности. В пункте 2.2 рассмотрен второй этап алгоритма, позволяющий увеличить длину ключевой последовательности до нескольких миллионов бит без значительного увеличения вычислительной сложности алгоритма генерации.

2.1. Алгоритм генерации одномерных ключевых последовательностей с фиксированным минимальным циклическим расстоянием Хэмминга

В данном разделе рассматривается первый этап алгоритма генерации ключевых последовательностей, предназначенных для встраивания стойких ЦВЗ. На первом этапе секретный пароль пользователя преобразуется в одномерную ключевую последовательность с фиксированным минимальным циклическим расстоянием Хэмминга. В свою очередь, первый этап алгоритма, рассмотренный в данном разделе, может быть разбит на следующие шаги.

На первом шаге пароль пользователя, представленный в виде последовательности бит $P = p_1 p_2 p_3 \ldots p_n$, кодируется избыточным БЧХ-кодом с минимальным кодовым расстоянием l. Результатом кодирования является последовательность бит $T_{pass} = t_1 t_2 t_3 \ldots t_{n+k}$ (где биты $t_{n+1} t_{n+2} t_{n+3} .. t_{n+k}$ добавлены в результате избыточного кодирования). Очевидно, что на этом этапе число возможных паролей пользователя длиной n и число соответствующих им бинарных последовательностей T_{pass} равно 2^n. Кроме того, благодаря свойствам БЧХ-кода можно утверждать, что расстояние Хэмминга между двумя любыми последовательностями T'_{pass} и T''_{pass} равной длины больше или равно l, где l – минимальное кодовое расстояние БЧХ-кода, использованного на данном шаге.

На втором шаге для дальнейшего преобразования пароля пользователя в ключевую последовательность C используются бинарный код без запятых, состоящий из четырёх кодовых слов: $\tilde{S} = \{S_{00}, S_{01}, S_{10}, S_{11}\}$ (длина всех кодовых слов равна s бит) и М-последовательность $M = m_1 m_2 m_3 .. m_{n+k}$, где m_i – i-й бит последовательности M, $1 \le i \le n+k$. Ключевая последовательность $C = c_1 c_2 c_3 .. c_{(n+k)s}$ формируется на основе ранее полученной последовательности T_{pass} согласно следующему соотношению:

$$\{c_j c_{j+1} c_{j+2} \ldots c_{j+s-1}\} = \begin{cases} S_{00}, \text{ если } t_i = 0 \text{ and } m_i = 0 \\ S_{01}, \text{ если } t_i = 1 \text{ and } m_i = 0 \\ S_{10}, \text{ если } t_i = 0 \text{ and } m_i = 1 \\ S_{11}, \text{ если } t_i = 1 \text{ and } m_i = 1 \end{cases}, \quad (5)$$

где $j = i \times s$, $1 \le i \le n + k$.

Как было показано в работах [19, 20], ключевая последовательность C, сформированная по правилу (5), представляет собой кодовое слово циклически инвариантного кода $\tilde{C}$, т.е. кода, все кодовые слова которого различимы даже при условии их возможного циклического сдвига [23, 24]. Для подобного класса кодов [24] ключевой характеристикой является именно фиксированное минимальное циклическое расстояние Хэмминга, определяющее возможность корректного различения кодового слова в условиях возможных искажений. В рамках задачи встраивания стойкого ЦВЗ минимальное циклическое расстояние Хэмминга, таким образом, будет определять устойчивость используемых при встраивании ключевых последовательностей к возможным коллизиям при извлечении ЦВЗ, а также к зашумлению изображения-контейнера.

Циклическое расстояние Хэмминга между двумя ключевыми последовательностями C' и C'' длиной L может быть определено как

$$\lambda_{c'c''} = \min_{\Delta h} \sum_{h=1}^{h} c'_h \oplus c''_{h+\Delta h},$$

где $0 \le \Delta h \le L$ и $(h + \Delta h)$ вычисляется по модулю L. Таким образом, если $\lambda_{c'c''}$, то последовательности C' и C'' идентичны при некотором взаимном циклическом сдвиге $0 \le \Delta h \le L$; иначе для любого значения циклического сдвига $0 \le \Delta h \le L$ расстояние Хэмминга между C' и C'' больше или равно $\lambda_{c'c''}$.

Минимальное циклическое расстояние Хэмминга, таким образом, определяется для циклически инвариантного кода $\tilde{C}$ как минимально возможное значение циклического расстояния Хэмминга среди всех возможных пар кодовых слов из кода $\tilde{C}$. В работе [20] было

показано, что для любых двух ключевых последовательностей C' и C'' на основе правила (5) циклическое расстояние Хэмминга не превышает величины

$$\lambda = \min(l \cdot h_s, h_s \cdot (n+k)/2, h_c \cdot (n+k)),$$

где h_c – расстояние Хэмминга без запятых ("comma-free distance"), определяемое для кода без запятых $\tilde{S}$, h_s – минимальное кодовое расстояние кода $\tilde{S}$ (без учёта возможных сдвигов). Некоторые примеры формирования кода без запятых $\tilde{S}$, состоящего из 4 кодовых слов равной длины, приведены в табл. 1.

Кроме того, в работе [20] было показано, что по числу возможных ключевых последовательностей заданной длины рассмотренный в данном разделе код значительно превосходит другие известные циклически инвариантные коды, позволяющие генерировать кодовое слово на основе задаваемого пользователем пароля.

Табл. 1. Примеры кодов без запятых, состоящих из 4 кодовых слов

Длина кодового слова, бит	Расстояние Хэмминга без запятых, h_c	Минимальное кодовое расстояние, h_s	S^{00}	S^{01}	S^{10}	S^{11}
5	1	1	10110	01001	10111	01000
6	1	1	101100	010011	101000	010111
7	2	1	0001101	1110010	0011101	1100010

2.2. Алгоритм преобразования одномерных ключевых последовательностей в двумерные шумоподобные шаблоны для встраивания стойкого ЦВЗ

На втором этапе алгоритма генерации двумерных шумоподобных шаблонов производится непосредственно преобразование сгенерированных на первом этапе одномерных ключевых последовательностей в двумерные бинарные шумоподобные шаблоны с сохранением фиксированного минимального циклического расстояния Хэмминга.

Как показано в [15, 20, 22], существует простой способ биективно отобразить множество всех кодовых слов циклически инвариантного кода на множество двумерных бинарных массивов с заданным минимальным значением циклического расстояния Хэмминга. Так, чтобы преобразовать одномерную ключевую последовательность C в два двумерных шумоподобных шаблона M_0 и M_1, предназначенные для встраивания ЦВЗ согласно требованиям, приведённым в параграфе 1, необходимо выполнить следующие шаги.

На первом шаге необходимо сформировать два временных бинарных массива $R_o(v,h)$ и $R_1(v,h)$ размером $V \times H$ бит, где $H = (n+k)s$, $V \times H = M \times N$, используя алгоритм формирования ортогональных оптических кодов, представленный в [15]. Так, первая строка массивов $R_o(v,h)$ и $R_1(v,h)$ формируется согласно соотношению $R_o(1,h) = C_h$, $R_1(1,h) = C_h$. Далее g-я строка массива $R_o(v,h)$ формируется путём циклического сдвига *(g-1)*-й строки на $g \times q_0$ позиций (где q_0 – простое число и величина $g \times q_0$ вычисляется по модулю целого числа H). Аналогично формируется массив R_1: *(g-1)*-я строка массива формируется путём циклического сдвига предыдущей строки на $g \times q_0$ позиций ($q_1 \neq q_0$ – простое число, умножение $g \times q_0$ производится по модулю H).

В работах [14] и [15] было доказано, что двумерные бинарные массивы $R_o(v,h)$ и $R_1(v,h)$ имеют близкое к максимуму (т.е. к $V \times H$) значение циклического расстояния Хэмминга при ненулевых значениях сдвига (для случая циклического сдвига двумерных массивов предполагается, что массив $R_o(v,h)$ остаётся неизменным, а массив $R_1(v,h)$ циклически сдвигается на Δh строк и Δv столбцов).

На последнем шаге массивы $R_o(v,h)$ и $R_1(v,h)$ преобразуются в шаблоны M_0 и M_1 размером $(N \times M)$ согласно следующему соотношению.

$$\begin{aligned} M_0(u \bmod N, u \bmod M) &= R_0(u \bmod V, u \bmod H) \\ M_1(u \bmod N, u \bmod M) &= R_1(u \bmod V, u \bmod H) \end{aligned}, \quad (6)$$

где $u \in [1, N \cdot M]$.

Данный шаг необходим для формирования шумоподобных шаблонов, размер которых совпадает с размером изображения-контейнера. Такой подход на этапе формирования шумоподобных шаблонов встраивания позволяет значительно упростить процедуру непосредственно встраивания ЦВЗ, а именно избежать ресемплирования или кадрирования изображений в процессе встраивания. Этот факт особенно важен с учётом того, что при встраивании ЦВЗ в гиперспектральные изображения объём изображения, содержащего один спектральный канал, может достигать сотен миллионов пикселей.

Согласно [14] и [15], предложенная последовательность преобразований исходной ключевой последовательности C позволяет сохранить минимальное циклическое расстояние Хэмминга равным λ и для полученных двумерных шаблонов, причём данное циклическое расстояние Хэмминга будет наблюдаться только для нулевых значений сдвига. Отличие построенных двумерных шаблонов от исходных ключевых последовательностей будет заключаться лишь в том, что в случае двумерных шаблонов циклический сдвиг шаблонов также является двумерным, т.е. сдвиг шаблонов производится на Δh строк и Δv столбцов. Учитывая это, а также принимая во внимание тот факт, что полученные шумоподобные шаблоны M_0 и M_1 состоят из V повторений исходной ключевой последовательности C, минимальное циклическое расстояние Хэмминга для шаблонов M_0 и M_1 может быть вычислено как:

$$\lambda_{2d} = V \cdot \min(l \cdot h_s, h_s \cdot (n+k)/2, h_c \cdot (n+k)). \quad (7)$$

Фактически это означает, что не существует таких M_0 и M'_0, что циклическое расстояние Хэмминга между ними меньше λ_{2d}.

На рис. 1 приведён пример сгенерированного согласно (6) бинарного шумоподобного шаблона.

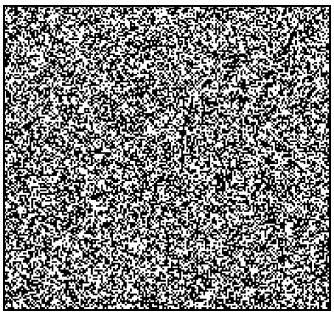

Рис. 1. Пример построенного шумоподобного шаблона для встраивания ЦВЗ

Таким образом, представленный в пунктах 2.1 и 2.2 двухэтапный алгоритм позволяет на основе пароля (секретного ключа) сформировать пару шумоподобных шаблонов M_0 и M_1 для встраивания ЦВЗ. Алгоритм генерации позволяет задавать фиксированное значение минимального циклического расстояния Хэмминга для генерируемых шаблонов, что позволяет значительно снизить вероятность коллизии при извлечении ЦВЗ (согласно [13–15]) и повысить стойкость ЦВЗ к атакам прямого перебора ключа и приближенного вычисления ключа. Как будет показано в следующем параграфе, совместное использование алгоритма предложенного встраивания ЦВЗ (параграф 1) и алгоритма генерации шумоподобных шаблонов (параграф 2) позволяет обеспечить также и устойчивость встроенного ЦВЗ к сжатию изображения-контейнера с потерями.

3. Экспериментальное исследование разработанных алгоритмов

Для исследования стойкости разработанных алгоритмов как к непреднамеренным искажениям, так и к целенаправленным атакам на ЦВЗ был проведён ряд вычислительных экспериментов. Для всех экспериментальных исследований использовались бинарные шаблоны M_0 и M_1 размером 4095×4095 пикселей, основанные на 47-битном пароле (секретном ключе) и избыточном коде БЧХ(4095,47,955). Для построения ключевой последовательности C (см. пункт 2.1) использовался код без запятых, указанный в табл. 1 (длина кодового слова s=5). Согласно (7), минимальное циклическое расстояние Хэмминга для данного класса шумоподобных шаблонов встраивания равно

$$\lambda_{2d} = 819 \cdot \min(1910 \cdot 5, 2047 \cdot 1, 4095 \cdot 1) = 1676493 .$$

Эксперимент по встраиванию ЦВЗ был проведён для 15 гиперспектральных изображений размером 4095×4095 пикселей. Каждое изображение содержало 450 спектральных каналов, встраивание производилось во все каналы. Для оценки влияния интенсивности встраивания на качество исходного изображения процедура встраивания повторялась со значениями интенсивности $\alpha \in [1,8]$ для каждого изображения. Встраиваемый ЦВЗ имел объём 64 бита и представлял собой бинарное изображение $W(x,y)$: $N' = 8$, $M' = 8$. При встраивании ЦВЗ сгенерированные бинарные шаблоны M_0 и M_1 были кадрированы до размера гиперспектрального изображения и использовались согласно соотношению (2).

Для всех последующих экспериментов по извлечению ЦВЗ порог обнаружения (4) был установлен равным 0,00002.

На рис. 2 показана зависимость визуального качества изображения после встраивания ЦВЗ от показателя интенсивности встраивания ЦВЗ α. В качестве меры визуального качества были выбраны значения *PSNR* и *PSNR-HVS-M*, полученные путём поканального сравнения исходного изображения и изображения после встраивания ЦВЗ. Показатель *PSNR-HVS-M* в данном случае представлял собой модифицированный показатель PSNR, вычисленный с учётом модели человеческого зрения (HVS) [25]. В целом, визуальная незаметность искажений, внесённых при встраивании ЦВЗ, достигалась при значениях $\alpha \le 3$.

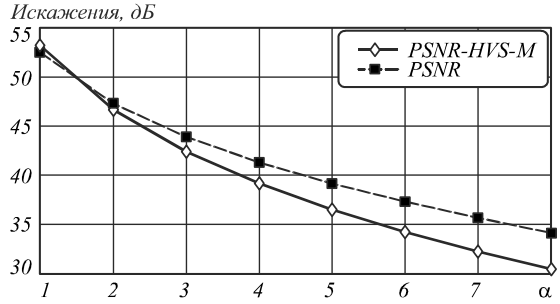

Рис. 2. Уровень искажений изображения-контейнера в зависимости от значения параметра интенсивности встраивания α

3.1. Устойчивость разработанного алгоритма встраивания к атакам с «приближённым вычислением ЦВЗ»

Для оценки устойчивости ЦВЗ к атакам, направленным на приближенное вычисление шумоподобных шаблонов M_0 и M_1, не известных атакующему, был проведён следующий эксперимент. Как уже было рассмотрено в параграфе 1, наиболее частой атакой подобного типа для гиперспектральных изображений является усреднение нескольких спектральных каналов одного изображения и/или анализ шумовой составляющей данных кадров. В случае, когда один и тот же шумоподобный шаблон используется для встраивания ЦВЗ во все спектральные каналы изображения, подобный способ анализа позволяет с достаточно высокой степенью достоверности восстановить неизвестный шаблон встраивания или его фрагмент.

Для оценки устойчивости разработанных алгоритмов к подобным сценариям атаки эксперимент был проведён следующим образом.

Во-первых, для шумоподобных искажений, вносимых в отдельный кадр в результате встраивания ЦВЗ, был оценён коэффициент межканальной корреляции, т.е. степень схожести вносимых при встраивании ЦВЗ искажений для соседних спектральных каналов. Для набора, состоящего из $T = 450$ спектральных каналов одного гиперспектрального изображения размером 4095×4095 пикселей, была оценена шумоподобная компонента, вносимая в результате встраивания:

$$D_t(n,m) = I_t(m,n) - I_t^{'}(m,n),$$

где $I_t(m,n)$ – изображение (t-й спектральный канал) до встраивания ЦВЗ, $I'_t(m,n)$ – после встраивания.

Далее для каждой пары соседних кадров вычислялось максимальное значение взаимной корреляции [18] $C_{max}(t)$ между шумоподобными компонентами $D_t(n,m)$ и $D_{t+1}(n,m)$. В случае, если значение $C_{max}(t)$ близко к нулю для любого t, то приближенное вычисление шумоподобных шаблонов встраивания за счёт усреднения нескольких спектральных каналов становится невозможным и можно говорить о стойкости ЦВЗ к подобному типу атак. С другой стороны, если $C_{max}(t)$ близко к 1 для большого числа спектральных каналов (т.е. идентичные шумоподобные компоненты вносятся сразу в несколько спектральных каналов), то ЦВЗ является уязвимым к атаке с приближенным вычислением шаблонов встраивания ЦВЗ.

В результате проведённого эксперимента значение $C_{\max}(t)$ было вычислено для 450 последовательных кадров и найдено среднее значение взаимной корреляции

$$\bar{C}_{\max} = \frac{1}{T}\sum_{t=0}^{T-1} C_{\max}(t) = 0,0272. \qquad (8)$$

Максимальное значение $C_{\max}(t)$ для данной выборки кадров было равно 0,0302.

Полученные результаты позволяют утверждать, что предложенный алгоритм встраивания и алгоритм генерации шумоподобных шаблонов встраивания обеспечивают стойкость к известным способам атаки с приближенным вычислением ЦВЗ.

3.2. Оценка устойчивости к атакам с прямым перебором ключа

Предложенный в параграфе 2 алгоритм извлечения ЦВЗ основан на использовании т.н. «информированного» корреляционного детектора ЦВЗ; фактически при извлечении ЦВЗ из кадра производится вычисление взаимно-корреляционной функции между известными детектору массивами M_1 и M_0 и отдельным спектральным каналом анализируемого изображения. Защищённость подобной схемы от преднамеренных атак зависит в первую очередь от сложности атаки прямым перебором, т.е. от обнаружения ЦВЗ без знания корректного ключа встраивания. Фактически ЦВЗ является уязвимым к такой атаке, если атакующий может за обозримое время перебрать все возможные значения ключа (и соответствующие ему значения M_1 и M_0) и выбрать среди них тот, что приводит к успешному обнаружению ЦВЗ.

Предположим, что атакующий последовательно перебирает все возможные секретные ключи встраивания (для представленного алгоритма их число равно 2^{47}), генерирует на их основе пары массивов M_1 и M_0 и использует их для извлечения ЦВЗ из выбранного изображения. Вычислительная сложность подобной атаки будет пропорциональна величине $N_{br} = \left|\tilde{M}\right| / [2\cdot(\bar{N}_{collis}+1)]$, где $\left|\tilde{M}\right|$ – число различных пар массивов (т.к. пара M_1 и M_0 генерируется на основе одного секретного ключа), $\bar{N}_{collis}$ – среднее число коллизий на одну пару массивов. В рассматриваемом случае величина $\bar{N}_{collis}$ должна быть оценена экспериментально, а величина $\left|\tilde{M}\right|$ определяется числом возможных секретных ключей встраивания и равна 2^{47}.

Для экспериментальной оценки величины $\bar{N}_{collis}$ был проведён следующий эксперимент. На этапе встраивания ЦВЗ было использовано 10 различных «истинных» секретных ключей, для каждого ключа производилась генерация пары шаблонов M_1 и M_0. Каждая пара шаблонов использовалась для встраивания ЦВЗ в отдельное гиперспектральное изображение, состоящее из 450 спектральных каналов. После встраивания ЦВЗ для каждого из изображений запускалась атака прямого перебора, т.е. последовательно производились попытки извлечь ЦВЗ с использованием всех возможных ключей встраивания. Как уже было отмечено ранее, число таких «неправильных» ключей равно (2^{47}–1), что делает практически нереализуемым их полный перебор в ходе проводимого эксперимента. Учитывая этот факт, эксперимент был упрощён следующим образом – для проведения атаки использовались не все (2^{47}–1) «неправильных» ключей встраивания, а только 5000 пар шаблонов M_1 и M_0, наиболее «близких» к исходной паре по критерию минимума циклического расстояния Хэмминга. Далее оценка числа коллизий проводилась исходя их предположения, что подавляющее большинство возникающих коллизий при извлечении ЦВЗ приходится именно на эти 5000 наиболее «близких» шаблонов.

Далее по всем 10 сгенерированным ключам встраивания было вычислено среднее число коллизий:

$$\bar{N}_{collis} = \frac{1}{10}\sum_{j=1}^{10} N_j ,$$

где N_j – число обнаруженных коллизий для i-го «истинного» ключа встраивания.

В результате проведённого эксперимента, после 50000 проведённых попыток извлечения ЦВЗ с использованием «неправильных» ключей не было обнаружено ни одной коллизии, т.е. было получено значение $\bar{N}_{collis} = 0$. Исходя из этого, оценка вычислительной сложности атаки прямого перебора принимает вид:

$$N_{br} = \left|\tilde{M}\right| / 2 = 2^{47} / 2 \approx 10^{14}.$$

Такая сложность атаки прямого перебора однозначно позволяет говорить о неэффективности подобных атак против предлагаемого алгоритма. Для сравнения, уже упомянутые выше алгоритмы встраивания ЦВЗ с использованием М-последовательностей ([6, 12, 15]) требуют всего $5\cdot10^4$ попыток извлечения ЦВЗ для реализации подобной атаки.

3.3. Исследование устойчивости встроенного ЦВЗ к сжатию с потерями

Для исследования устойчивости встроенного ЦВЗ к сжатию изображения с потерями был проведён сле-

дующий эксперимент. После встраивания ЦВЗ каждое изображение было подвергнут сжатию с потерями: сжатие каждого спектрального канала изображения производилось алгоритмом JPEG с показателем качества сжатия $Q = 80$.

Далее для 10 гиперспектральных изображений было оценено число спектральных каналов, необходимое для полностью корректного извлечения 64-битного ЦВЗ $W(x,y)$. Под полностью корректным извлечением в данном эксперименте подразумевалась ситуация, когда извлечённый из искажённого изображения ЦВЗ $W'(x,y)$ совпадал с исходным ЦВЗ с точностью до бита. Также среди 10 изображений было подсчитано максимальное число спектральных каналов $F_{\min}$, необходимое для корректного извлечения ЦВЗ. Результаты исследования устойчивости ЦВЗ к сжатию представлены в табл. 2.

Таким образом, можно утверждать, что даже при наименьших возможных значениях интенсивности встраивания встроенный ЦВЗ обладает устойчивостью к сжатию изображения-контейнера. Полученные результаты позволяют также говорить о том, что предложенный алгоритм встраивания ЦВЗ позволяет обеспечить меньшее (по показателю *PSNR*) искажение изображения по сравнению с существующими алгоритмами встраивания стойкого ЦВЗ в изображения. Так, для интенсивности встраивания $\alpha = 1$ предложенный алгоритм позволяет достигнуть значения *PSNR 51dB*.

Табл. 2. Устойчивость встроенного ЦВЗ к сжатию с потерями (M-JPEG)

Интенсивность встраивания	Среднее число каналов для корректного извлечения ЦВЗ, F_{avg}	Максимальное число каналов для корректного извлечения ЦВЗ, $F_{\max}$	Минимальное число каналов для корректного извлечения ЦВЗ, $F_{\min}$
$\alpha = 1$	121	186	72
$\alpha = 2$	101	188	70
$\alpha = 3$	75	100	65

В то же время широко известные алгоритмы встраивания ЦВЗ, схожие с предложенным по принципу модуляции ЦВЗ и по устойчивости ЦВЗ к преднамеренным атакам (например, основанные на использовании дискретного косинусного преобразования или вейвлет-преобразования [25, 26]), позволяют достигать значений *PSNR* не более *48-49 dB*.

Заключение

В работе предложены новые алгоритмы встраивания и извлечения ЦВЗ, основанные на кодировании ЦВЗ с расширением спектра, а также предложен алгоритм генерации шумоподобных шаблонов для встраивания ЦВЗ на основе секретного ключа. В работе показано, что разработанный алгоритм генерации шаблонов встраивания ЦВЗ обладает следующими свойствами:

- является стойким к известным атакам, направленным на приближенное вычисление ЦВЗ;
- делает практически нереализуемой атаку «прямого перебора» ключа встраивания – так, число попыток, требуемых атакующему для успешного проведения такой атаки, составляет не менее 10^{14};
- позволяет практически полностью избежать возникновения коллизий при извлечении ЦВЗ (в ходе эксперимента не было обнаружено ни одной коллизии);
- позволяет генерировать двумерные шаблоны встраивания объёмом до нескольких миллионов бит, что позволяет эффективно встраивать ЦВЗ в крупномасштабные изображения.

Полученные экспериментальные результаты также показывают, что даже при наименьших возможных значениях интенсивности встраивания ($\alpha \leq 3$) встроенный ЦВЗ остаётся устойчивым к сжатию с потерями. В то же время данные параметры встраивания позволяют достигнуть меньшего по сравнению с известными аналогами уровня вносимых искажений (для предложенного алгоритма величина *PSNR* достигает *51dB*, для известных аналогов [25, 26] *PSNR* составляет не более *48-49 dB*).

Благодарности

Работа выполнена за счёт Российского научного фонда (РНФ), грант №14-31-00014.

Литература

1. **Lin, E.T.** Temporal synchronization in video watermarking / E.T. Lin, E.J. Delp // IEEE Transactions on Signal Processing. – 2004. – Vol. 52(10). – P. 3007-3022.
2. **Delannay, D.** Digital watermarking algorithms robust against loss of synchronization. PhD Thesis / D. Delannay. – Louvain: Universite catholique de Louvain, 2004.
3. **Doërr, G.** Security pitfalls of frame-by-frame approaches to video watermarking / G. Doërr, J.L. Dugelay // IEEE Transactions on Signal Processing. – 2004. – Vol. 52(10). – P. 2955-2964.
4. **Pavel, G.** Embedding, Extraction and Detection of Digital Watermark in Spectral Images: PhD Thesis / G. Pavel. – Lappeenranta: Lappeenranta University of Technology, 2005.
5. **Bianchi, T.** Secure watermarking for multimedia content protection: A review of its benefits and open issues / T. Bianchi, A. Piva // IEEE Signal Processing Magazine. – 2013. – Vol. 30(2). – P. 87-96.
6. **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.
7. **Hartung, F.** Digital watermarking of raw and compressed video / F. Hartung, B. Girod // Proceedings of SPIE. – 1996. – Vol. 2952. – P. 205-213.
8. **Hartung, F.** Copyright protection in video delivery networks by watermarking of pre-compressed video / F. Hartung, B. Girod // Lecture Notes in Computer Science. – 1997. – Vol. 1242 – P. 423-436.
9. **Hartung, F.** Fast public-key watermarking of compressed video / F. Hartung, B. Girod // IEEE International Conference on Image Processing. – 1997. – Vol. 1. – P. 528-531.
10. **Hartung, F.** Digital watermarking of MPEG-2 coded video in the bitstream domain / F. Hartung, B. Girod // IEEE International Conference on Acoustics, Speech, and Signal Processing. – 1997. – Vol. 4. – P. 2621-2624.

11. **Hartung, F.** Watermarking of uncompressed and compressed video / F. Hartung., B. Girod // Signal processing. – 1998. – Vol. 66(3). – P. 283-301.
12. **Tirkel, A.Z.** A unique watermark for every image / A.Z. Tirkel, T.E. Hall // IEEE Multimedia. – 2001. – Vol. 8(4). – P. 30-37.
13. **van Schyndel, R.G.** Key independent watermark detection / R.G. van Schyndel, A.Z. Tirkel, I.D. Svalbe // IEEE International Conference on Multimedia Computing and Systems, –1999. – Vol. 1. – P. 580-585.
14. **van Schyndel, R.G.** Spread-Spectrum Digital Watermarking Concepts and Higher Dimensional Array Constructions / R.G. van Schyndel, A.Z. Tirkel, I.D. Svalbe, T.E. Hall, C.F. Osborne // First International Online Symposium on Electronics Engineering. – 2000.
15. **Van Schyndel, R.G.** Algebraic construction of a new class of quasi-orthogonal arrays for steganography / R.G. Van Schyndel, A.Z. Tirkel, I.D. Svalbe, T.E. Hall, C.F. Osborne // Proceedings of SPIE. – 1999. – Vol. 3657. – P. 354-364.
16. **Chen, L.** Communication system security / L. Chen, G. Gong. – CRC press, 2012. – 750 p.
17. **Mitekin, V.A.** A new method for high-capacity information hiding in video robust against temporal desynchronization / V.A. Mitekin, V.A. Fedoseev // Seventh International Conference on Machine Vision (ICMV 2014), 94451A (February 12, 2015). Proceedings of SPIE9445. – 2015. – Vol. 9445. – 7p. – doi:10.1117/12.2180550.
18. **Tsai, D.M.** Fast normalized cross correlation for defect detection / D.M. Tsai, C.T. Lin // Pattern Recognition Letters. – 2003. – Vol. 24(15). – P. 2625-2631.
19. **Mitekin, V.A.** A new watermarking sequence generation algorithm for collision-free digital watermarking / V.A. Mitekin, E.I. Timbay // Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on. – 2012. – P. 256-260.
20. **Moreno, O.** New families of arrays in two dimensions for watermarking applications / O. Moreno, A.Z. Tirkel, U. Parampalli, R.G. Van Schyndel // Electronics letters. – 2010. – Vol. 46(22). – P. 1500-1502.
21. **Seo, J.S.** Design of template in the autocorrelation domain / J.S. Seo, C.D. Yoo // Proceedings of SPIE. –2002. – Vol. 4675. – P. 305-312.
22. **Omrani, R.** New constructions and bounds for 2-D optical orthogonal codes / R. Omrani, P. Elia, P.V. Kumar // Lecture Notes in Computer Science. – 2005. – Vol. 3485 – P. 389-395.
23. **Bitan, S.** Constructions for optimal constant weight cyclically permutable codes and difference families / S. Bitan, T. Etzion // IEEE Transactions on Information Theory. – 1995. – Vol. 41(1). – P. 77-87.
24. **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 for Consumer Electronnics. – 2007. – Vol. 4. – 4 p.
25. **Hsu, C.T.** DCT-based watermarking for video / C.T. Hsu, J.L. Wu // IEEE Transactions on Consumer Electronics. – 1998. – Vol. 44(1). – P. 206-216.
26. **Preda, R.O.** A robust digital watermarking scheme for video copyright protection in the wavelet domain / R.O. Preda, D.N. Vizireanu // Measurement. – 2010. – Vol. 43(10). – P. 1720-1726.

References

[1] Lin ET, Delp EJ. Temporal synchronization in video watermarking, IEEE Transactions on Signal Processing 2004; 52(10): 3007-22.
[2] Delannay D. Digital watermarking algorithms robust against loss of synchronization. Technical report, UCL 2004.
[3] Doërr G, Dugelay JL. Security pitfalls of frame-by-frame approaches to video watermarking. IEEE Transactions on Signal Processing 2004; 52(10): 2955-64.
[4] Pavel G. Embedding, Extraction Detection of Digital Watermark in Spectral Images, Technical report. Lappeenranta university of technology 2005.
[5] Bianchi T, Piva A. Secure watermarking for multimedia content protection: A review of its benefits open issues. IEEE Signal Processing Magazine 2013; 30(2): 87-96.
[6] Cox IJ, Kilian J, Leighton FT. Shamoon, T. Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing; 6(12): 1673-87.
[7] Hartung FH, Girod B. Digital watermarking of raw compressed video, Advanced Imaging Network Technologies, International Society for Optics Photonics, 1996; 205-13.
[8] Hartung F, Girod B. Copyright protection in video delivery networks by watermarking of pre-compressed video. Multimedia Applications, Services Techniques-ECMAST'97. Lecture Notes in Computer Science 1997; 1242; 423-36.
[9] Hartung, F. Girod, B. Fast public-key watermarking of compressed video. International Conference on Image Processing, 1997; 1: 528-31.
[10] Hartung F, Girod B. Digital watermarking of MPEG-2 coded video in the bitstream domain. IEEE International Conference on Acoustics, Speech, Signal Processing ICASSP-97 1997: 4: 2621-4.
[11] Hartung F, Girod B. Watermarking of uncompressed compressed video. Signal processing 1998; 66(3): 283-301.
[12] Tirkel AZ, Hall TE. A unique watermark for every image, IEEE MultiMedia 2001; 8(4): 30-7.
[13] van Schyndel RG, Tirkel AZ, Svalbe ID. Key independent watermark detection. Multimedia Computing Systems, 1999, IEEE International Conference on', IEEE, 1999; 1: 580-5.
[14] van Schyndel RG, Tirkel AZ, Svalbe ID, Hall TE, Osborne CF. Spread-Spectrum Digital Watermarking Concepts Higher Dimensional Array Constructions. First International Online Symposium on Electronics Engineering 2000.
[15] van Schyndel RG, Tirkel AZ, Svalbe ID, Hall TE, Osborne CF. Algebraic construction of a new class of quasi-orthogonal arrays for steganography. Electronic Imaging 99, International Society for Optics Photonics 1999; 354-64.
[16] Chen L, Gong G. Communication system security. CRC press; 2012.
[17] Mitekin VA, Fedoseev VA. A new method for high-capacity information hiding in video robust against temporal desynchronization. Seventh International Conference on Machine Vision (ICMV 2014), International Society for Optics and Photonics 2015; 94451A. Proc of SPIE9445 2015; 9445. – 7p. doi:10.1117/12.2180550.
[18] Tsai DM, Lin CT. Fast normalized cross correlation for defect detection. Pattern Recognition Letters 2003; 24(15): 2625-31.
[19] Mitekin VA,Timbay EI. A new watermarking sequence generation algorithm for collision-free digital watermarking. IEEE Eighth International Conference on'Intelligent Information Hiding Multimedia Signal Processing (IIH-MSP) 2012; 256-60.

[20] Moreno O, Tirkel AZ, Parampalli U, Van Schyndel R. New families of arrays in two dimensions for watermarking applications. Electronics letters 2010; 46(22):1500-2.
[21] Seo JS, Yoo CD. Design of template in the autocorrelation domain. Electronic Imaging 2002, International Society for Optics Photonics 2002; 305-12.
[22] Omrani R, Elia P, Kumar PV. New constructions bounds for 2-D optical orthogonal codes. Sequences and Their Applications-SETA 2005; 3485: 389-95.
[23] Bitan S, Etzion T. Constructions for optimal constant weight cyclically permutable codes difference families. IEEE Transactions on Information Theory 1995; 41(1): 77-87.
[24] Ponomarenko N, Silvestri F, Egiazarian K, Carli M, Astola J, Lukin V. On between-coefficient contrast masking of DCT basis functions. Proceedings of the Third International Workshop on Video Processing Quality Metrics 2007; 4: 4 p.
[25] Hsu CT, Wu JL. DCT-based watermarking for video. IEEE Transactions on Consumer Electronics, 1998; 44(1): 206-16.
[26] Preda RO, Vizireanu DN. A robust digital watermarking scheme for video copyright protection in the wavelet domain. Measurement 2010; 43(10): 1720-6.

AN ALGORITHM FOR GENERATING DIGITAL WATERMARKS ROBUST AGAINST BRUTE-FORCE ATTACKS

V.A. Mitekin
Samara State Aerospace University, Samara, Russia,
Image Processing Systems Institute, Russian Academy of Sciences, Samara, Russia

Abstract

This paper presents a new method for high-capacity robust watermarking of hyperspectral images. A new algorithm for two-dimensional "noise-like" watermarking patterns generation is proposed as part of robust watermark embedding and detection procedures. The experimental research provided in this work shows that the average complexity of the brute-force key retrieval attack can be increased to 10^{14} watermark extraction attempts (compared to 10^4-10^5 for known robust watermarking schemes). Experimental results also show that the watermark preserves its robustness against lossy compression of host video, at the same time preserving a higher video quality (*PSNR* up to *51dB)* compared to known wavelet-based and DCT-based watermarking algorithms.

Key words: Information hiding; image watermarking; brute-force attack; spread spectrum watermarking; cyclically permutable code.

Citation: Mitekin VA. An algorithm for generating digital watermarks robust against brute-force attacks. Computer Optics 2015; 39(5): 808-17. DOI: 10.18287/0134-2452-2015-39-5-808-817.

Acknowledgements: This work was financially supported by the Russian Scientific Foundation (RSF), grant No. 14-31-00014.

Сведения об авторе

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), majoring in Applied Mathematics and Informatics in 2006. 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 an assistant professor at the Geoinformatics and Information Security sub-department at SSAU. His scientific interests include image processing and recognition, steganography and steganalysis, cryptography.

Поступила в редакцию 11 ноября 2015 г.
Окончательный вариант – 8 декабря 2015 г.