УДК 519.72

С. О. Вихарев, Е. Т. Мирончиков, М. В. Гофман

МЕТОДИКА ПОСТРОЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, УСТОЙЧИВЫХ К СБОЯМ СИНХРОНИЗАЦИИ

Дата поступления: 14.12.2015
Решение о публикации: 28.01.2016

Цель: Построить цифровые водяные знаки, устойчивые к сбоям синхронизации. **Методы:** Описываемые в статье методы относятся к области теории информации и стеганографии. **Результаты:** Предложена методика построения цифровых водяных знаков на основе БЧХ-синхрокодов. Представлены метод встраивания в цифровой аудиосигнал предлагаемых водяных знаков и алгоритм их выделения даже после того, как из аудиосигнала будут удалены некоторые отсчёты. **Практическая значимость:** Представленные в статье цифровые водяные знаки можно использовать в качестве средства для внедрения дополнительной информации в цифровой аудиосигнал так, что даже после удаления некоторых отсчётов аудиосигнала остаётся возможность восстановить внедрённую информацию.

БЧХ-код, синхронизация, цифровой водяной знак, цифровой аудиосигнал.

Sergey O. Vikharev, post-graduate student; **Yevgeny T. Mironchikov**, Dr. Sci. (Eng.), professor; ***Maksim V. Gofman**, Cand. Sci. (Eng.), senior lecturer, maxgof@gmail.com (Petersburg State Transport University) A METHOD FOR BUILDING SYNCHRONISATION FAULT-TOLERANT DIGITAL WATERMARKS

Objective: To build digital watermarks that are tolerant to synchronisation faults. **Methods:** Methods described in the paper fall within the domain of theory of information and steganography. **Results:** A method for building digital watermarks based on BCH codes iss proposed. A method for embedding the proposed watermarks in the digital audio signal, and an algorithm for their acquisition even after some readings would be deleted from the audio signal were presented. **Practical importance:** Digital watermarks presented in the paper can be used as a means for introducing additional information into a digital audio signal in a manner that allows restoring embedded information even after deletion of some audio signal readings.

BCH code, synchronisation, digital watermark, digital audio signal.

Цифровые аудиосигналы как объекты, содержащие аудиоинформацию, могут иметь большую ценность. Так, они могут представлять собой результат работы музыкантов и певцов и быть ориентированы на удовлетворение эстетических потребностей людей или служить вместилищем информации для работы, например, секретарей, журналистов,

следователей, работников служб безопасности и т. д.

Часто цифровые аудиосигналы наделяются дополнительными свойствами, которые позволяют защитить авторские права или внедрить в аудиосигнал цифровой ярлык или тэг. Так, звукозаписывающим компаниям важно, чтобы их юридические права на музыкальное произведение были защищены, а людям, которые работают со звуковой информацией, – чтобы имелась возможность внедрить тэг в цифровой аудиосигнал.

Аудиосигналы представляют собой объекты, допускающие обработку. Их можно сжимать, их части – удалять, изменять или добавлять новые. Из-за этого добавочная информация (от звукозаписывающей компании) или тэги может быть утеряна или искажена, поэтому вопрос встраивания дополнительной информации в цифровые аудиосигналы остается открытым.

Встраивание дополнительной информации в виде цифровых водяных знаков – на сегодня один из основных способов защиты авторских прав или внедрения тэгов. Когда водяные знаки встраиваются в цифровой аудиосигнал последовательно во временно́й области, тогда при удалении части отсчётов цифрового аудиосигнала невозможно будет определить, где начало и конец водяного знака, т. е. фактически произойдёт сбой синхронизации.

Причины сбоев синхронизации могут быть различными. Так, весьма часты сбои при хранении больших объемов аудиоданных на различных носителях, особенно при многократных считываниях. Помимо технических причин сбои синхронизации могут быть следствием действий злоумышленников.

Вопросы применения последовательностей Баркера при построении водяных знаков, устойчивых к сбоям синхронизации, рассматриваются в статьях [2–4]. При этом сами последовательности Баркера не несут никакой полезной информации, а служат лишь для установления синхронизации.

В этой статье описывается методика построения цифровых водяных знаков на основе БЧХ-синхрокодов [1], которые не только восстанавливают синхронизацию, но и позволяют хранить в себе информацию. Кроме того, предлагается алгоритм их встраивания в цифровой аудиосигнал так, что они не будут слышны человеческому уху.

Сбои синхронизации и синхрокоды

Цифровой аудиосигнал – это последовательность квантованных отсчётов аналогового аудиосигнала. Если из цифрового аудиосигнала пропадёт несколько отсчётов, то, скорее всего, человеческое ухо это не отметит. Однако если в такой аудиосигнал были внедрены цифровые водяные знаки, то их считывание станет весьма затруднительным, если вообще возможным, так как исказятся ориентиры для установления синхронизации, по которым можно было бы определить позиции элементов цифрового водяного знака.

В качестве ориентиров обычно используют начала и концы блоков или сегментов, на которые разбивается цифровой аудиосигнал. И тогда при пропаже нескольких первых или последних отсчётов блока удастся восстановить синхронизацию, если, например, не рассматривать оставшиеся отсчёты блока, а ориентироваться на границы соседнего блока. Благодаря этому достаточно определить, сколько отсчётов от блока осталось, чтобы установить начало соседнего блока.

В общем случае цифровой аудиосигнал не обладает никакими специфическими свойствами, на основании которых из него можно было бы выделить блоки, оставшиеся после удаления некоторых отсчётов, поэтому если в обычный цифровой аудиосигнал встроить водяные знаки, неустойчивые к сбоям синхронизации, то их не удастся выделить обратно после манипуляций, приведших к сбоям.

Водяные знаки, устойчивые к сбоям синхронизации, допускают возможность определить, сколько элементов осталось от водяного знака. В качестве инструмента создания таких

водяных знаков в этой статье предлагается использовать БЧХ-синхрокоды.

Для синхрокодового слова можно определить, сколько элементов с начала или с конца было потеряно, конечно, если это число не больше некоторого порогового значения, зависящего от применяемого синхрокода. Если встраивать элементы синхрокодовых слов в каждый отсчёт цифрового аудиосигнала, то при выпадении нескольких отсчётов сигнала пропадёт и несколько элементов синхрокодового слова, а значит, если применить методику вычисления сдвига синхронизации к оставшимся элементам синхрокодового слова, то удастся определить, сколько отсчётов из рассматриваемого блока осталось и где начало следующего блока, в котором будет ещё один водяной знак.

Для синхрокодов определяют два вида сбоев синхронизации: потерю и избыток. Пусть есть два синхрокодовых слова:

$$c_1 = (c_{1,n-1} \quad c_{1,n-2} \quad \dots \quad c_{1,0});$$

$$c_2 = (c_{2,n-1} \quad c_{2,n-2} \quad \dots \quad c_{2,0}),$$

которые, соответственно, в полиномиальной форме выглядят так:

$$c_k(x) = \sum_{i=0}^{n-1} c_{k,i} x^i.$$

А также пусть эти кодовые слова передаются так, что их элементы образуют последовательность

$$\alpha = c_{1,n-1}, c_{1,n-2}, \dots, c_{1,0}, c_{2,n-1}, c_{2,n-2}, \dots, c_{2,0}.$$

Потерей синхронизации в r символов является ситуация, когда теряются первые r символов последовательности α. В этом случае вместо первого кодового слова c_1 получится вектор

$$(c_{1,n-r-1} \quad c_{1,n-r-2} \quad \dots \quad c_{1,0} \quad c_{2,n-1} \quad c_{2,n-2} \quad \dots c_{2,n-r}).$$

Избытком синхронизации в r символов является ситуация, когда теряются последние r символов последовательности α. Тогда вместо второго кодового слова c_2 получится вектор

$$(c_{1,r-1} \quad c_{1,r-2} \quad \dots \quad c_{1,0} \quad c_{2,n-1} \quad c_{2,n-2} \quad \dots \quad c_{2,r})$$

Синхрокоды можно построить разными способами. Наиболее просты, эффективны и исследованы с точки зрения свойств восстановления синхронизации синхрокоды, построенные на основе кодов БЧХ.

Синхрокоды на основе кодов БЧХ

Перед построением кодовых слов таких синхрокодов создают подходящий код БЧХ. Синхрокод является смежным классом БЧХ-кода. Смежный класс получается прибавлением смещающего полинома к каждому кодовому слову БЧХ-кода. Смещающий полином не должен делиться на x, а значит, его свободный член не должен быть равен нулю.

Как и всякий блоковый код, синхрокод на основе БЧХ-кода имеет ряд основных параметров. Это, в первую очередь, длина n кодового слова, число k исходных информационных символов, а также максимальная величина произошедшего сдвига r_c, который ещё можно выявить посредством синхрокода. Величина r_c определяется по формуле

$$r_c = \left[\frac{n-k-s-1}{2} \right],$$

где $[a]$ – целая часть числа a; s – степень смещающего полинома.

Алгоритм построения синхрокодового слова на основе БЧХ-кода

Входные данные: порождающий полином $g(x)$ БЧХ-кода и информационный полином $m(x)$.

Выходные результаты: синхрокодовое слово $c(x)$ в полиномиальной форме.

1. Умножение информационного полинома на порождающий полином $g(x)$:

$$c_{\text{БЧХ}}(x) = m(x)g(x).$$

2. Задание смещающего полинома $p(x)$.

3. Сложение результата 3-го шага со смещающим полиномом, масштабированным x^{-1}:

$$c(x) = c_{\text{БЧХ}}(x) + x^{-1}p(x).$$

На практике вместо полинома x^{-1} обычно используется полином $w(x)$, который является обратным к полиному x^{-1} по модулю порождающего полинома $g(x)$ над полем $GF(2)$:

$$((x^{-1}w(x)) \bmod g(x)) \bmod 2 = 1.$$

Алгоритм определения величины сдвига синхронизации

Входные данные: полином

$$c'(x) = \sum_{i=1}^{n} c'_i x^{i-1},$$

который в отсутствие сбоев синхронизации представляет собой синхрокодовое слово.

Выходные значения: величина потери синхронизации $r_{\text{потеря}}$ и величина избытка синхронизации $r_{\text{избыток}}$.

1. Вычитание смещающего полинома из полинома $c'(x)$:

$$r_1(x) = (c'(x) - x^{-1}p(x)) \bmod 2.$$

2. Умножение на одночлен степени $r_c + 1$:

$$r_2(x) = x^{r_c+1} r_1(x).$$

3. Получение остатка от деления полинома $r_2(x)$ на порождающий полином:

$$r_3(x) = r_2(x) \bmod g(x).$$

4. Определение максимальной $d_{\max}$ и минимальной $d_{\min}$ степеней членов полинома $r_3(x)$:

$$d_{\max} = \deg_{\max} r_3(x) \text{ и } d_{\min} = \deg_{\min} r_3(x),$$

где $\deg_{\max} a(x)$ и $\deg_{\min} a(x)$ – это максимальная и минимальная степени членов полинома $a(x)$, соответственно. Таким образом, $d_{\max}$ – это наивысшая степень ненулевого слагаемого полинома $r_3(x)$, а $d_{\min}$ – это низшая степень ненулевого слагаемого полинома $r_3(x)$.

5. Если $d_{\max} > r_c + s$, то произошла потеря синхронизации, в этом случае

$$r_{\text{потеря}} = d_{\max} - r_c - s.$$

Если же $d_{\min} < r_c$, то произошёл избыток синхронизации, в этом случае

$$r_{\text{избыток}} = r_c - d_{\min}.$$

Если $r_3(x) = 0$, то сбоя синхронизации не было, а $c'(x)$ – это синхрокодовое слово, в этом случае

$$r_{\text{потеря}} = r_{\text{избыток}} = 0.$$

Пример определения величины сдвига при помощи синхрокода

В качестве основы для синхрокода используем БЧХ-код со следующими параметрами: длина кодового слова $n = 63$, число информационных символов $k = 30$. Порождающий полином

$$g(x) = 1 + x + x^2 + x^5 + x^6 + x^8 + x^9 + x^{11} + x^{13} + x^{14} + x^{15} + x^{20} + x^{22} + x^{23} + x^{26} + x^{27} + x^{28} + x^{29} + x^{30} + x^{32} + x^{33}.$$

Смещающий полином $p(x) = x + 1$; значит, $s = 1$. Синхрокод с такими параметрами позволяет определить величину сдвига синхронизации вплоть до

$$r_{\text{с}} = \left[\frac{n-k-s-1}{2}\right] = 15.$$

При построении синхрокодовых слов для рассматриваемого случая вместо x^{-1} удобно использовать полином

$$w(x) = 1 + x + x^4 + x^5 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{14} + x^{19} + x^{21} + x^{22} + x^{25} + x^{26} + x^{27} + x^{28} + x^{29} + x^{31} + x^{32}.$$

Пусть есть два синхрокодовых слова. Первое синхрокодовое слово имеет полиномиальную форму

$$c_1(x) = (m_1(x)g(x) + w(x)p(x)) \bmod 2 = \sum_{i=0}^{62} c_{1,i}x^i = x^3 + x^{11} + x^{12} + x^{13} + x^{16} + x^{17} + x^{18} + x^{20} + x^{21} + x^{22} + x^{23} + x^{25} + x^{26} + x^{28} + x^{30} + x^{32} + x^{33} + x^{35} + x^{38} + x^{41} + x^{42} + x^{44} + x^{50} + x^{51} + x^{53} + x^{54} + x^{55} + x^{57} + x^{59} + x^{62},$$

где $m_1(x) = \sum_{i=0}^{29} x^i$.

Второе синхрокодовое слово в форме полинома выглядит так:

$$c_2(x) = (m_2(x)g(x) + w(x)p(x)) \bmod 2 = \sum_{i=0}^{62} c_{2,i}x^i = 1 + x^2 + x^3 + x^4 + x^5 + x^{11} + x^{13} + x^{15} + x^{16} + x^{18} + x^{22} + x^{23} + x^{29} + x^{32} + x^{33} + x^{38} + x^{41} + x^{42} + x^{44} + x^{50} + x^{51} + x^{53} + x^{54} + x^{55} + x^{57} + x^{59} + x^{62},$$

где $m_2(x) = \sum_{i=3}^{29} x^i$.

Предположим, что кодовые слова поэлементно передаются в канал, начиная со старших степеней, а также что первым передаётся первое кодовое слово $c_1(x)$, потом второе кодовое слово $c_2(x)$. Таким образом, в канал будет передаваться последовательность

$$c_{1,62}, c_{1,61}, \ldots, c_{1,0}, c_{2,62}, c_{2,61}, \ldots, c_{2,0}.$$

Рассмотрим две ситуации: потерю и избыток синхронизации. При любом из этих сбоев синхронизации блок в полиномиальное форме, для которого будет вычисляться величина сдвига, вместо целого кодового слова будет содержать сумму из слагаемых первого и второго кодового слова.

Пусть произошла потеря синхронизации на величину сдвига $r = 3$. Значит, из первого кодового слова пропали три слагаемых наивысших степеней. Таким образом, вместо первого кодового слова получится вектор:

$$(c_{1,59} \quad c_{1,58} \quad \ldots \quad c_{1,0} \quad c_{2,62} \quad c_{2,61} \quad c_{2,60}),$$

который в полиномиальной форме будет таким:

$$c'(x) = \sum_{i=r}^{62} c_{1,i-r}x^i + \sum_{i=0}^{r-1} c_{2,62-i}x^{r-i-1} = x^2 + x^6 + x^{14} + x^{15} + x^{16} + x^{19} + x^{20} + x^{21} + x^{23} + x^{24} + x^{25} + x^{26} + x^{28} + x^{29} + x^{31} + x^{33} + x^{35} + x^{36} + x^{38} + x^{41} + x^{44} + x^{45} + x^{47} + x^{53} + x^{54} + x^{56} + x^{57} + x^{58} + x^{60} + x^{62}.$$

В соответствии с алгоритмом определения величины сдвига получим полином

$$r_3(x) = ((x^{r_c+1}(c'(x) - w(x) \times p(x))) \bmod g(x)) \bmod 2 = x^{15} + x^{16} + x^{18} + x^{19}.$$

По полиному $r_3(x)$ видно, что $d_{\max} = 19$, а $d_{\min} = 15$. Следовательно, выполняется нера-

венство $d_{\max} > r_c + s$, поэтому рассматриваемый сбой синхронизации представляет собой потерю синхронизации с величиной сдвига $r_{\text{потеря}} = d_{\max} - r_c - s = 3$, тогда как $r_{\text{избыток}} = r_c - d_{\min} = 0$.

Пусть возник избыток синхронизации на величину сдвига $r = 5$. Значит, из второго кодового слова пропали 5 слагаемых низших степеней. Таким образом, вместо второго кодового слова получится вектор:

$$(c_{1,4} \quad c_{1,3} \quad c_{1,2} \quad c_{1,1} \quad c_{1,0} \quad c_{2,62} \quad c_{2,61} \quad \dots \quad c_{2,5}),$$

который в полиномиальной форме будет таким:

$$c'(x) = \sum_{i=0}^{r-1} c_{1,r-i-1} x^{62-i} + \sum_{i=r}^{62} c_{2,i} x^{i-r} =$$

$$= 1 + x^6 + x^8 + x^{10} + x^{11} + x^{13} + x^{17} + x^{18} + x^{24} + x^{27} + x^{28} + x^{33} + x^{36} + x^{37} + x^{39} + x^{45} + x^{46} + x^{48} + x^{49} + x^{50} + x^{52} + x^{54} + x^{57} + x^{61}.$$

В соответствии с алгоритмом определения величины сдвига получим полином

$$r_3(x) = ((x^{r_c+1}(c'(x) - w(x)з(x))) \times \times \bmod g(x)) \bmod 2 = x^{10} + x^{13} + x^{16}.$$

По полиному $r_3(x)$ видно, что $d_{\max} = 16$, а $d_{\min} = 10$. Следовательно, выполняется неравенство $d_{\min} < r_c$, значит, возник избыток синхронизации с величиной сдвига $r_{\text{избыток}} = 5$, тогда как $r_{\text{потеря}} = 0$.

Рассмотренный БЧХ-синхрокод (63,30) позволяет верно определить не только величину сдвига вплоть до $r_c = 15$, но и вид сбоя синхронизации. Так, если произошла потеря синхронизации со сдвигом на $1 \le r \le r_c$, то $r_{\text{избыток}} = 0$, тогда как $r_{\text{потеря}} = r$; то же самое можно сказать о ситуации, когда возник избыток синхронизации, только в этом случае будет $r_{\text{потеря}} = 0$.

Метод встраивания водяного знака в цифровой аудиосигнал

Цифровой аудиосигнал, т. е. последовательность квантованных отсчётов аналогового аудиосигнала, можно представлять в виде вектора. В общем случае любой отсчёт цифрового аудиосигнала может быть утерян, поэтому для устойчивости водяного знака к сбоям синхронизации синхрокодовое слово, являющееся водяным знаком, полезно внедрять в цифровой аудиосигнал так, чтобы каждый элемент вектора, описывающего аудиосигнал, содержал часть синхрокодового слова.

Один из вариантов встраивания водяного знака – это изменение младших разрядов значения отсчёта цифрового аудиосигнала в соответствии со встраиваемым значением. Пусть есть водяной знак, представляющий собой БЧХ-синхрокодовое слово c:

$$c = (c_0 \quad \dots \quad c_{n-1}),$$

где $c_i \in \{0,1\} \forall i \in \{0,\dots,n-1\}$, а цифровой аудиосигнал пусть представляет собой вектор

$$y = (y_1 \quad \dots \quad y_N),$$

где $y_i \in \{0,\dots,2^{16}-1\} \forall i \in \{1,\dots,N\}$. Предположим, что длина N вектора **y** кратна длине n синхрокодового слова:

$$N = kn,$$

где k – это целое положительное число. В этом случае вектор **y** можно разделить на k векторов, длина которых равна длине синхрокодового слова. Далее такие «подвекторы» будем называть блоками, или сегментами цифрового аудиосигнала.

Так как длина вектора **y** кратна длине синхрокодового слова, изменение младшего бита i-го элемента вектора **y** на битовое значение j-го элемента вектора **c** можно выполнить так:

$$y'_i = (y_i - (y_i \bmod 2)) + c_j$$
$$\text{при} \quad j = (i-1) \bmod n,$$

где $i \in \{1,\ldots,N\}$, a mod b – это остаток от деления числа a на число b. Из чисел y'_i можно составить вектор

$$y' = (y'_1 \quad \ldots \quad y'_N),$$

который будет описывать цифровой аудиосигнал, содержащий водяной знак **c** в каждом своём сегменте.

Алгоритм выделения двоичных синхрокодовых слов из аудиофайла

Входные данные: вектор $y_в = (y_{в,1} \ldots y_{в,N'})$ где $y_{в,i}$ – целые числа; $N' \geq n$, n – длина синхрокодового слова.

Выходные данные: множество C выделенных синхрокодовых слов, представленных в виде битовых векторов.

1. Присвоить вектору **c** первые n значений вектора $y_в$:

$$c \leftarrow (\text{МлБит}(y_{в,1}) \quad \ldots \quad \text{МлБит}(y_{в,n})),$$

где МлБит (a) – значение младшего бита целого числа a.

2. Присвоить переменной i значение 1:

$$i \leftarrow 1.$$

3. В соответствии с описанным ранее алгоритмом по вектору **c** определить пару чисел ($r_{\text{избыток}}$, $r_{\text{потеря}}$).

4. Если $(r_{\text{потеря}}, r_{\text{избыток}}) = (0,0)$, то перейти к шагу 5. Если ($r_{\text{потеря}}$, $r_{\text{избыток}}$) = (r,0), при этом $1 \leq r \leq r_c$, то перейти к шагу 6. Если ($r_{\text{потеря}}$, $r_{\text{избыток}}$) = $(0,r)$, при этом $1 \leq r \leq r_c$, то перейти к шагу 7. Если $(r_{\text{потеря}}, r_{\text{избыток}}) = (r,r')$, то перейти к шагу 8.

5. Сбоя синхронизации не было, а значит вектор **c** – синхрокодовое слово (в векторной форме). Добавить его в множество **C**. Присвоить переменной i значение $i + n$:

$$i \leftarrow i + n;$$

перейти к шагу 9.

6. Произошла потеря синхронизации. Присвоить переменной i значение $i + n – r$:

$$i \leftarrow i + n - r;$$

перейти к шагу 9.

7. Возник избыток синхронизации. Присвоить переменной i значение $i + r$:

$$i \leftarrow i + r;$$

перейти к шагу 9.

8. Присвоить переменной i значение i +1:

$$i \leftarrow i + 1;$$

перейти к шагу 9.

9. Если $N' - i \geq n$, то присвоить вектору **c** элементы вектора $y_в$ с i по $i + n – 1$:

$$c \leftarrow (\text{МлБит}(y_{в,i}) \quad \ldots \quad \text{МлБит}(y_{в,i+n-1}));$$

перейти к шагу 3; иначе, если $N' - i < n$, то **ОСТАНОВ**.

Пример восстановления данных после атаки «вырезание»

Пусть в соответствии с описанным методом цифровой водяной знак ***c*** был встроен в аудиосигнал ***y***, в результате был получен аудиосигнал ***y′***.

Теперь пусть на цифровой аудиосигнал ***y′*** была выполнена атака «вырезание», т. е. было удалено несколько отсчётов аудиосигнала, в результате которой получился аудиосигнал

$$y_в = (y_{в,1} \quad \ldots \quad y_{в,N'}),$$

где $N' \geq n$; n – длина синхрокодового слова. Применив алгоритм выделения синхрокодовых слов к вектору $y_в$, получим множество

$$C = \{c_1, c_2, \ldots, c_K\},$$

где K – количество выделенных синхрокодовых слов; $\boldsymbol{c}_k$ $(k \in \{1, 2, \ldots, K\})$ – битовый вектор длиной n, представляющий собой синхрокодовое слово.

Пусть первый элемент вектора $\mathbf{c}_k$ – это коэффициент при старшей степени полиномиальной формы соответствующего синхрокодового слова, а последний его элемент – свободный член полиномиальной формы. Таким образом, если синхрокодовое слово в векторной форме $c_k = (c_{k,1} \quad \ldots \quad c_{k,n})$, то в полиномиальной форме синхрокодовое слово будет $c_k(x) = \sum_{i=1}^{n} c_{k,i} x^{n-i}$.

Теперь, если вычесть из каждого полинома $c_k(x)$ смещающий полином $x^{-1}p(x)$, а затем к разности применить БЧХ-декодирование, получится множество информационных полиномов $\{m_1(x), m_2(x), \ldots, m_K(x)\}$.

Следует отметить, что из-за атаки «вырезание» синхрокодовые слова $\boldsymbol{c}_k$ в общем случае могут не совпасть с исходным водяным знаком $\boldsymbol{c}$. Значит, информационные полиномы $m_k(x)$ также в общем случае могут не совпасть с исходным информационным полиномом $m(x)$.

Заключение

Рассмотрен метод построения цифровых водяных знаков на основе БЧХ-синхрокодов. Приведены примеры вычисления сдвигов синхронизации при разных видах сбоев синхронизации. Предложен такой алгоритм встраивания в цифровой аудиосигнал представленных водяных знаков, который позволяет использовать их устойчивость к сбоям синхронизации и противостоять атаке «вырезание» во временно́й области. Предложен алгоритм восстановления данных после атаки «вырезание», осуществлённой по отношению к аудиосигналу с представленными цифровыми водяными знаками.

Биографический список

1. Питерсон У. У. Коды, исправляющие ошибки : моногр. / У. У. Питерсон, Э. Уэлдон. – М. : Мир, 1976. – 594 с.

2. Huang J. A blind audio watermarking algorithm with self-synchronization / J. Huang, Yo. Wang, Yu. Q. Shi // IEEE Int. Symp. Circuits Syst. – 2002. – Vol. 3. – P. 627–630.

3. Wang X.-Ya. A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT / X.-Ya. Wang, H. Zhao // IEEE Trans. Signal Proc. – 2006. – Vol. 54, Is. 12. – P. 4835–4840.

4. Wu Sh. Efficiently self-synchronized audio watermarking for assured audio data transmission / Sh. Wu, J. Huang, D. Huang, Y. Q. Shi // IEEE Trans. Broadcast. – 2005. – Vol. 51, Is. 1. – P. 69–76.

References

1. Piterson U. U. & Ueldon E. Kody, ispravlyayushchiye oshibki: monografiya [Error-Correcting Codes]. Moscow, Mir, 1976. 594 p.

2. Huang J., Wang Yo. & Shi Yu. Q. A blind audio watermarking algorithm with self-synchronization. *IEEE Int. Symp. Circuits Syst.*, 2002, Vol. 3. Pp. 627-630.

3. Wang X.-Ya. & Zhao H. A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT. *IEEE Trans. Signal Proc.*, 2006. Vol. 54, Is. 12, pp. 4835-4840.

4. Wu Sh., Huang J., Huang D. & Shi Y. Q. Efficiently self-synchronized audio watermarking for assured audio data transmission. *IEEE Trans. Broadcast.*, 2005. Vol. 51, Is. 1, pp. 69-76.

ВИХАРЕВ Сергей Олегович – аспирант; МИРОНЧИКОВ Евгений Тимофеевич – д-р. техн. наук, профессор; *ГОФМАН Максим Викторович – канд. техн. наук, ст. преподаватель, maxgof@gmail.com (Петербургский государственный университет путей сообщения Императора Александра I).