



УДК 519.72

С. О. Вихарев, Е. Т. Мирончиков

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА МЕТОДИКИ ПОСТРОЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, УСТОЙЧИВЫХ К АТАКЕ «ВЫРЕЗАНИЕ»

Дата поступления: 09.06.2016

Решение о публикации: 06.09.2016

Цель: Показать эффективность методики построения цифровых водяных знаков, устойчивых к атаке «вырезание». **Методы:** Используемые в статье методы относятся к области теории информации и стеганографии. **Результаты:** Представлены результаты имитационного моделирования методики построения цифровых водяных знаков на основе БЧХ-синхрокодов; пример встраивания в цифровой аудиосигнал предлагаемых водяных знаков, а также пример их выделения даже после удаления из аудиосигнала некоторых случайных отсчётов. **Практическая значимость:** Представленные в статье цифровые водяные знаки можно использовать в качестве средства для внедрения дополнительной информации в цифровой аудиосигнал, так что даже после атаки «вырезание» на аудиосигнал с предлагаемыми цифровыми водяными знаками остаётся возможность восстановить внедрённую информацию.

БЧХ-код, синхронизация, цифровой водяной знак, цифровой аудиосигнал, атака «вырезание».

***Sergy O. Vikharev**, postgraduate student, vso9@yandex.ru; **Yevgeniy T. Mironchikov**, D. Sci. (Eng.), professor (Petersburg State Transport University) EXPERIMENTAL VERIFICATION OF A METHOD FOR BUILDING DIGITAL WATERMARKS RESISTANT TO CUTTING ATTACK

Objective: To demonstrate efficiency of a method for building digital watermarks resistant to cutting attacks. **Methods:** Methods applied in the paper fall within the domain of information theory and steganography. **Results:** Results of simulation modelling of a method for building digital watermarks based on BCH-codes are presented, as are an example of building proposed watermarks into digital audio signal, and an example of their extraction even after some accidental counts were removed from audio signal. **Practical importance:** Digital watermarks proposed in the paper can be used as a means for introducing additional information into digital audio signal, thus even after a cutting attack on audio signal with proposed digital watermarks it is still possible to recover embedded information.

BCH-code, synchronization, digital watermark, digital audio signal, cutting attack.

Цифровые аудиосигналы как объекты, содержащие аудиоинформацию, могут иметь большую ценность. Так, они могут представлять собой результат работы музыкантов и певцов и удовлетворять эстетические потребности людей. Или быть вместилищем

информации для работы, например, секретарей, журналистов, следователей, работников служб безопасности и т. д.

Рассмотрим два вида аудиоинформации: музыкальную и речевую. Общая цель – встроить цифровой водяной знак (ЦВЗ) в аудио-

контейнер для борьбы с атакой «вырезание» [9–11]. Эта атака представляет собой удаление некоторой доли отсчётов из цифрового аудиосигнала, в результате чего теряется возможность восстановить встроенную информацию [12, 14]. При этом ЦВЗ не должен быть слышимым [7]. Другими словами, отношение сигнал/шум должно удовлетворять порогам слышимости [6, 13].

Для достижения этой цели нужно разработать систему встраивания и извлечения информационных синхросигналов в аудиосигнал [2, 3]. При этом информационные синхросигналы, представляя собой ЦВЗ, должны быть устойчивыми к атаке «вырезание».

Атака «вырезание» может привести к тому, что некоторые элементы информационных синхросигналов будут утеряны. Вследствие этого возникает сбой синхронизации. Предлагаемые в работе ЦВЗ обладают устойчивостью к сбоям синхронизации, а именно позволяют определить, сколько элементов от информационного синхросигнала осталось.

Различают два вида сбоев синхронизации: потерю синхронизации, когда теряется начало информационного синхросигнала; избыток синхронизации, когда теряется конец информационного синхросигнала.

Процессы встраивания и выделения ЦВЗ в аудиосигнал

В качестве основы для информационных синхросигналов рекомендуется использовать синхрокоды на основе БЧХ-кодов, так как они хорошо изучены, просты и дешевы для применения в аппаратуре [1, 4, 5].

Для эксперимента используется двоичный БЧХ-код со следующими параметрами: длина кодового слова 63, количество информационных символов 30. Порождающий полином

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

Однако перед встраиванием БЧХ – кодового слова выполняется преобразование, операции которого позволяют получить кодовые слова так называемых синхрокодов. Благодаря синхрокодам можно определить величину и вид сбоя синхронизации. Синхрокодовые слова строятся путём прибавления специального полинома, который называется смещающим. В нашем случае таким полиномом будет $p(x) = x + 1$. Синхрокод с такими параметрами позволяет определить величину сдвига синхронизации вплоть до

$$r_c = \left\lfloor \frac{n - k - s - 1}{2} \right\rfloor = 15,$$

где $s = 1$ – степень смещающего полинома; $n = 63$ – длина кодового слова синхрокода; $k = 30$ – количество информационных символов в синхрокодовом слове. При этом следует учесть, что сложение не выполняется напрямую с самим смещающим полиномом. Вместо это смещающий полином масштабируется полиномом $1/x$, а уже результат масштабирования складывается с БЧХ – кодовым словом. Но в нашем случае в качестве масштабирующего полинома следует использовать полином, который является обратным к полиному x^{-1} по модулю порождающего полинома $g(x)$ над полем $GF(2)$, т. е. полином

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

Атака «вырезание» в общем случае может быть предпринята на любую часть аудиосигнала. Следовательно, чтобы вполне использовать свойство предлагаемых ЦВЗ, быть устойчивыми к сбоям синхронизации, их элементы следует встраивать в каждый отчёт аудиосигнала.

Наиболее распространённым методом встраивания информации в аудиосигнал является изменение младших битов числовых значений отсчётов аудиосигнала. Так, в [8] предлагается следующий подход. Предпо-

жим, что ЦВЗ представляет собой двоичный вектор

$$\mathbf{c} = (c_1 \ c_2 \ \dots \ c_N),$$

где $c_i \in \{0, 1\}$, а сам аудиосигнал представляет собой вектор

$$\mathbf{y} = (y_1 \ y_2 \ \dots \ y_N),$$

где $y_i \in \{0, 1, \dots, 2^{16} - 1\}$. Тогда числовое значение каждого элемента вектора \mathbf{y} заменяется на числовое значение по следующему правилу:

$$y_i' = \begin{cases} \left\lfloor \frac{y_i}{S} \right\rfloor \cdot S + \frac{3S}{4}, & \text{если } c_i = 1, \\ \left\lfloor \frac{y_i}{S} \right\rfloor \cdot S + \frac{S}{4}, & \text{если } c_i = 0, \end{cases}$$

где $\lfloor \cdot \rfloor$ – операция «пол»; S – «сила» встраивания. Величина S ограничена порогом слышимости. Процесс выделения встроенных двоичных символов выполняется следующим образом [15]:

$$c_i = \begin{cases} 1, & \text{если } y_i' - \left\lfloor \frac{y_i'}{S} \right\rfloor \cdot S \geq \frac{S}{2}, \\ 0, & \text{если } y_i' - \left\lfloor \frac{y_i'}{S} \right\rfloor \cdot S < \frac{S}{2}, \end{cases}$$

$$\begin{aligned} \mathbf{y}' = & (1016 \ 1112 \ 1208 \ 1304 \ 1400 \ 1496 \ 1624 \\ & 1720 \ 1816 \ 1912 \ 2008 \ 2104 \ 2200 \ 2296 \\ & 2424 \ 2520 \ 2616 \ 2712 \ 2808 \ 2904 \ 3000 \\ & 3096 \ 3224 \ 3320 \ 3416 \ 3512 \ 3608 \ 3704 \\ & 3800 \ 3880 \ 4024 \ 4104 \ 4200 \ 4312 \ 4408 \\ & 4504 \ 4600 \ 4680 \ 4824 \ 4904 \ 5016 \ 5096 \\ & 5192 \ 5288 \ 5400 \ 5496 \ 5624 \ 5704 \ 5816 \\ & 5912 \ 5992 \ 6088 \ 6184 \ 6280 \ 6424 \ 6504 \\ & 6600 \ 6712 \ 6792 \ 6904 \ 6984 \ 7096 \ 7208). \end{aligned}$$

Процесс выделения встроенной информации можно рассматривать как состоящий из двух стадий: выполнение указанных арифметических действий – первая;

Покажем на примере процедуру встраивания и выделения. Пусть

$$\mathbf{y} = (1000 \ 1100 \ \dots \ 7200).$$

Если «сила» встраивания $S = 32$, а ЦВЗ представляет собой полином

$$c_1(x) = (x^{33}m(x) - r(x) + w(x)p(x)) \bmod 2,$$

где $m(x) = \sum_{i=0}^{29} x^i$; $r(x)$ – остаток от деления x^{33} $m(x)$ на $g(x)$. В векторном виде получается

$$\mathbf{c}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Тогда аудиосигнал \mathbf{y} после встраивания будет таким:

вынесение решения – вторая. Результат первой стадии для рассматриваемого случая представляет собой вектор следующего вида:

Если атака «вырезание» привела к тому, что были потеряны первые три отсчёта, то после выделения встроенной информации вместо первого ЦВЗ будет получен вектор

$$\mathbf{c}' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Полином, по которому определяется величина и вид сбоя синхронизации для полученного вектора \mathbf{c}' , следующий:

$$\begin{aligned} r(x) &= ((x^{r_c+1}(c'(x) - \\ &- w(x)p(x))) \bmod g(x)) \bmod 2 = \\ &= x^{19} + x^{18} + x^{16} + x^{15}. \end{aligned}$$

Так как $19 > r_c + s$, видно, что произошла потеря синхронизации в $3 = 19 - r_c - s$ символа.

Теперь рассмотрим случай, когда в результате атаки «вырезание» утеряны пять последних отсчётов аудиосигнала y' . В этом случае вместо второго кодового слова будет получен вектор

$$\mathbf{c}' = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Получаем соответствующий полином:

$$\begin{aligned} r(x) &= ((x^{r_c+1}(c'(x) - \\ &- w(x)p(x))) \bmod g(x)) \bmod 2 = \\ &= x^{16} + x^{14} + x^{12} + x^{10}. \end{aligned}$$

Так как $10 < r_c$, видно, что произошел избыток синхронизации в $5 = r_c - 10$ символов. Полином $r(x)$ зависит от формы представления ЦВЗ. Так, он может отличаться у систематического и несистематического представления кодового слова БЧХ-кода. Однако результат оценки величины сбоя и вида синхронизации совпадают.

В общем случае предлагаемый ЦВЗ позволяет определить величину и вид сбоя синхронизации вплоть до потери количества символов в начале или в конце ЦВЗ, равного r_c .

Результаты имитационного моделирования

Важной характеристикой ЦВЗ, ориентированных на атаку «вырезание», является зависимость вероятности ошибки восстановления встроенной в ЦВЗ информации от доли удаляемых вырезанием отсчётов. Если позиции удаляемых отсчётов равномерно распределены по всей длине вектора, описывающего цифровой аудиосигнал, то для рассмотренного выше ЦВЗ, основанного на (63,30) БЧХ-коде, эта характеристика более сложна (см. таблицу).

Зависимость вероятности ошибки восстановления встроенной в ЦВЗ информации от доли удаляемых вырезанием отсчётов

Доля отсчётов аудиосигнала с ЦВЗ, подвергшихся атаке «вырезание»	Вероятность восстановления хранимой в ЦВЗ информации
0	1
0,01	0,52
0,02	0,27
0,03	0,16
0,04	0,09
0,05	0,04
0,06	0,02
0,07	0,01
0,08	0,009
0,09	0,004
0,1	0,002

Заключение

Рассмотрены процедуры создания ЦВЗ, устойчивых к сбоям синхронизации, вызванным атакой «вырезание», проведённой на случайные отсчёты аудиосигнала. Результаты имитационного моделирования показали, что предлагаемые ЦВЗ позволяют восстановить с положительной вероятностью встроенную в ЦВЗ информацию даже при доле удалённых отсчётов, равной 0,1.

Библиографический список

1. Берлекэмп Э. Алгебраическая теория кодирования : моногр. / Э. Берлекэмп – М. : Мир, 1971. – 479 с.
2. Вихарев С. О. Методика построения цифровых водяных знаков, устойчивых к сбоям синхронизации / С. О. Вихарев, Е. Т. Мирончиков, М. В. Гофман // Изв. ПГУПС. – 2016. – Т. 13, Вып. 1 (46). – С. 60–67.
3. Вихарев С. О., Мирончиков Е. Т., Гофман М. В. Свидетельство № 2016615347 от 20 мая 2016 г. о государственной регистрации программы для ЭВМ «Компьютерная модель оценки вероятности устойчивости цифровых водяных знаков, встроенных в аудиосигналы, к сбоям синхронизации, вызванным атакой «вырезание».
4. Золотарёв В. В. Помехоустойчивое кодирование. Методы и алгоритмы : справ. / В. В. Золотарёв, Г. В. Овечкин ; под. ред. чл.-корр. РАН Ю. Б. Зубарева. – М. : Горячая линия – Телеком, 2004. – 126 с.
5. Питерсон У. Коды, исправляющие ошибки : моногр. / У. Питерсон, Э. Уэлдон. – М. : Мир, 1976. – 594 с.
6. Bender W. Techniques for data hiding / W. Bender et al. // IBM Syst. J. – 1996. – Т. 35, № 3.4. – P. 313–336.
7. Boney L. Digital watermarks for audio signals / L. Boney, A. H. Tewfik, K. N. Hamdy // Proc. Third IEEE Int. Conf. Multimedia Computing and Systems, 1996. – IEEE, 1996. – P. 473–480.
8. Chen B. Quantization index modulation methods for digital watermarking and information embedding of multimedia / B. Chen, G. W. Wornell // J. VLSI Sig.

Proc. Syst. Sig., Image and Video Technol. – 2001. – Т. 27, № 1–2. – P. 7–33.

9. Chen N. A robust zero-watermarking algorithm for audio / N. Chen, J. Zhu // EURASIP J. Adv. Sig. Proc. – 2008. – Т. 2008. – P. 103.
10. Cox I. J. Digital watermarking / I. J. Cox et al. – San Francisco: Morgan Kaufmann, 2002. – Т. 1558607145.
11. Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks / ed. N. Cvejic. – IGI Global, 2007.
12. Steinebach M. StirMark benchmark: audio watermarking attacks / M. Steinebach et al. // Proc. Int. Conf. Inf. Technol. : Coding and Computing, 2001. – IEEE, 2001. – P. 49–54.
13. Swanson M. D. Robust audio watermarking using perceptual masking / M. D. Swanson et al. // Signal Proc. – 1998. – Т. 66, № 3. – P. 337–355.
14. Voloshynovskiy S. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks / S. Voloshynovskiy et al. // IEEE Commun. Mag. – 2001. – Т. 39, № 8. – P. 118–126.
15. Wu S. Efficiently self-synchronized audio watermarking for assured audio data transmission / S. Wu et al. // IEEE Trans. Broadcast. – 2005. – Т. 51, № 1. – P. 69–76.

References

1. Berlekemp E. Algebraicheskaya teoriya kodirovaniya: monografiya [Algebraic Coding Theory: A Monograph]. Moscow, Mir, 1971. 479 p.
2. Vikharev S. O., Mironchikov Ye. T. & Gofman M. V. *Izvestiya PGUPS – Proc. Petersburg Transp. Univ.*, 2016, T. 13, Is. 1 (46), pp. 60–67.
3. Vikharev S. O., Mironchikov Ye. T. & Gofman M. V. Certificate No. 2016615347, issued on May 20, 2016, On State Registration of Computer Program „Computer Model of Probability Assessment of Resistance of Digital Watermarks Built into Audio Signal to Synchronisation Errors Caused by Cutting Attack“.
4. Zolotarev V. V. & Ovechkin G. V. *Pomekhoustoychivoye kodirovaniye. Metody i algoritmy: spravochnik* [Noiseless Coding. Methods and Algorithms: Reference Book]; ed. Russian Academy of Sciences

corresponding member РАН Yu. B. Zubarev. Moscow, Goryachaya Liniya – Telekom, 2004. 126 p.

5. Peterson U. & Ueldon E. Kody, ispravlyayushchiye oshibki: monografiya [Error-Correcting Codes: A Monograph]. Moscow, Mir, 1976. 594 p.

6. Bender W. et al. Techniques for data hiding. *IBM Syst. J.*, 1996, T. 35, no. 3.4, pp. 313-336.

7. Boney L., Tewfik A. H. & Hamdy K. N. Digital watermarks for audio signals. *Proc. Third IEEE Int. Conf. Multimedia Computing and Systems*, 1996. IEEE, 1996. Pp. 473–480.

8. Chen B. & Wornell G. W. Quantization index modulation methods for digital watermarking and information embedding of multimedia. *J. VLSI Sig. Proc. Syst. Sig., Image and Video Technol.*, 2001, T. 27, no. 1-2, pp. 7-33.

9. Chen N. & Zhu J. A robust zero-watermarking algorithm for audio. *EURASIP J. Adv. Sig. Proc.*, 2008, T. 2008, pp. 103.

10. Cox I. J. et al. Digital watermarking. San Francisco, Morgan Kaufmann, 2002. T. 1558607145.

11. Digital Audio Watermarking Techniques and Technologies: Applications and Benchmarks; ed. N. Cvejic. IGI Global, 2007.

12. Steinebach M. et al. StirMark benchmark: audio watermarking attacks. *Proc. Int. Conf. Inf. Technol.: Coding and Computing*, 2001. IEEE, 2001. Pp. 49-54.

13. Swanson M. D. et al. Robust audio watermarking using perceptual masking. *Signal proc.*, 1998, T. 66, no. 3, pp. 337-355.

14. Voloshynovskiy S. et al. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *IEEE Commun. Mag.*, 2001, T. 39, no. 8, pp. 118-126.

15. Wu S. et al. Efficiently self-synchronized audio watermarking for assured audio data transmission. *IEEE Trans. Broadcast.*, 2005, T. 51, no. 1, pp. 69-76.

Благодарность

Авторы благодарят за помощь в организации и проведении имитационного моделирования к.т.н. М. В. Гофмана, доцента кафедры «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I.

*ВИХАРЕВ Сергей Олегович – аспирант, vso9@yandex.ru; МИРОНЧИКОВ Евгений Тимофеевич – доктор техн. наук, профессор (Петербургский государственный университет путей сообщения Императора Александра I).