УДК 004.056.55

Ковтуненко Аркадий Алексеевич, аспирант, Петербургский государственный университет путей сообщения Императора Александра I, г. Санкт-Петербург

ОБЗОР ОСНОВНЫХ МЕТОДОВ ЦИФРОВОГО МАРКИРОВАНИЯ И ВНЕДРЕНИЯ ВОДЯНЫХ ЗНАКОВ В АУДИОСИГНАЛЫ

Аннотация. За последние годы возросла важность использования цифровых водяных знаков для маркирования аудиосигналов. Данная статья служит для ознакомления с основными методами цифрового маркирования аудиосигналов – LSB, Spread Spectrum, Patchwork, Echo Hiding. Рассматриваются принципы работы методов, их преимущества и недостатки с точки зрения устойчивости к атакам и искажениям, прозрачности и вычислительной эффективности. Уделено внимание ссылкам на современные модификации рассматриваемых методов из преимущественно зарубежных научных работ 2023-2025 годов, совершенствующих недостатки классических подходов. Статья призвана упростить поиск современной литературы по данной области.

Abstract. In recent years, the importance of using digital watermarks for audio signal marking has significantly increased. This article provides an overview of the main methods of digital audio watermarking – LSB, Spread Spectrum, Patchwork, Echo Hiding. The principles od each method are examined, along with their advantages and disadvantages in terms of robustness against attacks and distortions, transparency and computational efficiency. Attention is paid to references to modern modifications of the methods under consideration from mainly foreign scientific works of 2023-2025, improving the shortcomings of classical approaches. The article is intended to simplify the search for modern literature in this field.

Ключевые слова: аудио, стеганография, водяные знаки, наименьшие значащие биты, расширение спектра, метод лоскута, сокрытие эха.

Keywords: audio, steganography, watermarking, least significant bit, spread spectrum, patchwork, echo hiding.

Введение

С развитием технологий генерации аудио на основе нейронных сетей [1] возрастает распространение фейковой информации и, соответственно, потребность в борьбе с подделкой аудиосигналов и нарушением авторских прав. Для этого существуют цифровые водяные знаки – скрытно внедрённая в аудиофайл информация о нём [2] (электронная подпись или идентификационный номер). Для понимания процесса маркирования аудиосигналов цифровыми водяными знаками нужно знать базовые методы – принципы их работы, преимущества и недостатки.

Целью данной статьи является ознакомление с основными методами маркирования аудиосигналов, а именно «наименьших значащих бит» (LSB сокр. от англ. Least Significant Bit), «расширения спектра» (SS сокр. от англ. Spread Spectrum), «лоскута» (от англ. patchwork), «сокрытия эха» (от англ. Echo Hiding). В рамках исследования будут рассмотрены принципы работы каждого метода, их сильные и слабые стороны, а также приведены ссылки на современные научные работы, исправляющие недостатки классических подходов и повышающие их эффективность.

Метод LSB

Метод Least Significant Bit один из самых простых и ранних методов маркирования. Применялся в стеганографии с 1980-х годов преимущественно для внедрения скрытой информации в изображения, но позже был адаптирован для встраивания цифрового водяного знака в аудио [3].

Принцип действия метода заключается в изменении наименьших значащих бит отсчётов аудиосигнала. Например, в отсчёте размером 16 бит, какие используются обычно в WAV-файлах, можно заменить только последний бит или же 2-3 последних, при этом, во втором случае, слышимые искажения сигнала будут более заметны, чем, соответственно, в первом.

Таким образом, метод позволяет внедрять большие объёмы скрытой информации в аудиосигнал. Это справедливо даже для изменения всего одного последнего бита в отсчёте, поскольку в среднем количество отсчётов в маркируемом аудиосигнале может исчисляться от сотен тысяч. Также изменение всего одного наименее значащего бита на отсчёт делает слышимые искажения пренебрежительно малыми. При всём этом метод не требует высоких вычислительных мощностей, является быстрым и лёгким решением для маркирования сигнала [4].

Однако ввиду своей примитивности метод LSB уязвим к любым преобразованиям аудиосигнала. Шум, сжатие, фильтрация, удаление или добавление отсчётов и т.д. искажают или полностью разрушают водяной знак. Также извлечь скрытую информацию вслепую не получится – нужно точно знать в какие отсчёты и в какое количество наименее значимых бит она была встроена.

В работах [5] [6] приводятся различные модификации метода LSB для цифрового водяного знака в аудиосигналах с улучшенной незаметностью и устойчивостью к атакам и искажениям. В работе [7] наоборот используется уязвимость LSB для обнаружения несанкционированных изменений в аудиофайлах.

Расширение спектра

Метод расширения спектра также является одним из первых методов в области цифровых водяных знаков и появился ещё до их массового использования. Изначально метод расширения спектра был разработана для применения в радиосвязи в середине XX века, но с 90-х годов метод стали адаптировать для использования цифровых водяных знаков [8].

Принцип работы метода заключается в следующем: исходный сигнал преобразуется в частотную область после чего создаётся ключ (псевдослучайная последовательность), каждый бит водяного знака модулируется как +1 или -1 и масштабируется на ключ. Полученный сигнал прибавляется к исходному в

выбранных частотных диапазонах (области спектра, которые могут переносить водяной знак без ущерба для точности восприятия) [9]. Извлечение водяного знака происходит посредством корреляции принятого сигнала с оригинальным ключом.

При этом подходе водяной знак распределяется по широкой полосе частот с малой амплитудой, благодаря чему обеспечивается высокая устойчивость к разного рода атакам и искажениям [10]. Также из-за распределения сигнала по частотам и при грамотном выборе силы внедрения водяной знак не влияет на звуковое восприятия сигнала, не создавая слышимых артефактов. Защита обеспечивается за счёт использования псевдослучайной последовательности в роли ключа, без знания которого злоумышленнику не получится как извлечь водяной знак, так и в целом обнаружить его наличие в сигнале.

Однако, чтобы не нарушать качество звука, мощность внедрения должна быть ограничена, из-за чего получится внедрить только малый объём информации, хотя для идентификатора его вполне достаточно. Также в качестве недостатка следует отметить, что если аудиосигнал подвергся временным искажениям, то синхронизация ключей нарушается и извлечение водяного знака становится невозможным. В то же время если злоумышленник владеет несколькими копиями одного аудиосигнала с разными водяными знаками, он может усреднить их и таким образом удалить водяной знак, что критично для массового аудиоконтента. При всём этом метод использует такие операции как преобразование в частотной области, корреляционный анализ, генерация и синхронизация псевдослучайных последовательностей, что требует большого числа вычислений [11].

В работе [12] метод расширения спектра используется в системе водяных знаков для минимизации задержек и обеспечения устойчивости к искажениям, а в работе [13] новый подход стеганографии базируется на расширении спектра в аудиофайлах.

Метод лоскута

Является уже более поздним методом, предложен впервые в 1996 году [3], где он был представлен как статистический подход к скрытию информации в изображениях, но, ввиду своей универсальности, быстро стал использоваться и в области аудиостеганографии.

Принцип метода заключается в том, что выбирается пара случайных участков цифрового объекта (лоскутов), один из них увеличивается, а один уменьшается на одну и ту же величину. В случае аудиосигнала «лоскутами» служат отсчёты, а величиной зачастую амплитуда. Порядок уменьшения и увеличения элементов пары зависит от внедряемого бита (1 или 0). При извлечении вычисляется разность средних значений между каждой парой и знак этой разности интерпретируется как 1 или 0. Таким образом, пара элементов переносит один бит скрытой информации.

При данном методе изменения в аудиофайле практически не заметны, благодаря их минимальности и статистическому распределению по всему объекту. Также для проверки водяного знака достаточно наличие ключа, на основе которого производился выбор пар отсчётов, без самого оригинального аудиосигнала [14]. Такой подход называется «слепым детектированием» и, по понятным причинам, эффективнее. Алгоритм метода лоскута при этом остаётся достаточно простым в реализации и энергоэффективным, при этом показывая достойный уровень устойчивости к различным обработкам сигнала.

Недостатки метода вытекают из его сильных сторон: раз для извлечения водяного знака требуется только ключ, то при его искажении или потере извлечение становится невозможным. Поскольку для передачи одного бита используется пара отсчётов аудиосигнала, метод характеризуется низкой ёмкостью внедряемой информации и чувствительностью к синхронизации – изменение порядка отсчётов приводит к неправильному извлечению водяного знака.

В работах [15] [16] [17] приводятся различные варианты улучшения метода лоскута, демонстрирующие более низкую вероятность ошибок, повышенную надёжность, энергоэффективность и устойчивость к атакам и искажениям.

Скрытие эха

Метод Echo Hiding также впервые появился в работе [3], где авторы впервые предложили использовать неравномерные задержки между эхо-сигналами как способ кодирования информации. Эхо-сигналами в аудио принято называть копию исходного сигнала, но характеризующуюся уменьшенной громкостью, небольшой задержкой и зачастую затуханием со временем.

Принцип метода заключается во внедрении эхо-сигналов в отсчёты аудиофайла с определённой задержкой. Для кодирования нулевого и единичного бита используется разная задержка, но оба варианта задержки не должны превосходить порог чувствительности слуховой системы человека. При извлечении водяного знака сигнал обрабатывается автокорреляцией, обнаруживая эхо и выявляя задержки.

Самым значимым преимуществом метода является его минимальное влияние на качество звука – при грамотном внедрении эхо-сигналов изменения невосприимчивы на слух, – а также он хорошо устойчив к частотным и амплитудным искажениям и атакам.

Однако метод сокрытия эха очень ограничен в пропускной способности и уязвим к атакам по времени (обрезке, сдвигу, масштабированию). Но главным недостатком является необходимость точной настройки параметров эхо-сигналов, таких как время задержки и амплитуда, и выбор отсчётов для внедрения эха, так как использования эха в отсчётах с низкой энергией будет заметно влиять на слышимость.

В работе [18] рассматривается использование симметричных эхо-сигналов, компенсирующих влияние друг друга, тем самым минимизируя искажения. В

работе [19] метод скрытия эха оптимизируется для противостояния атакам по времени. В работе [20] ставится акцент на подборе оптимального времени задержки и амплитуды эха в зависимости от спектральных характеристик аудио, значительно увеличивая вместимость водяного знака и устойчивость извлечения.

Заключение

Как бы ни было очевидно, не существует универсального метода маркирования аудиосигналов. У каждого метода есть свои сильные и слабые стороны, выбор алгоритма должен осуществляться исходя из целей внедрения, типа сигнала, допустимого уровня искажений и списка угроз.

Например, метод LSB целесообразен в системах, где важна вместимость и отсутствует риск серьёзных искажений. Метод SS подходит для потоковых сервисов, где сигнал подвергается многократной обработке. Метод лоскута ограничен в ёмкости и уязвим к атакам по известному ключу, поэтому может использоваться для неперсонифицированного отслеживания распространения аудиоконтента. Метод скрытия эха эффективен в вещательных и трансляционных системах, где сохраняется высокая частотная и временная структура сигнала.

Многие недостатки классического представления этих методов были доработаны в современных работах, но всё же фундаментальные черты методов остаются закреплены за ними до сих пор. Поэтому перспективным является использование гибридных подходов, объединяющих различные методы в зависимости от их преимуществ и недостатков для достижения баланса между надёжностью, ёмкостью и незаметностью.

Литература

1. Google представила ИИ-генератор видео со звуком и пообещала новую эру // РБК [Электронный ресурс] / URL: https://www.rbc.ru/technology_and_media/20/05/2025/682cdce39a7947e999a3cd3c (дата обращения: 27.05.2025).
2. I. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, San Francisco, 2002.
3. Bender W, Gruhl D, Morimoto N, Lu A. Techniques for data hiding. IBM System Journal. 1996.
4. Bah J., Ramakishore R. LSB Technique And Its Variations Used In Audio Steganography: A Survey. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 4, April – 2013.
5. Chetan, M & Bhat, Prarthana & Shet, Vrushabh & Husenbhai, Sana & Bhat, Ashwini. (2021). Audio Watermarking Using Modified Least Significant Bit Technique. 1-5. 10.1109/CCUBE53681.2021.9702715.
6. Ferdaush, Mst & Bhuiyan, Touhid. (2025). Proposal of an optimum method of audio steganography to secure data transfer. Journal of Infrastructure, Policy and Development. 9. 10020. 10.24294/jipd10020.
7. A. Ghobadi, A. Boroujerdizadeh, A. H. Yaribakht and R. Karimi, Blind audio watermarking for tamper detection based on LSB, 2013 15th International Conference on Advanced Communications Technology (ICACT), PyeongChang, Korea (South), 2013, pp. 1077-1082.
8. Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12), 1673–1687.
9. Hartung, F., & Girod, B. (1999). Spread Spectrum Watermarking: Malicious Attacks and Counterattacks.
10. Kirovski, D., & Malvar, H. S. (2003). Spread-Spectrum Watermarking of Audio Signals. IEEE Transactions on Signal Processing, 51(4), 1020–1033.

11. Jiang N, Wang J. The theoretical limits of watermark spread spectrum sequence. ScientificWorldJournal. 2014 Mar 23;2014:432740. doi: 10.1155/2014/432740. PMID: 24790566; PMCID: PMC3982297.
12. Santin-Cruz, C.J.; Dolecek, G.J. Audio Watermarking System in Real-Time Applications. Informatics 2025, 12, 1.
13. Zhelezov, Stanimir & Kordov, Krasimir & Nachev, Atanas & Pavlova, Daniela & Gindev, Panayot & Litchkov, Nikolay & Nesterov, Konstantin. (2024). A New Approach for Spread Spectrum Steganography in Audio Containers. 474-477. 10.1109/SUMMA64428.2024.10803739.
14. Chincholkar, Y.D., & Ganorkar, S. (2019). Audio Watermarking Algorithm Implementation using Patchwork Technique. 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 1-5.
15. Гофман, М. В. Устойчивое цифровое маркирование в аудиостегосистемах с множественным входом и множественным выходом / автореф. дис. ... д-ра техн. наук / 2.3.6 – Методы и системы защиты информации, информационная безопасность / М. В. Гофман; Петербургский государственный университет путей сообщения императора Александра I. – Санкт-Петербург, 2023.
16. Zhenghui Liu, Yuankun Huang, and Jiwu Huang. 2019. Patchwork-Based Audio Watermarking Robust Against De-Synchronization and Recapturing Attacks. Trans. Info. For. Sec. 14, 5 (May 2019), 1171–1180.
17. Chuxuan Tong, Iynkaran Natgunanathan, Yong Xiang, Jianhua Li, Tianrui Zong, Xi Zheng, and Longxiang Gao. 2024. Enhancing Robustness of Speech Watermarking Using a Transformer-Based Framework Exploiting Acoustic Features. IEEE/ACM Trans. Audio, Speech and Lang. Proc. 32 (2024), 4822–4837.
18. Masoumeh Velayatipour, Mohammad Mosleh, Mohsen Yoosefi Nejad, and Mohammad Kheyrandish. 2025. Towards secure quantum communication: a novel quantum audio watermarking based on bipolar echo hiding. Computing 107, 3 (Mar 2025).

19. Santin-Cruz CJ, Dolecek GJ. Audio Watermarking System in Real-Time Applications. *Informatics*. 2025; 12(1):1.
20. Tianyu Yang, Canghong Shi, Minfeng Shao, Sani M. Abdullahi, Imran Mumtaz, Yong Liu, Ling Xiong, An adaptive and large payload audio watermarking against jittering attacks, Computers and Electrical Engineering, Volume 124, Part A, 2025, 110321, ISSN 0045-7906.