Рисунок 4 – Некорректная работа метода

Таким образом, можно сказать, что выделение акцентных цветов для изображений, имеющих высокий контраст между фоном и акцентным цветом с использованием представленного метода, работает корректно и позволяет регулировать точность выделения с помощью параметров t и k. Однако в случае низкой контрастности и общей насыщенности всех оттенков результаты могут быть неточны.

ЛИТЕРАТУРА

1. Wang L., Zhang Y., Feng J. On the Euclidean distance of images // IEEE transactions on pattern analysis and machine intelligence. 2005. Vol. 27, no. 8. P. 1334–1339.

2. Adams R., Bischof L. Seeded region growing // IEEE Transactions on pattern analysis and machine intelligence. 1994. Vol. 16. no. 6. P. 641–647.

3. CIE International Commission on Illumination, Recommendations on Uniform Color Spaces, Color-Difference Equations, Psychometric Color Terms, Supplement. No. 2 to CIE Publication No. 15, Colorimetry, 1971.

УДК 004.056.55:004.627

Н.В. Попеня, ст. преп.
(БГТУ, г. Минск)

СТРУКТУРА ГИБРИДНОГО МЕТОДА ЗАЩИТЫ АВТОРСКИХ ПРАВ НА МУЛЬТИМЕДИЙНЫЙ КОНТЕНТ

Стремительный рост объемов мультимедийного трафика в глобальных сетях, который по прогнозам составляет более 80% от всего интернет-трафика [1], обостряет проблему защиты авторских прав на цифровой контент. Традиционные криптографические средства и системы управления цифровыми правами (DRM) обеспечивают защиту преимущественно на этапе передачи данных, оставляя контент уязвимым для копирования. В связи с этим актуальным направлением является применение методов компьютерной стеганографии, позволяю-

щих скрытно и неотделимо внедрять маркеры авторства непосредственно в медиаданные [2].

Ключевым препятствием для внедрения стеганографических систем является использование стандартов сжатия с потерями, таких как H.264/AVC для видео и AAC для аудио. Алгоритмы квантования, лежащие в их основе, удаляют психовизуальную и психоакустическую избыточность, что приводит к необратимому разрушению информации, встроенной классическими методами пространственной области. Анализ предметной области показывает, что большинство существующих робастных алгоритмов функционируют изолированно, защищая либо только видеоряд, либо только аудиоряд, что снижает общую надежность системы [3].

Предлагаемый метод базируется на концепции декомпозиции мультимедийного контейнера и независимой адаптивной обработки его составляющих. В отличие от монолитных подходов, архитектура разработанной системы предполагает разделение исходного файла на элементарные потоки (демультиплексирование) с последующим параллельным встраиванием данных. Для видеопотока применяется адаптивная модуляция индекса квантования (QIM) коэффициентов дискретного косинусного преобразования (DCT), использующая анализ движения и текстуры. Для аудиопотока используется метод эхокодирования с адаптивным кепстральным анализом [4].

Важной структурной особенностью метода является реализация механизма криптографической связки. Данный подход подразумевает перекрестный контроль целостности: верификационные данные видеопотока могут быть встроены в аудиопоток, и наоборот. В результате, для успешного удаления авторской метки злоумышленнику необходимо подвергнуть деструктивной атаке все составляющие медиаконтейнера, что делает атаку нецелесообразной из-за критической потери качества контента.

Для строгого описания процессов защиты разработана теоретико-множественная модель гибридной стегосистемы Σ, которая представляется кортежем:

$$\Sigma = \langle C, D, M, P, K, F, F^{-1}, S \rangle, \quad (1)$$

где C – множество исходных контейнеров;

D – преобразование декомпозиции на видео- и аудиосегменты;

M – множество авторских сообщений;

P – процедура подготовки данных;

K – пространство ключей;

F и F^{-1} – функции встраивания и извлечения;

S – множество результирующих стегоконтейнеров.

Особое внимание в структуре метода уделено предварительной подготовке данных. Для обеспечения инвариантности авторской метки к битовым ошибкам применяется каскадная схема обработки. Она включает сериализацию данных в компактный бинарный формат, помехоустойчивое кодирование для исправления одиночных инверсий и симметричное шифрование для обеспечения конфиденциальности. Сама структура данных оптимизирована и содержит блоки идентификации автора и контента, временную метку и контрольную сумму CRC32 [5].

Адаптивный характер метода требует управления сложным набором параметров, что отражено в структуре стегоключа K. Он объединяет три функциональных подмножества: параметры шифрования и кодирования; пороговые значения детекторов движения и энергии для выбора областей встраивания; параметры силы встраивания, такие как шаг квантования и амплитуда эха. Такая детализация позволяет гибко настраивать баланс между робастностью и скрытностью системы в зависимости от требований к качеству контента.

Реализация предложенной структуры базируется на использовании специализированных алгоритмов для каждого типа медиаданных, учитывающих их психовизуальные и психоакустические особенности. Для видеоканала разработан и применен двухпроходный алгоритм адаптивной стеганографии. На первом, аналитическом этапе, производится оценка межкадрового движения с использованием алгоритма Лукаса-Канаде и анализ внутрикадровой текстуры с помощью оператора Лапласа. Это позволяет сформировать карту пригодности областей, исключая динамичные сцены, где артефакты сжатия наиболее вероятны. Непосредственное встраивание осуществляется на втором этапе методом модуляции индекса квантования (QIM) коэффициентов дискретного косинусного преобразования (DCT). Ключевой особенностью здесь является динамическое изменение шага квантования: в текстурированных областях он увеличивается для повышения робастности, а в гладких – уменьшается для обеспечения скрытности.

Параллельно в аудиоканале реализуется метод эхо-кодирования, который использует временную задержку сигнала для кодирования битов информации. Для преодоления проблемы искажения амплитуды эха, возникающей при сжатии кодеком AAC, в структуру детектора введен блок адаптивного кепстрального анализа. Порог детектирования информационного пика в кепстре не является фиксированным, а вычисляется динамически для каждого аудиофрейма на основе статистики фонового шума. Такой подход позволяет минимизировать вероятность ложных срабатываний и уверенно извлекать данные даже из зашумленного сигнала [4].

Экспериментальная апробация разработанной структуры проводилась путем моделирования атак сжатия с использованием современных стандартов кодирования. Тестовая выборка включала видеопоследовательности высокого разрешения и разнородные аудиофрагменты. Для видеопотока применялась компрессия кодеком H.264/AVC (реализация libx264) со средним битрейтом 10 000 кбит/с. Для аудиопотока использовался кодек AAC с битрейтом 256 кбит/с, что соответствует стандартному качеству стриминговых платформ.

Результаты экспериментов показали высокую эффективность предложенного гибридного подхода. Средний коэффициент битовых ошибок (BER) для видеоканала составил менее 10%, а для аудиоканала – менее 6%. Полученные значения ошибок находятся в пределах корректирующей способности примененных на этапе подготовки данных. Это означает, что после декодирования помехоустойчивого кода результирующая авторская метка восстанавливается полностью без искажений. Таким образом, подтверждена способность системы сохранять целостность встроенной информации в условиях агрессивной среды передачи, характерной для современных видеохостингов.

Предложенный подход преодолевает ограничения традиционных одноканальных методов за счет одновременного использования информационных ресурсов видео- и аудиопотоков, объединенных механизмом криптографической связки.

Формализация математической модели системы и структуры многокомпонентного ключа позволила реализовать адаптивное управление параметрами встраивания, учитывающее локальные характеристики сигнала (динамику, текстуру, энергию). Сочетание разработанной методики предварительной подготовки данных, включающей помехоустойчивое кодирование, с адаптивными алгоритмами модуляции DCT-коэффициентов и кепстрального анализа обеспечило инвариантность скрытых меток к воздействию современных алгоритмов сжатия.

ЛИТЕРАТУРА

1. Cisco Annual Internet Report (2018–2023) White Paper [Электронный ресурс] / Cisco. – San Jose : Cisco Systems, 2020. – Режим
доступа: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. – Дата доступа:09.02.2026.

2. Cox, I. J. Digital Watermarking and Steganography / I. J. Cox [et al.]. – 2nd ed. – Burlington : Morgan Kaufmann, 2008. – 593 p.

3. Al-Nabhani, A. Robust Video Watermarking: A Review [Электронный ресурс] / A. Al-Nabhani, H. Al-Mawali, H. Jalab // Inter-

national Journal of Computer Science Issues. – 2016. – Vol. 13, Issue 6. – P. 32–40. – URL: https://ijcsi.org/papers/IJCSI-13-6-32-40.pdf. – Дата доступа: 09.02.2026.

4. Попеня Н.В., Романенко Д. В. Метод аудиостеганографии для AAC-сжатых аудиосигналов на основе эхо-кодирования и адаптивного кепстрального анализа // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2025. № 2 (296). С. 110–119.

5. Попеня Н.В. Методика подготовки и структура авторских данных для защиты видеофайла методами стеганографии // Труды БГТУ. Сер. 4, Принт- и медиатехнологии. 2025. № 2 (297). С. 71–77.

УДК 004.43

М.Ф. Кудлацкая, доц., канд. техн. наук
(БГТУ, г. Минск)

УПРАВЛЕНИЕ ГЛОБАЛЬНЫМ СОСТОЯНИЕМ В REACT-ПРИЛОЖЕНИЯХ

В течение длительного периода стандартом для управления данными в React-приложениях являлась библиотека Redux. Это сформировало архитектурную парадигму, предполагающую хранение всех типов данных – от бизнес-сущностей до состояния UI-компонентов – в едином глобальном дереве состояния (Store). Однако эволюция React, в частности внедрение Hooks API и Context API, а также рост сложности клиентских интерфейсов, выявили ряд системных ограничений монолитного подхода [1]:

– избыточность шаблонного кода (Boilerplate);

– накладные расходы на производительность;

– нарушение принципа разделения ответственности.

Ключевым трендом современной frontend-разработки стало четкое разграничение двух категорий данных: состояния сервера (Server State) и состояния клиента (Client State).

1. Client State: синхронные, локальные данные, полностью контролируемые клиентским приложением (темы оформления, состояние модальных окон, данные форм).

2. Server State: асинхронные данные, персистентно хранящиеся на удаленном сервере. Клиент владеет лишь их проекцией, которая может устареть в любой момент времени.

Попытки управлять серверным состоянием посредством универсальных менеджеров (например, Redux) требуют ручной реализации механизмов загрузки, кэширования, дедупликации запросов и инвалидации данных.