Алгоритм цифрового водяного знака на основе DWT–DCT

Цифровой водяной знак (ЦВЗ) является важным инструментом защиты авторских прав и аутентификации мультимедийных данных. При разработке алгоритмов водяного знака необходимо учитывать два ключевых требования:

- Незаметность (imperceptibility): встроенная метка не должна ухудшать визуальное качество изображения.
- Устойчивость (robustness): метка должна сохраняться после распространённых атак — сжатия, шума, масштабирования и других искажений.

С этой целью широкое распространение получили гибридные методы, в частности алгоритм на основе комбинации дискретного вейвлет-преобразования (DWT) и дискретного косинусного преобразования (DCT). Использование DWT обеспечивает многомасштабное разложение изображения, а DCT позволяет выбрать частоты, оптимальные для внедрения метки.

1. Теоретические основы

1.1. Дискретное вейвлет-преобразование (DWT)

DWT разбивает изображение на четыре поддиапазона:

- LL – аппроксимация (низкие частоты, глобальная структура).
- HL, LH, HH – детали (высокочастотные компоненты по горизонтали, вертикали и диагонали).

Для встраивания метки в коде используется двухуровневое DWT:

- Первое разложение формирует LL, LH, HL, HH.
- Второе разложение применяется к компоненте HL, после чего в поддиапазоне HL2 осуществляется внедрение.

Такой выбор обеспечивает баланс между незаметностью (не искажается LL) и устойчивостью (HL содержит достаточно энергии для надёжного встраивания).

1.2. Дискретное косинусное преобразование (DCT)

Каждый блок изображения размером n × n подвергается DCT. Полученные коэффициенты упорядочиваются по схеме зигзага.

- Низкочастотные коэффициенты (в начале зигзага) отвечают за общее восприятие изображения.
- Высокочастотные коэффициенты легко теряются при сжатии.
- Поэтому встраивание выполняется в среднечастотной зоне (mid-band).

В коде диапазон mid-band выбирается по долям: low = 0.3, high = 0.7 (т.е. отбираются коэффициенты с 30% по 70% длины зигзага).

Псевдослучайные последовательности (PN-sequences)

Для повышения надёжности используется распространённый спектр (spread spectrum):

- Для каждого бита водяного знака генерируются две PN-последовательности (−1,+1).
- Если встраивается бит 0, добавляется PN0, если 1 — PN1.
- Коэффициенты DCT модифицируются по правилу:

$$C' = C + \alpha \cdot PN$$

где α — коэффициент силы встраивания.

2. Процесс встраивания (Encode)

- Применяется двухуровневое DWT к исходному изображению.
- Из поддиапазона HL2 извлекаются блоки 4×4.
- Для каждого блока выполняется DCT.
- В mid-band коэффициенты встраиваются биты водяного знака с использованием PN-последовательностей и коэффициента α.
- Выполняются обратные преобразования: IDCT → IDWT → восстановленное изображение с внедрённым водяным знаком.

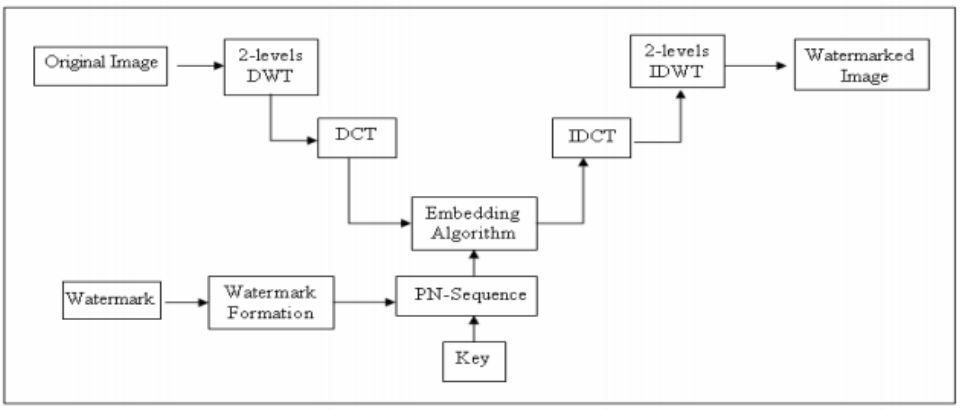

Рис.1: Комбинированная процедура встраивания водяного знака с использованием DWT-DCT.

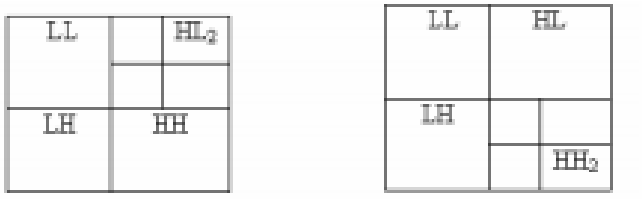

Рис.2: Многомасштабные поддиапазоны DWT исходного изображения.

3. Процесс извлечения (Decode)

- К изображению с водяным знаком применяется то же двухуровневое DWT.
- В поддиапазоне HL2 выполняется блочное DCT.
- Для каждого блока вычисляется корреляция mid-band коэффициентов с PN0 и PN1.
- Побеждает последовательность с большей корреляцией → восстанавливается бит (0 или 1).
- Итоговый водяной знак формируется усреднением результатов по всем блокам.

4. Метрики оценки

Для количественной оценки применяются:

- PSNR (Peak Signal-to-Noise Ratio) — измеряет искажение изображения. Значение выше 30 дБ считается приемлемым.

- Bit Accuracy — доля правильно восстановленных битов:

$$Acc = \frac{\text{число совпавших битов}}{\text{длина водяного знака}} \times 100\%$$

5. Преимущества и ограничения

Преимущества:

- Высокая устойчивость к сжатию JPEG и добавлению шума.
- Незаметность благодаря использованию среднечастотной зоны.
- Возможность регулирования баланса «качество/устойчивость».

Ограничения:

- Относительно высокая вычислительная сложность по сравнению с методами только DWT или DCT.
- Уязвимость к сильным геометрическим атакам (крупное кадрирование, масштабирование).

Алгоритм DWT–DCT является одним из наиболее эффективных гибридных методов цифрового водяного знака. Использование двухуровневого вейвлет-разложения и выбор среднечастотных коэффициентов в DCT позволяет достичь баланса между незаметностью и устойчивостью. Такой подход делает метод перспективным для защиты авторских прав и аутентификации цифровых изображений в реальных условиях эксплуатации

Алгоритм цифрового водяного знака на основе DWT–DCT–SVD

Защита авторских прав и аутентификация источника цифрового контента требуют встраивания метки, сохраняющейся после типичных преобразований (сжатие, шум, размытие, умеренные геометрические искажения) и при этом незаметной для зрителя. Для достижения указанного компромисса рассматривается гибридная схема DWT–DCT–SVD.

Её идея заключается в том, чтобы: (i) выбрать устойчивую по энергии область изображения с помощью 2D-вейвлет-разложения; (ii) перейти к блочному частотному представлению через DCT и адресно работать в среднечастотной зоне (mid-band); (iii) кодировать биты посредством квантования индексов (QIM) на наибольшем сингулярном значении SVD, вычисленном для mid-band-части каждого блока.

В дальнейшем излагаются теоретические предпосылки, процедурные шаги, метрики оценки и ключевые проектные решения.

1. Теоретические основы и выбор архитектуры

1.1. Одноуровневое 2D-DWT (вейвлет Хаара)

Пусть входное изображение в градациях серого обозначено II. Одноуровневое разложение даёт:

$$I \xrightarrow{\text{DWT}} (LL_1, LH_1, HL_1, HH_1).$$

Компонента LL_1 аккумулирует основную энергию и глобальные структуры, что делает её сравнительно стабильной к множеству искажений. В предлагаемой конфигурации метка встраивается именно в LL_1 ; потенциальный риск визуальной заметности компенсируется маской (при наличии), ограничивающей модификации текстурными областями.

1.2. Блочное DCT и mid-band

Поддиапазон LL_1 разбивается на блоки 4 × 4. Для блока BB вычисляется C = DCT(B). Коэффициенты упорядочиваются «змейкой» (zigzag), а mid-band выбирается как долевой интервал $[0.30, 0.70]$ длины зигзага. Такой выбор исключает DC-компоненту (вносит

наибольшую заметность) и крайние высокие частоты (наиболее чувствительны к компрессии), обеспечивая тем самым баланс между незаметностью и робастностью.

1.3. SVD для mid-band и QIM-кодирование

Из матрицы C формируется «маскированная» матрица C_{mb} , нулевая вне mid-band. Выполняется разложение

$$C_{\mathrm{mb}} = U\,\Sigma\,V^{\top}, \quad \Sigma = \mathrm{diag}(s_0, s_1, s_2, s_3),\ s_0 \geq s_1 \geq \dots$$

и модифицируется **только** наибольшее сингулярное значение s_0 с помощью **QIM**. Пусть шаг квантования $\Delta > 0$. Для бита $b \in \{0,1\}$ задаётся правило:

$$s_0' = \left(\left\lfloor \frac{s_0}{\Delta} \right\rfloor + 0.25 + 0.5\,b\right)\Delta,$$

то есть для b = 0 остаток после деления на Δ тяготеет к 0.25Δ, а для b = 1 — к 0.75Δ. При декодировании бит восстанавливается тестом порога по остатку:

$$\hat{b} = \mathbf{1}\left[(s_0 \bmod \Delta) > 0.5\Delta\right].$$

Широкая разделительная полоса 0.5Δ обеспечивает помехоустойчивое бинарное решение.

2. Процедура метода

2.1. Предобработка и маска

Изображение подрезается до размеров, кратных 4, чтобы корректно разложить LL_1 на блоки 4×4. Бинарная маска (если задана) масштабируется к размеру LL_1 методом ближайшего соседа и использует порог по среднему значению блока (> 0.5) для включения/исключения блока из обработки. Это позволяет локализовать модификации в менее заметных (текстурных) областях.

2.2. Встраивание и извлечение: идеи агрегирования

Каждый блок LL_1 , прошедший маску, несёт один локальный вклад в восстановление очередного бита. Нумерованные блоки циклически «закрепляются» за битами сообщения по индексу n mod L (где LL — длина метки). На этапе извлечения локальные решения агрегируются (усреднение/большинство) по группам, что повышает итоговую надёжность.

3. Метрики оценки и интерпретация

Для количественной проверки применяются:

- PSNR (дБ) — измеряет незаметность посредством отношения пиковой мощности сигнала к мощности ошибки между исходным изображением и с меткой; значения $\geq$ 30 обычно соответствуют хорошему визуальному качеству.
- Bit Accuracy (%) — доля корректно восстановленных битов по сравнению с исходной меткой; близость к 100% свидетельствует о высокой робастности в рассматриваемых условиях.

4. Анализ проектных решений

Почему LL_1 . Эта компонента энергетически стабильна, что положительно сказывается на стойкости к компрессии и сглаживанию. Потенциальное влияние на видимое качество компенсируется маской, исключающей однородные области.

Роль mid-band и блока 4 × 4. Работа в средних частотах уменьшает как визуальные искажения (не затрагиваем низкие частоты), так и риск стирания при JPEG (не уходим в самый высокий диапазон). Малый размер блока снижает вычислительную сложность и обеспечивает стабильность SVD.

SVD + QIM. Наибольшее сингулярное значение аккумулирует существенную часть энергии и более стабильно к возмущениям; двудольное размещение остатков (окна 0.25Δ и 0.75Δ) с разделителем 0.5Δ повышает надёжность двоичного решения при шуме.

Агрегирование по блокам. Циклическое сопоставление блоков битам сообщения создаёт множество независимых «голосов» для каждого бита; последующая агрегация существенно снижает вероятность ошибки.

5. Параметры и практические рекомендации

- **Шаг квантования Δ**: увеличение Δ улучшает декодирование в шуме (robustness), снижая при этом PSNR; уменьшение — наоборот. На практике целесообразно подбирать Δ в диапазоне, обеспечивающем PSNR ≥ 30 при требуемой точности.
- **Mid-band [0.30, 0.70]**: разумный выбор для блока 4 × 4; при других размерах блока границы можно адаптировать, чтобы учесть особенности целевых искажений.

- **Маска**: полезно строить по картам текстур/краёв (например, Sobel/LoG или saliency), чтобы ограничить модификации перцептуально «дешёвыми» зонами.
- **Длина метки LL**: при фиксированном числе валидных блоков меньшее LL даёт больше наблюдений на бит и, как следствие, лучшую итоговую точность.

Представленная схема **DWT–DCT–SVD** реализует устойчивое и перцептуально щадящее встраивание: DWT выбирает стабильную область LL_1 , блочное DCT с mid-band минимизирует видимые артефакты и потери при сжатии, а связка **SVD+QIM** предоставляет чёткую бинарную решающую процедуру с хорошей помехоустойчивостью. В совокупности с маскированием и агрегированием по блокам метод демонстрирует перспективность для задач защиты прав и аутентификации в реалистичных сценариях обработки изображений.

Алгоритм LSB (Least Significant Bit)

Алгоритмы LSB (*Least Significant Bit*) внедряют двоечную метку в младшие разряды значений пикселей (или коэффициентов в частотной области). Цель — достичь незаметности для наблюдателя при высокой ёмкости (payload). Ограничение подхода: низкая робастность к сильным преобразованиям (сжатие, фильтрация, геометрия). Поэтому LSB целесообразен для задач скрытия данных/лёгкого водяного знака в контролируемой среде, либо как подсистема в гибридных схемах.

1. Модель и обозначения

- Изображение в оттенках серого: $X \in \{0,\ldots,255\}^{H \times W}$. Для цветных изображений рассматриваются каналы R,G,B.
- Сообщение (метка): $m = (m_1,\ldots,m_L)$, $m_i \in \{ 0, 1 \}$.
- Скорость внедрения r (бит/пиксель или бит/канал/пиксель).
- Битовые плоскости: от 0 (LSB) до 7 (MSB) для 8-битного пикселя.
- Канал искажений $T(\cdot)$: сжатие JPEG, шум, размытие, ресэмплинг и т.д.
- Метрики: PSNR/SSIM (качество/незаметность), BER/Accuracy (точность извлечения).

2. Принцип LSB

2.1. LSB Substitution (прямая подстановка)

Идея: присвоить младшему биту пикселя требуемое значение. Если LSB уже равен нужному — пиксель не меняется; иначе изменяется на ± 1.

Плюсы: крайне простая и быстрая реализация, высокая ёмкость (до ~1 bpp для серого и ~3 bpp для RGB при 1 LSB/канал).

Минусы: характерные статистические следы (нарушение парности 2k , 2k+1) — уязвимость к χ^2-тестам, RS-анализу.

2.2. LSB Matching (встраивание ± 1)

Если LSB не совпадает с битом сообщения, пиксель случайно увеличивается или уменьшается на 1.

Плюсы: лучше сохраняет распределение пар (2k, 2k+1), сложнее обнаружить, чем Substitution.

Минусы: робастность не растёт существенно — по-прежнему чувствителен к сжатию/фильтрации.

2.3. Matrix Encoding и адаптивные схемы

- Matrix Encoding (например, Хэмминг (7,4)) уменьшает среднее число изменений на полезный бит ⇒ выше PSNR при той же полезной нагрузке.
- Content-adaptive (по текстуре/краям): встраивание преимущественно в текстурные области, что повышает незаметность и устойчивость.

3. Ёмкость, искажения и незаметность

3.1. Ёмкость

- Серое изображение, 1 LSB: максимум ≈ H × W.
- RGB, 1 LSB/канал: максимум ≈ 3HW бит.
- Использование k > 1 младших битовых плоскостей повышает ёмкость до k bpp/канал, но резко ухудшает качество и устойчивость.

3.2. Искажения и PSNR (оценка)

Для 1-LSB-Substitution при скорости r bpp вероятность изменения пикселя ≈ r / 2. Тогда:

$$\mathrm{MSE} \approx \frac{r}{2}, \qquad \mathrm{PSNR} \approx 10 \log_{10}\left(\frac{255^2}{r/2}\right).$$

Пример: r = 1 bpp ⇒ PSNR ≈ 51 дБ, визуально практически незаметно. При k > 1 (несколько LSB) возможная амплитуда изменения до 2^k - 1, MSE растёт, PSNR падает значительно.

4. Устойчивость к преобразованиям

- **JPEG/размытие:** LSB в пространственной области очень чувствителен — агрессивное сжатие легко разрушает метку.
- **Добавочный шум/лёгкая фотокоррекция:** переносится ограниченно; устойчивость повышают повторение битов и голосование.

- **Геометрия** (кроп, поворот, масштаб): возникает рассинхронизация позиций, извлечение затруднено.
- **Выбор канала и плоскости:** в RGB канал B обычно менее заметен, чем R/G; плоскость 0-я (LSB) надёжна по незаметности, но слабее по устойчивости; 1-я плоскость может немного повысить устойчивость ценой заметности.

LSB — это не «жёсткий» робаст-водяной знак в строгом смысле; он подходит для высокой ёмкости при мягких преобразованиях. Для реальной устойчивости нужен переход к частотным или гибридным методам и/или ECC.

5. Детектирование (стегоанализ) и меры снижения риска

5.1. Инструменты стегоанализа

χ^2-тест, RS-анализ, Sample Pairs, признаки в остаточной области, марковские модели и др. особенно эффективны при большой нагрузке или последовательном (неадаптивном) встраивании.

5.2. Как снизить детектируемость

- Уменьшать скорость внедрения rr.
- Случайно распределять позиции с секретным ключом (PRNG).
- Подготавливать сообщение: сжимать и шифровать (равномернее распределение бит).
- Применять Matrix Encoding для уменьшения числа изменений.
- Использовать адаптивные маски (края/текстуры).
- Избегать насыщенных пикселей (0/255) в LSB Matching.

6. Проектирование системы

- **Подготовка сообщения:** сжатие + шифрование + при необходимости **ECC** (Хэмминг/BCH/LDPC).
- **Выбор области внедрения:** пространство (LSB) — для высокой ёмкости и незаметности; при требованиях устойчивости — частотная область или гибрид.

- **Выбор каналов/бит-плоскостей** и **адаптивной маски** (по краям/текстурам/салиентности).
- **План позиций по ключу** (PRNG) для безопасности.
- **Встраивание:** Substitution / Matching / Matrix Encoding при контроле нагрузки rr.
- **Извлечение:** синхронизация позиций, чтение битов, голосование/декодирование ECC, проверка целостности.
- **Оценка: PSNR/SSIM** (качество), **BER/Accuracy** (надёжность), базовые тесты стегоанализа (детектируемость).

7. Сильные и слабые стороны

Преимущества

- Крайняя простота и скорость, высокая ёмкость (особенно в RGB).
- Высокая незаметность при умеренной нагрузке (часто PSNR > 50 дБ).

Ограничения

- Низкая устойчивость к JPEG/размытию/геометрии.
- Детектируемость при больших нагрузках или неадаптивном размещении.
- При увеличении числа LSB качество быстро ухудшается.

LSB — базовый и практичный инструмент для скрытия данных и «лёгкого» водяного знака: он обеспечивает высокую ёмкость и отличную незаметность при низкой вычислительной цене. Однако из-за ограниченной устойчивости и детектируемости при повышенной нагрузке LSB требует осмотрительной настройки (малая скорость, случайные позиции по ключу, адаптивные маски, Matrix Encoding/ECC). Для задач, где критична реальная робастность, LSB следует рассматривать как подсистему в составе гибридной архитектуры, а не как самостоятельное решение.