УДК 004

СОВРЕМЕННЫЕ МЕТОДЫ И АЛГОРИТМЫ ШИФРОВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ИЗОБРАЖЕНИЯХ: ОБЗОР ТЕХНОЛОГИЙ И ПРОГРАММНЫХ РЕШЕНИЙ

Конспаев М.А.,
магистрант, Казахский университет технологий и бизнеса имени К. Кулажанова, г. Астана, Республика Казахстан

Муханова А.А.,
доктор PhD , Казахский университет технологий и бизнеса имени К. Кулажанова, г. Астана, Республика Казахстан

В статье представлен обзор современных методов и алгоритмов шифрования цифровых водяных знаков в изображениях. Рассматриваются основные типы водяных знаков, методы их внедрения (DCT, DWT, SVD, LSB, гибридные подходы), а также криптографические методы защиты (AES, RSA, хаотические шифры, стеганография). Описываются программные платформы, области практического применения и метрики оценки (PSNR, NC, BER). Особое внимание уделено современным трендам — использованию нейросетей, генеративных моделей и квантовой криптографии.

Ключевые слова: Цифровой водяной знак, шифрование, защита изображений, DCT, DWT, криптография, стеганография, GAN, квантовая безопасность

В современную цифровую эпоху защита визуального контента приобретает всё большую значимость, особенно в связи с широким распространением цифровых изображений и мультимедийной информации в интернете. Одним из ключевых направлений обеспечения безопасности изображений является внедрение цифровых водяных знаков (digital watermarking), которые позволяют подтвердить авторство, защитить авторские права, а также обеспечить аутентичность и целостность данных. Основной задачей внедрения цифрового водяного знака является незаметное встраивание уникальной информации в изображение таким образом, чтобы сохранить его визуальное качество и обеспечить устойчивость к различным видам атак и искажений. Целью данной обзорной статьи является анализ современных алгоритмов шифрования цифровых водяных знаков, а также оценка существующих программных решений и технологий, применяемых в данной области. В рамках статьи

рассматриваются как теоретические основы watermarking, так и практические аспекты программной реализации методов защиты изображений.

Цифровой водяной знак представляет собой специальную информацию, встроенную в носитель (изображение), которая может быть извлечена или обнаружена при необходимости. Существуют различные типы водяных знаков, в зависимости от их видимости и устойчивости. Видимые водяные знаки открыто размещаются на изображении и сразу различимы, в то время как невидимые встроены таким образом, чтобы быть незаметными для человеческого глаза. Устойчивые водяные знаки сохраняются при различных видах атак или обработке изображения, тогда как хрупкие предназначены для обнаружения даже минимальных изменений. Также выделяют спонтанные водяные знаки, встроенные при генерации изображения, и запрашиваемые, применяемые при передаче или обмене контентом [1]. Эффективная система водяных знаков должна удовлетворять ряду требований: незаметность — встроенный знак не должен искажать визуальное восприятие изображения; устойчивость — водяной знак должен сохраняться при различных воздействиях, таких как сжатие, обрезка, фильтрация; емкость — система должна позволять внедрение достаточного объема информации; безопасность — встроенные данные должны быть защищены от несанкционированного извлечения и подделки.

Существует множество алгоритмов внедрения водяных знаков, которые можно классифицировать по способу обработки изображений. Пространственные методы основываются на модификации пиксельных значений, самый известный из которых — метод наименее значимых битов (LSB), когда информация внедряется в младшие биты пикселей. Несмотря на простоту, такие методы подвержены различным атакам и не обеспечивают должной устойчивости. Частотные методы работают в преобразованных областях изображения. К числу таких методов относятся дискретное косинусное преобразование (DCT), которое применяется, например, в алгоритмах сжатия JPEG; дискретное вейвлет-преобразование (DWT), позволяющее более локально контролировать изменения; и сингулярное разложение матриц (SVD), обладающее высокой устойчивостью к различным воздействиям. Кроме того, широкое применение находят гибридные методы, которые комбинируют преимущества различных подходов, например, DWT-DCT или DWT-SVD. Эффективность методов внедрения оценивается с использованием количественных метрик, таких как PSNR (отношение сигнал/шум), NC (нормализованная корреляция) и BER (битовая ошибка при извлечении водяного знака), что позволяет объективно сравнивать алгоритмы по критериям качества, устойчивости и точности [2].

1-таблица. Методы шифрования водяных знаков

Метод	Описание	Преимущества	Недостатки	Примеры применения
AES (Advanced Encryption Standard)	Симметричный блочный алгоритм шифрования, широко применяемый в безопасности	Высокая скорость, надёжная стойкость	Требуется безопасная передача ключа	Защита авторских прав в цифровых галереях
RSA (Rivest–Shamir–Adleman)	Асимметричный алгоритм шифрования с использованием открытого/закрытого ключей	Повышенная безопасность, удобство распределения ключей	Медленнее, ресурсоёмкий при больших объёмах	Секретное встраивание в юридические документы
Хаотические шифры	Используют свойства хаоса (чувствительность к начальному состоянию) для шифрования	Высокая непредсказуемость, простая реализация	Сложность восстановления при ошибке, чувствительность к шуму	Защита изображений в биомедицинских приложениях
Стеганография	Метод сокрытия информации в изображении, не меняя видимого содержания	Высокая незаметность, сочетается с другими методами	Уязвимость при сжатии и атаке	Тайная передача авторской информации
Биометрическая криптография	Использует биометрические данные (отпечатки пальцев, лицо и т.д.) для шифрования	Связь с личностью, высокая защита от подделок	Требует дополнительных сенсоров и точности	Авторизация владельца авторских прав

Разработка и внедрение систем шифрования водяных знаков в изображениях невозможны без использования специализированных программных платформ и средств. Одними из наиболее распространённых сред разработки в данной области являются MATLAB, Python, C/C++ и Java. MATLAB предоставляет мощный набор инструментов для обработки сигналов и изображений, включая встроенные функции для трансформирования, анализа и внедрения водяных знаков. Он широко используется в научных исследованиях благодаря простоте моделирования и визуализации. Python, в свою очередь, предлагает открытые библиотеки, такие как OpenCV, NumPy, SciPy и PyWavelets, позволяющие создавать гибкие и масштабируемые watermark-системы. Благодаря своей читаемости и поддержке со стороны сообщества, Python становится всё более популярным выбором для прототипирования и реализации алгоритмов [3]. Языки низкого уровня, такие

как C/C++, обеспечивают высокую производительность, что особенно важно для встраиваемых систем и обработки больших объёмов данных в реальном времени. Java используется преимущественно в кроссплатформенных решениях и встраиваемых приложениях. В дополнение к языкам программирования, существует множество готовых библиотек и модулей, предназначенных для шифрования, трансформации изображений и оценки устойчивости водяных знаков. Также разрабатываются удобные пользовательские интерфейсы, которые позволяют внедрять watermark-алгоритмы без глубоких знаний программирования.

Применение цифровых водяных знаков охватывает широкий спектр задач и отраслей. Одним из наиболее значимых направлений является защита авторских прав — внедрение уникального знака в изображение позволяет идентифицировать правообладателя и предотвращать незаконное распространение контента. Кроме того, watermarking активно используется для проверки подлинности изображений, что важно при передаче критически важных визуальных данных, таких как судебные материалы, документы и свидетельства. Новым направлением является интеграция цифровых водяных знаков в блокчейн-системы, где они служат для подтверждения неизменности и авторства изображений, обеспечивая дополнительный уровень децентрализованной безопасности. В медицинских системах водяные знаки помогают обеспечивать целостность снимков, таких как рентген или МРТ, в условиях хранения и передачи. Аналогичным образом watermarking применяется для защиты спутниковых снимков, научных иллюстраций и произведений искусства от подделок и незаконного копирования.

Сравнительный анализ алгоритмов шифрования водяных знаков проводится по множеству метрик, таких как устойчивость к искажениям, точность извлечения, скорость обработки и ресурсоёмкость. Устойчивость определяется способностью алгоритма сохранять встроенную информацию после применения атак, таких как сжатие JPEG, обрезка, добавление шума или поворот изображения. Точность измеряется через показатели извлечения, включая нормализованную корреляцию (NC) и битовую ошибку (BER). Скорость алгоритма особенно важна при внедрении в реальном времени или в мобильных устройствах. Ресурсоёмкость характеризует требования к памяти и вычислительным ресурсам [4]. Для объективной оценки алгоритмов используются таблицы и диаграммы производительности, которые позволяют наглядно сравнивать подходы по различным критериям. Также особое внимание уделяется уязвимостям: несмотря на высокие теоретические характеристики, некоторые алгоритмы подвержены атакам, направленным на уничтожение или подмену водяного знака. Таким образом, тщательная оценка методов необходима для выбора оптимального решения в зависимости от конкретной области применения.

Современные исследования в области шифрования цифровых водяных знаков демонстрируют активное внедрение технологий искусственного интеллекта и нейросетей. Глубокие нейронные сети используются как для оптимизации процесса внедрения водяных знаков, так и для их извлечения, позволяя значительно повысить устойчивость и незаметность встроенной информации. Одной из перспективных технологий является применение генеративных состязательных сетей (GAN), которые могут создавать изображения с уже встроенными незаметными водяными знаками или же обнаруживать фальсификации путём сравнения оригинала и копии. Кроме того, значительное внимание уделяется разработке методов watermarking для видео и трёхмерной графики, что обусловлено ростом объёмов визуального контента в мультимедийных приложениях, виртуальной и дополненной реальности. В этих условиях необходимо учитывать не только пространственные, но и временные и геометрические параметры. Параллельно с этим в научном сообществе рассматриваются возможности использования квантовой криптографии и вычислений в watermarking-системах будущего. Квантовые алгоритмы обещают значительно повысить безопасность и устойчивость к атакам благодаря физическим принципам, лежащим в основе их функционирования [5].

Несмотря на достигнутый прогресс, область цифровых водяных знаков сталкивается с рядом серьёзных вызовов. Одной из ключевых проблем является компромисс между незаметностью встроенного знака и его устойчивостью: повышение одного из этих параметров нередко приводит к ухудшению другого. Решение этой дилеммы требует продвинутых адаптивных алгоритмов, учитывающих контекст изображения и предполагаемые угрозы. Другой важной задачей является реализация обратимой защиты, при которой возможно не только извлечение водяного знака, но и восстановление изображения в исходном виде без потерь. Это особенно актуально в медицине и криминалистике, где искажения недопустимы [6]. Ещё одной проблемой остаётся масштабируемость и стандартизация решений: несмотря на разнообразие методов, отсутствуют общепринятые стандарты, что затрудняет совместимость между системами и их интеграцию в существующую инфраструктуру. Кроме того, алгоритмы водяных знаков должны быть устойчивыми к широкому спектру атак, включая удаление, замену, геометрические трансформации, сжатие, фильтрацию и шумовое искажение. Учитывая постоянно развивающиеся методы взлома, системы watermarking нуждаются в постоянном усовершенствовании.

В заключение можно отметить, что технологии шифрования водяных знаков в изображениях представляют собой важное и активно развивающееся направление цифровой безопасности. Современные методы, основанные на частотных преобразованиях, криптографии и гибридных подходах,

обеспечивают высокий уровень защиты визуальной информации. В статье были рассмотрены основные алгоритмы, программные средства, области применения, а также метрики оценки эффективности. Особое внимание уделено тенденциям, связанным с применением искусственного интеллекта и квантовых технологий. Для дальнейшего развития области рекомендуется сосредоточиться на создании стандартизированных и обратимых систем, обладающих высокой адаптивностью к различным условиям и устойчивостью к новым видам атак. Кроме того, необходима разработка удобных и универсальных программных решений, обеспечивающих интеграцию watermarking-технологий в широкую сферу приложений, от медицины и юриспруденции до цифровых медиа и метавселенных.

Список использованной литературы

1. Shedole S. M., Santhi V. Hybrid deep learning based digital image watermarking using GAN-LSTM and adaptive gannet optimization techniques // Multimedia Tools and Applications. – 2024. – Vol. 83. – No. 5. – P. 5873–5895.

2. Wang B., Su Y., Gao M., Lyu H., Zhang J., Zhou B. Color image encryption based on finger vein key and off-axis digital holography with phase-modulated reference light // Scientific Reports. – 2025. – Vol. 15. – No. 1. – P. 1542–1556.

3. Hoshi A. R., Zainal N., Fadhil M. Digital watermarking: Innovations and challenges in copyright protection // AIP Conference Proceedings. – 2024. – Vol. 3232. – No. 1. – P. 020023-1–020023-7.

4. Elbasi E., Topcu A. E., Alzoubi Y. Robust and Secure Watermarking Algorithm Based on High Frequencies of Integer Wavelet Transform // IEEE International Conference on Image Processing and Signal Processing (ICIPSP). – 2024. – P. 112–118.

5. Roy S., Chakraborty B. Watermarking: Characteristics, Methods, and Evaluation // Next-Generation Systems and Secure Communications / Ed. A. Sharma. – Wiley. – 2025. – Chapter 2. – P. 35–59.

6. Zhao G. Blockchain and Web3.0 Technology Innovation and Application: First Conference, BWTAC 2024, Guangzhou, China, November 6–8, 2024, Proceedings. – Springer. – 2024. – P. 221–233.

СУРЕТТЕГІ ЦИФРЛЫҚ СУ ТАҢБАЛАРЫН ШИФРЛАУДЫҢ ЗАМАНАУИ ӘДІСТЕРІ МЕН АЛГОРИТМДЕРІ: ТЕХНОЛОГИЯЛАР МЕН БАҒДАРЛАМАЛЫҚ ШЕШІМДЕРГЕ ШОЛУ

Конспаев М.А.*, *Муханова А.А.

Бұл мақалада сандық бейнелерге арналған сутаңбаларды енгізу мен шифрлау саласындағы заманауи әдістер мен алгоритмдерге шолу жасалады. Цифрлық сутаңбалардың негізгі түрлері, ендіру тәсілдері (DCT, DWT, SVD, LSB және гибридті модельдер), сондай-ақ криптографиялық шифрлау (AES,

RSA, хаостық жүйелер, стеганография) қарастырылады. Программалық құралдар мен платформалар, нақты қолдану салалары және бағалау метрикалары (PSNR, NC, BER) да сипатталады. Сонымен қатар, нейрожелілер, GAN, кванттық криптография сияқты жаңа зерттеу бағыттары талданады.

Кілт сөздері: Сандық сутаңба, шифрлау, бейне қорғау, DCT, DWT, криптография, стеганография, GAN, кванттық қауіпсіздік.

MODERN METHODS AND ALGORITHMS FOR ENCRYPTING DIGITAL WATERMARKS IN IMAGES: AN OVERVIEW OF TECHNOLOGIES AND SOFTWARE SOLUTIONS

Конспаев М.А.*, *Муханова А.А.

This article provides a comprehensive review of modern methods and algorithms for encrypting digital watermarks in images. It covers key types of watermarks, embedding techniques (DCT, DWT, SVD, LSB, and hybrid models), and cryptographic approaches (AES, RSA, chaotic maps, steganography). The paper discusses software platforms, practical application areas, and evaluation metrics (PSNR, NC, BER). Special focus is given to emerging research trends, including neural networks, GANs, and quantum cryptography..

Keywords: Digital watermark, encryption, image protection, DCT, DWT, cryptography, steganography, GAN, quantum security.