РАЗРАБОТКА АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЗАЩИТЫ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ ТОРГОВЫХ ПЛОЩАДОК

***А.Н. Земцов**, к.т.н., доцент, Волгоградский государственный технический университет, azemtsow@mail.ru;*
***М.А. Кузнецов**, к.т.н., доцент, Волгоградский государственный технический университет, 35km@mail.ru;*
***Д.А. Редняков,** Волгоградский государственный технический университет;*
***Д.А. Амелин**, Волгоградский государственный технический университет.*

УДК 004.056.55

Аннотация. В статье рассматривается задача защиты изображений товаров, размещаемых на электронных торговых площадках. Проблема несанкционированного копирования и повторного использования изображений различными продавцами приводит к нарушению авторских прав, подрыву доверия покупателей и демпингу добросовестных участников рынка. Предлагается архитектура информационной системы, обеспечивающей защиту изображений на основе комбинирования стеганографических и криптографических методов. Для реализации предложенного подхода использованы библиотеки *OpenCV* и *Qt*, а также методы выделения контуров и дискретных спектральных преобразований. Реализация рассчитана на интеграцию с мобильной версией и веб-версией маркетплейса. Проведено сравнение эффективности алгоритмов для задач сокрытия и верификации водяных знаков.

Ключевые слова: защита информации; авторское право; дискретное косинусное преобразование; маркетплейс; электронная коммерция; стеганография; скрытие данных; цифровой водяной знак.

DEVELOPMENT OF THE ARCHITECTURE OF AN INFORMATION SYSTEM FOR PROTECTING GRAPHIC INFORMATION OF TRADING PLATFORMS

***A.N. Zemtsov**, Ph.D. of Engineering Sciences, Associate Professor, Volgograd State Technical University;*
***M.A. Kuznetsov**, Ph.D. of Engineering Sciences, Associate Professor, Volgograd State Technical University;*
***D.A. Rednyakov**, Volgograd State Technical University;*
***D.A. Amelin**, Volgograd State Technical University.*

Annotation. This article examines the problem of protecting product images posted on e-commerce platforms. Unauthorized copying and reuse of images by various sellers leads to copyright infringement, the undermining of consumer trust, and the dumping of bona fide market participants. An architecture for an information system providing image protection based on a combination of steganographic and cryptographic methods is proposed. The proposed approach utilizes the OpenCV and Qt libraries, as well as edge detection and discrete spectral transform methods. The implementation is designed for integration with the mobile and web versions of the marketplace. The effectiveness of the algorithms for watermark concealment and verification is compared.

Keywords: information security; copyright; discrete cosine transform; marketplace; e-commerce; steganography; data hiding; digital watermark.

Введение

В последние годы сфера электронной коммерции переживает интенсивное развитие. Маркетплейсы позволяют тысячам продавцов размещать свои предложения в одном каталоге, используя для наглядности графические материалы: фотографии товаров и их составляющих, изображения упаковки, дополненные основной информацией о товаре. Графический контент является важнейшим компонентом восприятия товара, т.к. формирует первичное впечатление покупателя о товаре, влияет на решение о его покупке и снижает риск его возврата.

Однако открытость и масштабность современных торговых площадок создают серьезную проблему: несанкционированное использование изображений товаров другими продавцами с целью предложения аналогичных или схожих товаров. Другими словами, недобросовестный продавец может просто скопировать фотографии товара из магазина другого продавца и загрузить ее под своим лотом, при этом минимизируя затраты на создание цифровой копии товара, когда не требуется проведение специальной фотосессии экспертом-фотографом, а также обработка полученных изображений, и продвигать товар с заимствованными изображениями как собственный. Подобная деятельность влечет за собой нарушение права на интеллектуальную собственность продавцов, которые создали графический контент [1]. Кроме того, покупатель приобретает товар по набору изображений, таким образом сопоставляя его со своими ожиданиями. В случае, когда изображения были заимствованы и товар отличается по качеству или комплектности, возникает недовольство, возврат и, как следствие, снижение доверия не только к торговой площадке, но и к оригинальному товару, а также его производителю. В результате торговая площадка получает репутационные и юридические риски, т.к. наличие заимствований в фотоматериалах снижает ценность бренда, увеличивает нагрузку на модерацию, а также может привести к правовым претензиям.

Методы защиты графического контента на существующих торговых площадках недостаточны и плохо интегрированы. Видимые водяные знаки могут снижать эстетическую привлекательность изображения и могут быть легко удалены с помощью современных инструментов редактирования или машинного обучения [2]. Скрытые водяные знаки в информационных системах на существующих торговых площадках не применяются. Необходимо отметить сложность интеграции в архитектуру маркетплейса подобных решений с учетом основных требований: высокой производительности, масштабируемости, совместимости с *API* мобильных клиентов и веб-версиями торговой площадки, интеграции с модерацией и аналитикой. Кроме того, продавцы могут применять множество техник обработки изображений с целью обойти защиту: обрезка изображения, сжатие, изменение яркости или контраста, поворот, зеркальное отражение. Исследования в этой области не затрагивают специфику функционирования торговой площадки, заключающуюся в множественности товаров, быстроте обновления и разнообразии реализаций.

В настоящей работе предпринимается попытка разработать архитектуру информационной системы, способной защищать изображения товаров торговой площадки от повторного несанкционированного использования. Подобные системы должны удовлетворять ряду требований: иметь устойчивость к типичным операциям обработки изображений, оказывать минимальное влияние на визуальное качество изображения с целью не допустить ухудшения удовлетворенности покупателя, обеспечить интеграцию с инфраструктурой

маркетплейса, автоматическую модерацию, обнаружение фактов копирования и повторного использования изображений.

Существующие решения

Рассмотрим несколько существующих систем, использующихся для сокрытия передаваемого сообщения в различных форматах, например, аудио или изображение. Ряд систем используют элементарные алгоритмы сокрытия, которые сложно назвать стеганографическими. В связи с этим для сравнения существующих систем были выделены следующие критерии: формат входного контейнера для встраивания сообщения, тип передаваемого сообщения, использующийся стеганографический алгоритм встраивания сообщения, устойчивость заполненного контейнера к атакам и тип сервиса. Сравнительный анализ существующих систем представлен в табл. 1.

Таблица 1.

Критерий сравнения	*MP3Stego*	*Secret Letter*	*Bmp Packer*	*AppendX*	*Secur Engine*	Разраб. приложение
Формат контейнера	*MP3*	*JPEG, PNG*	*BMP*	*JPEG, PNG*	*Pencil*	*JPEG, PNG*
Тип передаваемого сообщения	Текст	Текст	Текст	Текст	Текст, изображение	Текст, изображение
Использующийся стеганографический алгоритм	НЗБ + *SHA*	НЗБ	*Blowfish, Twofish* и *AES*	Добавление сообщения в конец файла	НЗБ + *SHA*	НЗБ, ДКП, ДВП
Устойчивость к атакам	Нет	Нет	Частично	Нет	Частично	Частично
Тип сервиса	Консольное приложение для *Windows*	Android-приложение	Standalone приложение для *Windows*	Standalone приложение для *UNIX*	Standalone приложение для *Windows*	Кросс-платформенное приложение

Источник: составлено авторами

Консольное приложение *MP3Stego* для *MS Windows* используется для сокрытия текстового сообщения в файл формата *MP3*. С целью подтверждения подлинности перед внедрением вычисляется значение хеш-функции для сообщения с помощью алгоритма безопасного хеширования *SHA*. Внедрение осуществляется с помощью алгоритма наименьшего значащего бита [3, 4]. Заполненный контейнер не обладает устойчивостью к атакам. *Android*-приложение *Secret Letter* для мобильных телефонов и планшетов позволяет внедрить текстовое сообщение в изображения формата *JPEG* и *PNG*. Для внедрения используется алгоритм наименьшего значащего бита без дополнительной криптографической защиты. Заполненный контейнер не обладает устойчивостью к атакам увеличения яркости, поворота или увеличения шума. *Standalone*-приложение для *MS Windows BmpPacker* позволяет внедрить текстовое сообщение в изображения формата *BMP*. При внедрении используется несколько алгоритмов криптографической защиты: *Blowfish*, *Twofish* и *AES*. *Standalone*-приложение для *Unix*-систем *AppendX* позволяет внедрить текстовое сообщения в изображения формата *JPEG* и *PNG*,

используя примитивный алгоритм добавления сообщения без предварительной защиты в конец графического файла. Контейнер на выходе устойчивостью к атакам не обладает. *Standalone*-приложение для *MS Windows SecurEngine* позволяет внедрить текстовое или графическое сообщение в файлы формата *Pencil*-макета. Данное приложение – специализированное, в качестве алгоритма внедрения сообщения используется алгоритм наименьшего значащего бита, а для создания отпечатка сообщения используется алгоритм хеширования *SHA*.

Как видно из табл. 1, самым популярным стеганографическим методом встраивания, реализованным в представленных системах, является метод наименьшего значащего бита. Более продвинутые и надежные системы предварительно осуществляют шифрование передаваемого сообщения для обеспечения более высокого уровня защиты. Устойчивые к атакам стеганографические алгоритмы защиты графической информации встраивают данные сообщения в частотную область изображения [5, 6]. Традиционно используемыми спектральными преобразованиями являются дискретное косинусное преобразование [7, 8], дискретное вейвлет-преобразование [9, 10], дискретное преобразование Фурье [11] или их комбинации, на которых основываются современные гибридные методы защиты [12], в том числе использующие масштабно-инвариантную трансформацию признаков [13] и сингулярное разложение [14].

Разрабатываемая система будет работать с изображениями в качестве передаваемых сообщений и позволит пользователю выбрать контейнер, который будет иметь наименьший коэффициент потери данных при атаках извне.

Разработка архитектуры информационной системы защиты

На начальном этапе разработки информационной системы защиты необходимо сформулировать функциональные требования, которые представим в виде диаграммы в нотации *UML*, показанной на рис. 1.

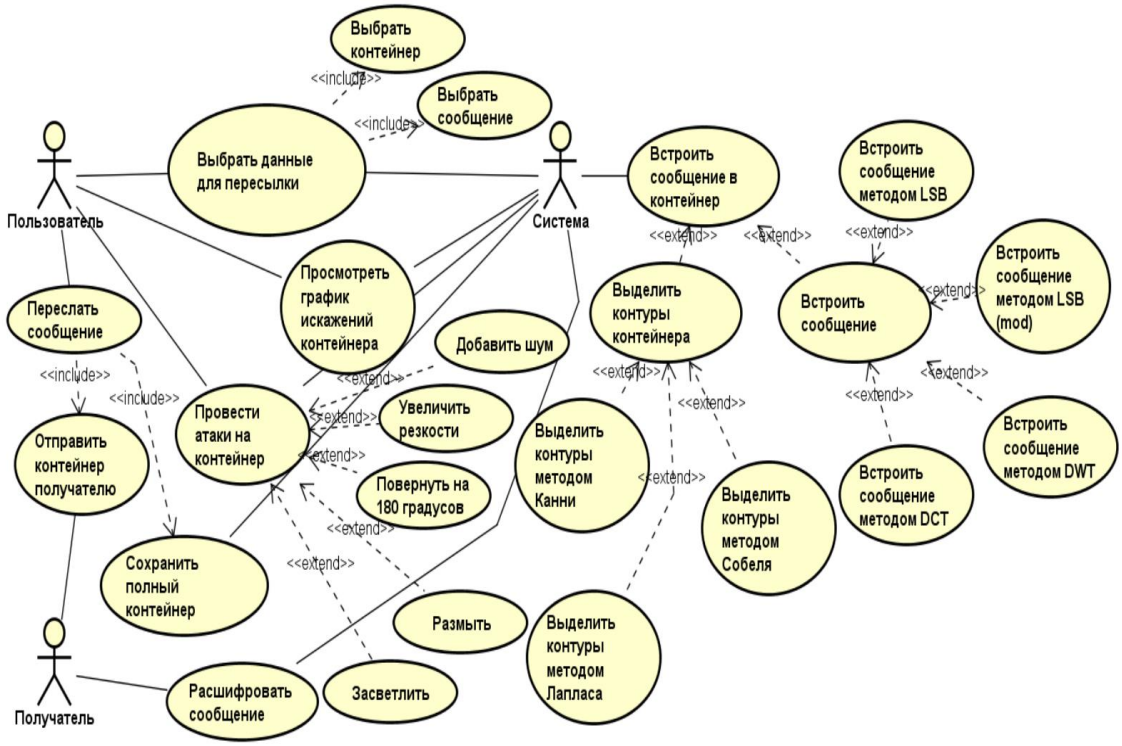


Рисунок 1

Источник: составлено авторами

Система должна обеспечивать возможность выбора графического изображения для размещения его в описании лота и последующей пересылки. Данное действие включает в себя выбор контейнера для пересылки и выбор сообщения. Заполненный контейнер хранится в базе данных описаний лотов. Сообщение должно быть представлено в виде текста или в виде другого изображения. Наиболее популярным форматом для контейнера является формат *JPEG*. В связи с этим в системе необходимо реализовать дискретное косинусное преобразование [15] для кодирования и сжатия изображений. Прямое ортогональное преобразование запишется в следующем виде:

$$d_{uv} = \frac{1}{4} C_u C_v \sum_{i=0}^{7} \sum_{j=0}^{7} I(i,j) \cos\left(\frac{(2j+1)u\pi}{16}\right) \cos\left(\frac{(2i+1)v\pi}{16}\right)$$

где: $C_f = \begin{cases} \frac{1}{\sqrt{2}}, f = 0 \\ 1, f > 0, \text{при } u \geq 0, v \leq 7 \end{cases}$

В результате вычисления дискретного косинусного преобразования получается матрица коэффициентов d_{uv} размером 8×8. Значения частотных коэффициентов убывают от левого верхнего угла матрицы к правому нижнему углу.

Для встраивания используются контуры изображения, для чего необходимо реализовать также алгоритмы выделения контуров.

В ходе разработки информационной системы было принято решение использовать библиотеку для работы с изображениями *OpenCV* и для организации графического интерфейса пользователя библиотеку *Qt*. Диаграмма компонентов в нотации *UML*, отображающая подключенные библиотеки, представлена на рис. 2.

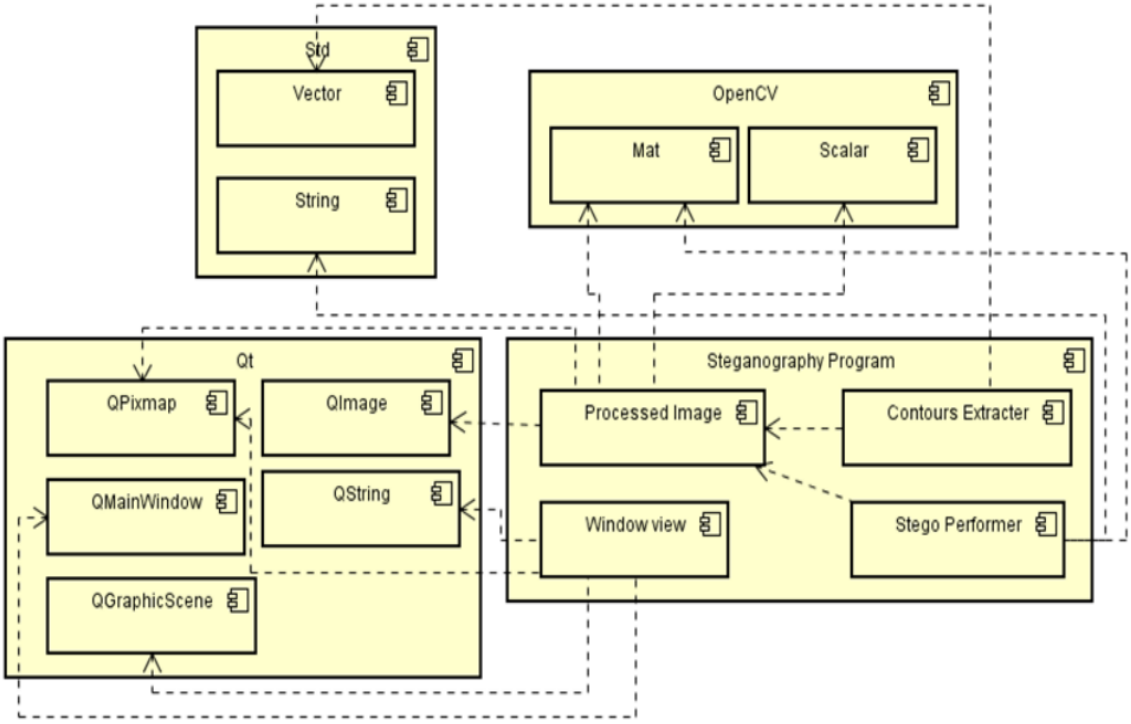


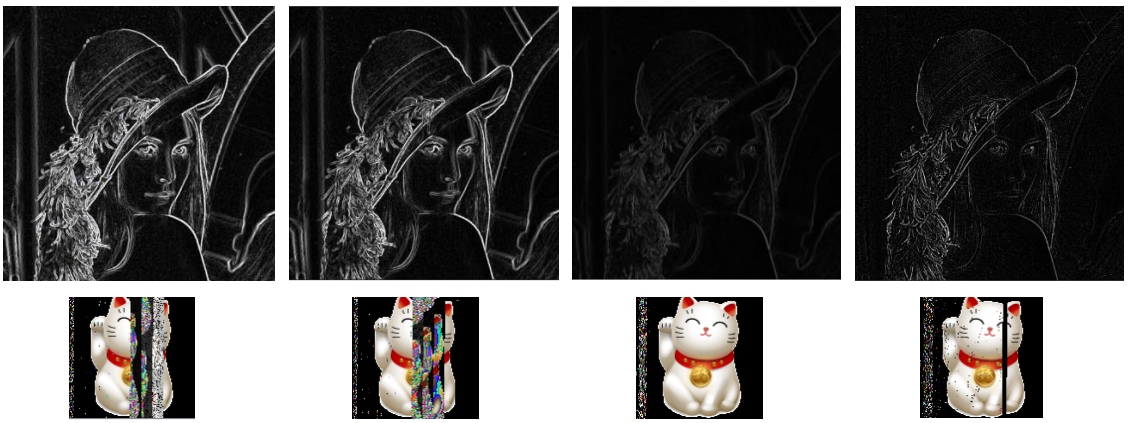
Рисунок 2

Источник: составлено авторами

Разработанная система представлена компонентом *Steganography Program*, в котором выделены главные компоненты: *Processed Image* – компонент для работы с изображениями; *Window View* – компонент для отображения диалоговых окон; *Contours Extractor* – компонент для выделения контуров изображений; *Stego Performer* – компонент для реализации стеганографических алгоритмов. Из библиотеки *OpenCV* были использованы два компонента: *Mat* – компонент, представляющий собой изображение и содержащий методы обработки и изменения изображения, а также компонент *Scalar* для реализации математических функций. Функциональные возможности библиотеки *OpenCV* позволяют реализовать атаки на изображения [16], выделение контуров с помощью операторов Собеля, Прюитта и других, а также реализовать вычисление дискретного косинусного и вейвлет-преобразований. Компонент разрабатываемой системы использует компонент *Mat* для представления изображения, проведения операций по выделению контуров, атаки на контейнеры, а также для отображения гистограмм искажений. Кроме того, компонент *Process Image* использует компонент *Scalar* для вычисления метрик оценки качества: среднего квадратического отклонения и пикового отношения сигнала к шуму. Наряду с *PhoneGap*, *ReactNative*, *Xamarin* [17] библиотека *Qt* широко используется для разработки кроссплатформенного программного обеспечения, в том числе для мобильных устройств [18, 19]. Из библиотеки *Qt* были использованы следующие компоненты: *QPixmap* – компонент для отображения картинки в пользовательском интерфейсе; *QImage* – компонент для работы с изображениями; *QMainWindow* – компонент для отображения диалоговых окон; *QString* – компонент для работы со строками; *QGraphicScene* – компонент для отрисовки изображения на холсте. С помощью компонентов библиотеки *Qt QGraphicScene* и *QPixmap* было реализовано отображение изображений в главном окне информационной системы. Компонент отображения главного окна использует компонент *QMainWindow* для работы с интерфейсом, отрисовки элементов управления, изображений. Компонент *QImage* является промежуточным компонентом для конвертации *QPixmap* в *Mat*, так как класс *QPixmap* не дает возможности обращаться непосредственно к пикселям изображения. Компонент *QString* необходим для получения текстового сообщения из поля ввода, а также отображения полученных в программе результатов. Кроме вышеупомянутых библиотек, система вынуждена использовать стандартную библиотеку контейнеров *Std*, т.к. *OpenCV* использует компоненты данной библиотеки. Для хранения выделенных контуров используется контейнер *Vector*, а для кодирования сообщения в изображение сообщение необходимо привести к типу *String*, что также является стандартным контейнером библиотеки *Std*.

Результаты экспериментов

Для выбора наилучшего алгоритма для сокрытия передаваемого сообщения необходимо произвести сравнение стеганографических алгоритмов. На рис. 3 показаны примеры вычисления значений градиента яркости изображения с помощью различных операторов для исходного изображения и соответствующих извлеченных цифровых водяных знаков.



а) опер. Собеля б) опер. Прюитта в) опер. Робертса г) опер. Лапласа

Рисунок 3

Источник: составлено авторами

С помощью количественных характеристик можно точнее определить качество кодирования передаваемого сообщения. В [20] приводятся основные метрики, с помощью которых можно оценить качество используемого стеганографического алгоритма. Данные метрики широко применяются для сравнительного анализа различных алгоритмов обработки изображений. В качестве первой метрики среднее квадратическое отклонение (СКО), которое используется для измерения усредненной разницы между пустым и заполненным контейнером. Выражение для вычисления среднего квадратического отклонения имеет вид:

$$\text{СКО} = \frac{1}{N_1 N_2} \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} \left(I(i,j) - K(i,j) \right)^2,$$

где: I – исходное изображение-контейнер; K – заполненный контейнер; размеры N_1 и N_2 исходного изображения I указаны в пикселях; j, i – целые числа. В качестве второй метрики выбрано пиковое отношение сигнала к шуму (ПОКС), которое используется для представления качества кодирования сообщения и показывает, насколько достоверно сообщение будет распознано в контейнере. Пиковое отношение сигнала к шуму описывается следующим выражением:

$$\text{ПОКС} = 10 \log_{10} \left(N_1 N_2 \frac{\max\limits_{i,j} I(i,j)^2}{\sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} \left(I(i,j) - K(i,j) \right)^2} \right)$$

В числителе указывается квадрат максимального значения интенсивности пикселя в изображении.

В табл. 2 представлены результаты сравнения работы некоторых стеганографических алгоритмов. Для используемого изображения после встраивания ПОКС получалось в диапазоне от 44,83 до 53,16 дБ, а СКО – от 7,83 до 0,5.

Таблица 2.

Алгоритм	Увеличение яркости	Поворот	Увеличение резкости	Фильтрация
НЗБ	2%, 1,8%	0%, 0%	4,71%, 5,78%	3,2%, 3,33%

Алгоритм	Увеличение яркости	Поворот	Увеличение резкости	Фильтрация
НЗБ-Кэнни	1,8%, 2,3%	0%, 0,9%	4,3%, 2,1%	8,33%, 5,21%
НЗБ-Собель	1,1%, 1,3%	0,3%, 0,2%	1,3%, 1,7%	4,7%, 2,1%
ДКП	100%, 100%	10%, 14%	100%, 100%	15,3%, 16,4%
ДКП-Кэнни	100%, 100%	10,4%, 10,2%	93,4%, 91,7%	8,33%, 6%
ДКП-Собель	100%, 100%	20,5%, 28,4%	100%, 100%	16,7%, 14,9%

Источник: составлено авторами

В результате проведения атак удалось выяснить, что наиболее разрушительное воздействие на контейнер для представленных алгоритмов оказывают поворот и фильтрация. Для алгоритмов на основе метода встраивания в наименьший значащий бит все атаки оказали разрушительное воздействие на извлеченное сообщение, поэтому представляется целесообразным использовать метод встраивания в наименьший значащий бит для алгоритмов выявления факта несанкционированного изменения изображения, т.к. в этом случае встроенный цифровой водяной знак будет разрушаться при любом изменении защищенного изображения. Алгоритмы на основе спектральных преобразований в целом показали устойчивость к изменению яркости и контраста изображения, а также увеличению резкости. При предварительном выделении контуров результат обработки изображений данными алгоритмами несколько улучшался в случае фильтрации и геометрических атак, но процент совпадения сообщений редко превышал значения в 20 процентов. Таким образом, для передачи защищенных данных лучше использовать модификации спектральных алгоритмов на основе операторов, вычисляющих приближенное значение градиента яркости изображения, относительно устойчивые к геометрическим атакам и фильтрации.

Заключение

В рамках проведенного исследования разработана и реализована архитектура информационной системы защиты графической информации, предназначенной для предотвращения несанкционированного копирования изображений товаров на торговых площадках. Предложенная система базируется на интеграции стеганографических и криптографических методов, а также на применении алгоритмов выделения контуров и дискретных спектральных преобразований, что позволило обеспечить баланс между визуальным качеством изображений и степенью защищенности встроенного цифрового водяного знака.

Проведенный сравнительный анализ существующих решений показал, что большинство программных систем, реализующих стеганографические методы, ориентированы на передачу текстовых сообщений и не обладают устойчивостью к типичным атакам на изображения: фильтрации, изменению яркости, масштабированию, повороту. Разработанная система устраняет указанные недостатки за счет внедрения данных в частотную область изображения и использования комбинированных подходов к встраиванию, включая методы предварительного выделения контуров. В отличие от существующих решений, система обеспечивает возможность автоматической генерации и проверки цифровых знаков, что позволяет реализовать функции обнаружения копирования и подтверждения подлинности изображений без участия пользователя.

Реализованный программный прототип демонстрирует устойчивость встроенных водяных знаков к основным типам искажений, возникающим при загрузке изображений на торговые площадки. Экспериментальные результаты подтвердили, что применение алгоритмов дискретного косинусного

преобразования в сочетании с фильтрацией контуров обеспечивает высокие значения ПОКС при минимальных искажениях визуального восприятия. Кроме того, комбинация спектрального преобразования с операторами выделения контуров показала лучшие показатели устойчивости к геометрическим искажениям и фильтрации, что делает данный подход перспективным для использования в системах автоматической модерации торговых площадок.

Полученные результаты подтверждают эффективность и применимость предложенной архитектуры информационной системы для защиты изображений товаров маркетплейсов, что делает ее перспективным инструментом для построения безопасных и прозрачных цифровых торговых экосистем.

Литература

1. Земцов А.Н. Методы цифровой стеганографии для защиты авторских прав: монография. – Saarbrucken: LAP Lambert. 2012. – 148 с.
2. Zhong X., Das A., Alrasheedi F., Tanvir A. A Brief, In-Depth Survey of Deep Learning-Based Image Watermarking // Applied Sciences, 2023. – № 13 (21). – 11852 с.
3. Wang H., Su Q. A color image watermarking method combined QR decomposition and spatial domain // Multimedia Tools and Applications, 2022. V. 81. – pp. 37895-37916.
4. Земцов А.Н., Чан Зунг Хань. Защита графической информации от неправомерного использования маркированием в пространственной области // Современные наукоемкие технологии, 2022. – № 12-2. – С. 211-216.
5. Gupta S., Saluja K., Solanki V., Kaur K., Singla P., Shahid M. Efficient methods for digital image watermarking and information embedding // Measurement: Sensors, 2022. – V. 24. DOI: 10.1016/j.measen.2022.100520.
6. Земцов А.Н., Цыбанов В.Ю. Защита от неправомерного использования графической информации в социальных сетях // Современные наукоемкие технологии, 2020. – № 7. – С. 51-56.
7. Alomoush W. Digital image watermarking using discrete cosine transform // Journal of Cloud Computing, 2023. – № 12 (96). DOI: 10.1186/s13677-023-00468-w.
8. Земцов А.Н., Чан З. Защита графической информации от неправомерного использования маркированием на основе модуляции индекса квантования // Современные наукоемкие технологии, 2023. – № 8. – С. 20-26.
9. Annadurai C., Nelson I., Devi K.N., Manikandan R., Gandomi A.H. Image Watermarking Based Data Hiding by Discrete Wavelet Transform Quantization Model with Convolutional Generative Adversarial Architectures // Applied Sciences, 2023. – V. 13 (2). DOI: 10.3390/app13020804.
10. Земцов А.Н., Аль-Макреби И.М. Об оценке вносимых искажений методом маркирования в низкочастотной области вейвлет-спектра изображения // Инженерный вестник Дона, 2015. – № 2-2 (36). – С. 31.
11. Cedillo-Hernandez M., Cedillo-Hernandez A., Garcia-Ugalde F.J. Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm // Mathematics, 2021. – V. 9 (15). DOI: 10.3390/math9151795.
12. Hasan N., Islam M.S., Chen W., Kabir M.A., Al-Ahmadi S. Encryption Based Image Watermarking Algorithm in 2DWT-DCT Domains // Sensors, 2021. – № 21(16). – 5540 с.
13. Hamidi M., El Haziti M., Cherifi H., Hassouni M. A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection // Journal of Imaging, 2021. – № 7 (10). – С. 218.

14. Shubuh S., Ernawan F., Amrullah A., Wahyu P. Robust Image Watermarking Based on IWT-DCT-SVD for Copyright Protection // Iraqi Journal for Computer Science and Mathematics, 2024. – V. 5 (4). DOI: 10.52866/2788-7421.1201.
15. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика, 2011. – № 4(34). – С. 90-104.
16. Берников В.В., Преображенский А.П., Чопоров О.Н. Возможности распараллеливания обработки изображений с помощью opencv и openmp // Моделирование, оптимизация и информационные технологии, 2019. – Т. 7. – № 2 (25). – С. 110-126.
17. Черников В.Н. Сравнительный анализ архитектур кроссплатформенного программного обеспечения // Вестник Воронежского государственного технического университета, 2018. – Т. 14. – № 5. – С. 47-53.
18. Шабинский Д.Э., Мещеряков Г.А. Разработка ПО под мобильные устройства (в частности, ANDROID). Особенности разработки мобильных приложений // Инновации и инвестиции, 2023. – № 4. – С. 200-203.
19. Коротков А.А., Букунов С.В. Кроссплатформенное приложение для обучения разработке графических пользовательских интерфейсов с помощью библиотеки Qt // Journal of Advanced Research in Technical Science, 2023. – № 35. – С. 65-73.
20. Земцов А.Н. Сравнительный анализ эффективности методов сжатия изображений на основе дискретного косинусного преобразования и фрактального кодирования // Прикладная информатика, 2011. – № 5 (35). – С. 77-84.