

Оригинальная статья

<https://doi.org/10.31429/20785836-17-3-59-63>

АНАЛИЗ МЕТОДОВ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

Пономарев В.Е.*, Завьялов В.А.

ФГБОУ ВО «Кубанский государственный университет»
(Ставропольская ул., д. 149, г. Краснодар, Россия, 350040)

Ссылка для цитирования: Пономарев В.Е., Завьялов В.А. Анализ методов экспертного исследования цифровых изображений. *Юридический вестник Кубанского государственного университета*. 2025;17(3):59–63. <https://doi.org/10.31429/20785836-17-3-59-63>

КОНТАКТНАЯ ИНФОРМАЦИЯ:

Пономарев Виталий Евгеньевич*, старший преподаватель кафедры криминалистики и правовой информатики ФГБОУ ВО «Кубанский государственный университет»

Адрес: Ставропольская ул., д. 149, г. Краснодар, Россия, 350040

Тел.: +7 (918) 682-17-75

E-mail: 9529788272@mail.ru

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Финансирование. Исследование не имело спонсорской поддержки (собственные ресурсы).

Статья поступила в редакцию: 11.08.2025

Статья принята к печати: 10.09.2025

Дата публикации: 29.09.2025

Аннотация: В данной статье авторами поднимается проблема, связанная с судебно-экспертным исследованием цифровых изображений.

Целью статьи является разработка криминалистических рекомендаций исследования цифровых изображений, отображающих современное состояние техники.

Для достижения указанной цели необходимо разрешить следующие *задачи*: дать определение цифровому изображению; изучить действующие методы судебной фототехнической экспертизы; дать определение метаданным и установить их содержание; исследовать признаков подделки цифровых изображений; изучить возможностей компьютерных программ в исследовании цифровых изображений, их адаптация для судебного исследования указанных объектов.

В ходе подготовки настоящего исследования использованы следующие *методы* научного познания: всеобщий диалектический метод познания явлений и процессов. Также применялся комплекс общенаучных (системный, структурно-функциональный, формально-логический, анализа, синтеза, дедукции, индукции, исторический и др.), частнонаучных (социологический, документальный и др.) и частноправовых (формально-юридический, политико-правовой, сравнительно-исторический, правовое моделирование и др.) исследовательских методов.

В настоящее время цифровые изображения все чаще и чаще используются в судебном доказывании, однако, в науке и практике отсутствуют методы, в том числе и экспертные, позволяющие проверить достоверность такого рода источников доказательств. В работе исследованы различные методы изучения цифровых изображений, начиная от их визуального осмотра, заканчивая применением различных программных продуктов, что, на взгляд авторов, может плодотворно использоваться в практике при рассмотрении различных категорий дел, обстоятельства, входящие в предмет доказывания по которым, устанавливаются путем исследования цифровых изображений.

Ключевые слова: криминалистика, судебная экспертиза, технико-криминалистическая экспертиза документов, компьютерно-техническая экспертиза, цифровые изображения, цифровые следы.

Введение

Цифровое изображение – файл, хранящийся в электронном виде на электронном носителе информации. Полученные изображения могут храниться на локальных устройствах, передаваться по

линиям связи, свободно размещаться в сети интернет. При общении между собой люди все чаще пользуются электронными средствами связи: электронной почтой, социальными сетями, мессенджерами. Отправляют и получают с их использованием большой объем визуальной информации – изображений.

Сегодня электронные изображения используются, помимо прочего, в качестве доказательств в судах, что в свою очередь требует изучения существующих приемов и методов, которые могли бы подтвердить подлинность изображения.

Изучалась литература, а также существующие программные средства и иные приемы и методы анализа изображений с целью выявления подлинности изображения.

Для целей нашего исследования подготовлена эмпирическая база, в которую включили различные изображения, с внесенными в них изменениями специальными программными средствами. Полученные изображения таким образом изображения исследованы с использованием различных существующих методик исследования цифровых изображений.

Методы исследования

Всеобщий диалектический метод познания явлений и процессов, общенаучные методы: системный, структурно-функциональный, формально-логический, анализа, синтеза, дедукции, индукции, исторический, частнонаучные методы: социологический, документальный, и частноправовые методы: формально-юридический, политико-правовой, сравнительно-исторический, правовое моделирование.

Результаты исследования

Все из описанные ниже методы исследования имеют свои недостатки. Практически все методы анализа изображений могут быть применены только к его оригиналу. Нельзя применять их к распечатанному и отсканированному первоначальному изображению или к снимку экрана, поскольку они уже не являются исходным изображением и соответственно, не несут значимую информацию. Недостаток любых визуальных методов анализа изображения – субъективный взгляд эксперта.

Фактически при редактировании изображения очень сложно учесть все аспекты. Исходя из этого комплексный анализ изображения, учитывающий источник получения файла изображения, визуальное и не визуальное содержание файла и иные следы позволяет с большой вероятностью установить наличие в изображении признаков подделки.

Научная дискуссия

Существующая практика сложилась таким образом: суды сегодня принимают в качестве доказательств копии документов и изображения, что, однако, создает условия для фальсификации представляемых в суд доказательств [2, с. 69]. Применение электронных доказательств весьма ограничено, суды предпочитают работать с распечатанными изображениями, в лучшем случае, заверенным нотариально [3, с. 283]. Существуют предложения признать распечатанные изображения первоначальными доказательствами. Интерес вызывают предложения использовать автоматические методы при анализе изображений, и использовании электронных образов документов [5, с. 305].

Методы, рассмотренные в данной статье применимы к растровым изображениям в форматах, использующих алгоритмы сжатия с потерей качества. В частности, к наиболее используемому и повсеместно распространенному формату файлов изображений, использующем алгоритмы сжатия с потерей качества – JPEG¹.

Сегодня основным методом фототехнической экспертизы изображений остается визуальная оценка [4, с. 282–288]. Главное правило при визуальном анализе изображений – чем лучше качество, тем большее число признаков подделки возможно выявить на изображении. Поиск визуальных признаков исправления изображения базируется на ограниченности методов исправления фотографий, предлагаемых Adobe Photoshop и аналогичными программами, на невнимательности или низкой квалификации лица, выполнившего редактирование, отличиях в качестве исходного и вставляемого в него изображения.

При исследовании изображения визуальным методом могут использоваться различные приемы, предусмотренные возможностями программ для просмотра и редактирования изображений. Что бы заметить инородные участки изображение увеличивается, каждый фрагмент рассматривается отдельно, изменяются настройки яркости, контрастности, насыщенности изображения до экстремальных значений. Любой из способов редактирования изображения может оставлять признаки, сопутствующие измененному изображению.

¹ GIMP-ELA: плагин Error Level Analysis для GIMP: репозиторий исходного кода [сайт]. Github; 2025 [обновлено 10 сентября 2025; процитировано 10 августа 2025]. Доступно: <https://github.com/sentenza/GIMP-ELA>.

Относительно легко выявляются визуальные артефакты в виде повторяющихся клонированных участков изображения. При невнимательной работе может быть убрана какая-то часть исходного изображения или наоборот видны следы подложки, которые были недостаточно качественно удалены. Это может проявляться в наличии на изображении фрагментов инородного происхождения: пятен или контуров.

Наиболее явно на изображении заметны следы вставки другого изображения: плохо вырезанный контур, отличающийся цвет. Обычно, вставленное изображение смотрится чужеродно по отношению к первоначальному изображению. К данной группе признаков можно отнести нарушения размеров, перспективы, положения, наклона, тени и освещения, источников света изображения, которые также могут быть выявлены визуально при осмотре изображения.

Однако, оценка любого цифрового изображения не ограничивается только визуальными данными. Дополнительно могут быть исследованы многие другие аспекты: метаданные, источник откуда было получено изображение, имя файла, структура и параметры сжатия полученного изображения.

Метаданные – дополнительная информация, добавляемая к изображению, содержащая данные об условиях и способах получения файла, оборудовании с использованием которого было получено изображение, авторство и, даже, координаты места, где было сделано изображение. Существуют различные стандарты сохранения метаданных, такие как EXIF, XMP, IPTC и другие, однако необходимо отметить, что любой из указанных форматов никак не защищен и может быть легко изменен, что лишает метаданные идентификационного значения. Метаданные по сути представляют собой простой текст, в электронной форме и легко могут быть удалены, изменены или скопированы.

Можно выявить не соответствие внутреннего (информация, прикрепленная к файлу и структура файла) и внешнего содержания (информация о изображении, полученная из других источников). Анализ метаданных изображения базируется на поиске несоответствий, ошибок подобного рода. Отсутствие всех метаданных или их части, которая должна присутствовать, может говорить о наличии в изображении несанкционированных изменений или о попытке сокрыть присутствие таких изменений. Однако, это утверждение не всегда справедливо, поскольку, например, пересылка изображения через социальную сеть и повторное сохранение уничтожает метаданные.

В связи с этим важный признак изображения – это источник его происхождения. Данные о источнике позволяют судить о том с использованием какого аппаратно-программного комплекса (цифровая фотокамера или сканер) или программного обеспечения (текст, сохраненный в формате изображения или снимки экрана – скриншоты, результат работы иных программ) было получено или изменено изображение. Программное обеспечение, с помощью которого были внесены изменения и был сохранен файл, например, Adobe Photoshop записывается в метаданных [6, с. 245].

Следы программного редактирования могут остаться в контейнере изображения и они типичны для конкретного программного изображения: названия тегов, заголовки файлов [1, с. 8]. Поэтому, не только запись, сделанная в метаданных, позволяет судить о источнике изображения. При создании изображения камерой или сканером, создании, изменении или сохранении изображения любой программой, в частности при отправке и получении изображения через мессенджер или социальную сеть оно обрабатывается алгоритмом сжатия. При этом каждая социальная сеть или приложение использует свои параметры сжатия при сохранении изображения.

В этом легко убедиться отправив одно и тоже исходное изображение размером 4,19 MB и разрешением 4000x3000 с использованием разных интернет-ресурсов. Для Telegram мы получаем 89,5 KB и разрешение 1280x960, для Vk и WhatsUp получаем разрешение 1600x1200, но разный размер 381 KB и 127 KB соответственно. Это лишь косвенные данные, грубо указывающие на присутствие отличий.

Анализировать изображения вручную достаточно трудоёмкая задача, для более детального изучения существует специальное программное обеспечение: JPEGsnoop¹ – бесплатная утилита, которая извлекает и отображает множество параметров изображения. Анализируя данные, программа создает «подпись сжатия» – совокупность параметров сжатия изображения. У изображений, созданных одним и тем же программным обеспечением, подпись сжатия будет совпадать. Программа содержит базу «подписей сжатия» для многих популярных программ и устройств, которую также можно пополнять.

¹ ImpulseAdventure. JPEGsnoop: репозиторий исходного кода [сайт]. Github; 2025 [обновлено 10 сентября 2025; процитировано 10 августа 2025]. Доступно: <https://github.com/ImpulseAdventure/JPEGsnoop>.

Таким образом, используя данные о структуре полученного файла, по косвенным признакам содержащихся в метаданных, названию файла и его структуре можно определить пересылался ли данный файл с использованием социальных сетей или мессенджеров, сохранялся ли он устройством или программой, а также по данным о параметрах использованного сжатия установить конкретное устройство.

Способ сжатия далеко не единственный признак, существуют и другие косвенные данные. Так, определенные марки цифровых камер или сканеров используют конкретные цветовые модели, которые могут быть изменены при редактировании изображения. Среди иных свойств, позволяющих ассоциировать изображение с конкретным устройством, можно назвать настройки, содержащиеся в устройстве и используемые для формирования изображения – таблицы Хаффмана, размер изображения, таблицы квантования, способ задания метаданных. Таблицы Хаффмана и таблицы квантования задаются для каждого устройства производителями фототехники и их набор характерен для конкретного производителя и модели устройства [7, с. 69–73]. Использование данных таблиц квантования для установления конкретного устройства описано в литературе [8].

Большой интерес представляет использование для анализа цифровых изображений метода, разработанного доктором Нилом Кравец – ELA (Error Level Analysis)¹. Растровое изображение это матрица пикселей, каждому из которых задан свой цвет, имеющий числовое выражение. Поскольку изображение в таком формате занимает много места, то его неудобно и нецелесообразно хранить и передавать в «сыром» виде. Для оптимизации размера изображения используются различные алгоритмы сжатия изображений: сжатие без потерь качества и сжатие, ухудшающее параметры итогового изображения. Сегодня наиболее часто используемый и передаваемый в интернете формат файла изображения с потерей качества – JPEG.

Когда изображение в формате JPEG редактируется и снова сохраняется, оно сжимается заново, теряя часть качества (данных о цвете) при повторном сохранении. Скопированный извне образец изображения создает ситуацию, когда на одном и том же изображении присутствуют участки, которые были сохранены не одинаковое число раз. Например, исходная фотография сохранялась три раза, а вставленный фрагмент всего лишь один раз. Таким образом, оценив уровень ошибок, содержащихся в изображении, можно увидеть слои правок и те изменения, которые были внесены в изображение. Что важно при этом можно определить конкретные фрагменты изображения, которые были подвергнуты редактированию. Для выявления измененного изображения методом ELA используются специальные программные продукты, например, реализованные в виде сайта².

Для выявления изменений изображения можно использовать метод и программные решения для анализа уровня цифрового шума изображений³. Цифровой шум – это случайные изменения яркости или цвета отдельных пикселей изображения [8], обычно появляется в следствии технических недостатков устройств съёмки – сканеров или цифровых фотокамер. Наличие шума свидетельствует о аппаратном происхождении изображения.

Визуально увидеть шум бывает сложно, метод анализа шума базируется на обратном фильтре шумов, который удаляет все части изображения, кроме шума⁴. При редактировании изображения часть шумов теряется, создавая «идеальные» участки изображения, которые после применения фильтра выглядят как темные области. Данный метод позволяет выявить те изменения, которые невозможно заметить с использованием других методов.

Список использованной литературы:

1. Гераськин А.С., Желтов С.Ю. Анализ методов проверки фотоизображений на наличие внесённых изменений. *Информационная безопасность регионов*. 2016;(25(4)):5–10.
2. Казакова А.В. Является ли копия документа доказательством в российском уголовном процессе? *Российское право: образование, практика, наука*. 2021;(4):64–71.
3. Кочеткова Е.А. Об использовании электронных доказательств в гражданском процессе. *Вестник ВГУ. Серия: Право*. 2020;(42(3)):280–283.

¹ JPEG [сайт]. Википедия: свободная энциклопедия; 2025 [обновлено 10 сентября 2025; процитировано 10 августа 2025]. Доступно: <https://ru.wikipedia.org/wiki/JPEG>.

² GIMP-ELA: плагин Error Level Analysis для GIMP: репозиторий исходного кода [сайт]. Github; 2025 [обновлено 10 сентября 2025; процитировано 10 августа 2025]. Доступно: <https://github.com/sentenza/GIMP-ELA>.

³ Noise Analysis: Forensics tools/Photo-forensics [сайт]. 29a.ch; 2025 [обновлено 10 сентября 2025; процитировано 10 августа 2025]. Доступно: <https://29a.ch/photo-forensics/#noise-analysis>.

⁴ Там же.

4. Малюка А.А. Особенности исследования цифровых фотографических изображений как объектов судебной фототехнической экспертизы. *Известия Тульского государственного университета. Экономические и юридические науки*. 2013;(4–2):282–288.
5. Серова А.И., Спивак А.И. Использование методов машинного обучения для определения нарушений целостности JPEG-изображений. *Научно-технический вестник информационных технологий, механики и оптики*. 2018;(2):299–306.
6. Смирнов К.О. Исследование цифровых изображений с помощью Exif-стандарта. *Интерактивная наука*. 2017;(12):243–246.
7. Хатунцев Н.А., Лизоркин А.М. Метод доказывания неизменности фотоизображений в рамках компьютерно-технической экспертизы (на примере из экспертной практики). *Теория и практика судебной экспертизы*. 2014;(35(3)):69–73.
8. Hany Farid. Digital Image Ballistics from JPEG Quantization: A Followup Study. Computer Science Technical Report TR2008-638. Dartmouth; 2008. [сайт]. Digital Commons; 2025 [обновлено 12 января 2008; процитировано 10 августа 2025]. Доступно: https://digitalcommons.dartmouth.edu/cgi/viewcontent.cgi?article=1322&context=cs_tr.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Пономарев Виталий Евгеньевич

старший преподаватель кафедры криминалистики и правовой информатики ФГБОУ ВО «Кубанский государственный университет»

ORCID: 0000-0002-1613-5749

AuthorID: 1271771

SPIN-код: 7764-6343

Завьялов Владимир Александрович

кандидат юридических наук, доцент кафедры криминалистики и правовой информатики ФГБОУ ВО «Кубанский государственный университет»

ORCID: 0000-0002-0054-7087

AuthorID: 1011348

SPIN-код: 2268-2677