УДК 343.982.4

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ИССЛЕДОВАНИИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ ДОКУМЕНТОВ

Алексей Федорович Купин
Управление научно-исследовательской деятельности (научно-исследовательский институт криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации, Московский государственный технический университет имени Н. Э. Баумана, Москва, Россия, alexcrim@rambler.ru

Аннотация. В статье рассматриваются порядок и особенности применения программного обеспечения, которое использует модели машинного обучения, глубокого обучения и некоторые другие возможности искусственного интеллекта как при подделывании цифровых изображений документов, так и при проведении судебных экспертиз в отношении указанных источников информации. Изучены способы маскировки признаков применения инструментов искусственного интеллекта в цифровых изображениях документов.

Приводится описание разработанной компьютерной программы, позволяющей выявлять признаки применения инструментов искусственного интеллекта при создании или редактировании цифровых изображений документов посредством использования возможностей следующих инструментов: метода анализа изображений (Error Level Analysis, ELA); метода изучения метаданных EXIF и XMP; метода исследования неоднородности фоточувствительности (Photo Response Non-Uniformity, PRNU-анализ); методов анализа шума и JPEG-следов; метода градиентного анализа; метода изучения изображения с применением сверточной нейронной сети (CNN Forensics), которая проводит глубокий анализ шума (Noiseprint) или классификационный анализ (AI Patch).

Изучены факторы, влияющие на распространение моделей машинного обучения, глубокого обучения и некоторых других возможностей искусственного интеллекта в различные виды деятельности, предлагаются к внедрению в практическую деятельность экспертов, специализирующихся на исследованиях цифровых изображений документов, алгоритмы работы этих моделей с дальнейшей разработкой соответствующего методического обеспечения.

Ключевые слова: искусственный интеллект, машинное обучение, редактирование документа, методы судебной экспертизы, цифровое изображение документа

Для цитирования: Купин А. Ф. Применение искусственного интеллекта при исследовании цифровых изображений документов // Судебная экспертиза. 2025. № 4 (84). С. 71–80.

APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE STUDY OF DIGITAL DOCUMENT IMAGES

Alexey Fedorovich Kupin
Research Directorate (Research Institute of Criminalistics) of the Chief Criminalistic Directorate (Criminalistic Center) of the Investigative Committee of the Russian Federation, Bauman Moscow State Technical University, Moscow, Russia, alexcrim@rambler.ru

Abstract. The article considers the procedure and peculiarities of application of software that uses machine learning models, deep learning and some other artificial intelligence capabilities, both in forging digital images of documents and in conducting forensic examinations with respect to such sources of information. Ways of masking the use of artificial intelligence tools in digital images of documents are studied.

Description of a computer program developed to identify signs of the use of artificial intelligence tools in creating or editing digital images of documents by using the following tools: method of image analysis (Error Level Analysis, ELA); method of studying EXIF and XMP metadata; method of Photo Response Non-Uniformity (PRNU-analysis); methods of noise analysis and JPEG-traces; method of gradient analysis; method of image study with the use of neural network module "AI Patch Detector" – module-detector of inserts with the use of artificial intelligence is given.

Factors influencing the spread of machine learning models, deep learning and some other possibilities of artificial intelligence in various types of activity are studied, the algorithms for working with these models are proposed to be implemented by experts specializing in the research of digital document images, with further development of appropriate methodological support.

Keywords: artificial intelligence, machine learning, document editing, methods of forensic examination, digital image of the document

For citation: Kupin A. F. Application of artificial intelligence in the study of digital document images. Forensic Examination, 71–80, 2025. (In Russ.).

Технические средства и программные продукты, обладающие функциональными возможностями использования систем искусственного интеллекта (далее – ИИ), являются очередной ступенью научно-технологического развития. Роль и значение ИИ для решения различных задач, возникающих в процессе криминалистического обеспечения раскрытия и расследования преступлений, подробно и системно изложены в работах ученых-криминалистов А. А. Бессонова [1], Д. В. Бахтеева [2], достаточно полно рассматривались применительно к области проведения и последующего оформления результатов судебных экспертиз [3], в том числе применительно к общим вопросам производства технико-криминалистических экспертиз документов [4], поэтому мы не будем подробно останавливаться на этих моментах и уделим основное внимание предметному рассмотрению возможностей применения ряда инструментов ИИ в практической плоскости, в части как описания следов, оставляемых на электронных документах инструментами ИИ, так и возможностей выявления этих следов с помощью различных инструментов ИИ.

Для начала отметим, что благодаря применению инструментов ИИ видоизменились способы и возможности подделки электронных документов. Новые технологии, основанные на применении указанных инструментов, позволили повысить качество изготавливаемых подделок, увеличился риск дачи экспертами ошибочных выводов по результатам исследования электронных документов. Под инструментами ИИ в контексте рассматриваемой проблемы нами понимается программное обеспечение (далее – ПО), которое использует модели машинного обучения, глубокое обучение или другие методы ИИ для автоматизации процессов, анализа данных (изображений, текстов и т. д.).

Поскольку чаще всего изменениям с помощью ИИ подвергаются определенные виды электронных документов – отсканированные и сфотографированные документы, в которых производится удаление, видоизменение, добавление реквизитов, то именно они станут объектами нашего исследования[1]. В настоящее время особенности, связанные с выявлением подделки цифровых изображений документов, изготовленных с помощью инструментов ИИ, которые необходимо учитывать эксперту, обусловлены следующими обстоятельствами.

1. Большая часть ручного труда становится автоматизированной и более точной, при этом не исключена ручная доработка конечных результатов. Как следствие, в подготовленных таким образом подделках становится сложнее обнаружить признаки внесения изменений.

2. Изменяются не только видимые человеческому глазу элементы изображения, но и скрытые характеристики, такие как зашумленность изображения, показатели яркости и цветности, коэффициенты сжатия, минимальные отклонения в геометрии объектов. Поэтому отсутствие аномалий этих характеристик в цифровом изображении не всегда однозначно свидетельствует о том, что редактирование изображения не производилось.

3. Область редактирования может не ограничиваться только зоной непосредственного изменения документа. При обработке изображения с помощью инструментов ИИ может значительно изменяться все изображение целиком, а не только участок, подверженный редактированию. В результате признаки на измененной области изображения документа могут также наблюдаться и на других участках цифрового изображения, которые не подвергались целенаправленному редактированию.

4. Возможности инструментария ИИ постоянно и стремительно расширяются, что часто делает затруднительным выделение признаков, однозначно указывающих на применение этих технологий, особенно в случаях использования для подделки профессиональных ресурсов, обладающих более широкими возможностями по сравнению с открытыми, бесплатными версиями ИИ, имеющими ограниченный функционал.

5. В ряде случаев технология выполнения подделок цифровых изображений документов с помощью инструментов ИИ позволяет комбинировать множество различных операций, делающих обрабатываемые изображения малопригодными для проведения исследования в части разграничения признаков, указывающих

[1] Данные объекты будут обозначены в рамках статьи как цифровые изображения документов.

на применение инструментов ИИ, от признаков, которые могут образовываться в процессе действий, не связанных напрямую с подделкой цифровых изображений (например, сжатие изображения, копирование изображения и т. д.).

6. Для проведения экспертного исследования в целях выявления в цифровых изображениях документов следов применения инструментов ИИ требуются специальные познания не только в области компьютерной (компьютерно-технической) экспертизы, технико-криминалистической экспертизы документов и ряда других экспертиз, но и специфические навыки, позволяющие понимать принципы работы инструментов ИИ и пользоваться этими инструментами в практической деятельности.

7. В настоящий момент отсутствует апробированное методическое обеспечение, позволяющее решать отдельные задачи, связанные с установлением фактов применения инструментов ИИ для изготовления цифровых изображений документов и их редактирования.

Говоря о выявлении признаков подделки документов с помощью инструментов ИИ, нужно обязательно брать в расчет, что умелое владение навыками работы с таким инструментарием позволяет злоумышленнику эффективно осуществлять следующие действия:

1) удалять отдельные реквизиты документов без изменения цвета и яркости участка изображения;

2) выполнять поиск отдельных реквизитов нужного содержания на других документах, размещенных в сети Интернет, при успешном поиске таких реквизитов удалять фон, на котором они располагаются, и затем перемещать эти реквизиты в другой документ с последующим редактированием значений пикселей созданного таким образом цифрового изображения документа;

3) целенаправленно производить улучшение либо ухудшение качества изображения для сокрытия следов проведенного редактирования;

4) выполнять генерацию отдельных реквизитов, в том числе подписей и рукописных текстов на цифровом изображении документа;

5) проводить изменения отдельных характеристик цифровых изображений документов, невидимых либо слабо различимых для человеческого глаза;

6) осуществлять другие действия, чей перечень многообразен вследствие того, что инструментарий ИИ позволяет безгранично использовать свой функционал в зависимости от написанного программного кода под конкретную задачу, решение которой актуально в конкретный промежуток времени.

Помимо применения в целях создания подделок, инструменты ИИ также могут использоваться для выявления признаков внесения изменений в цифровые изображения документов, трудноразличимых с помощью иных криминалистических методов и средств. Так, для выявления признаков подделки цифровых изображений документов может применяться общедоступное ПО, например Forensically[1], Ghiro[2], Amped Authenticate[1], но эти программные средства по отдель-

[1] Forensically. URL: https://29a.ch/photo-forensics/#forensic-magnifier (дата обращения: 10.09.2025).

[2] Ghiro. URL: https://getghiro.org/ (дата обращения: 10.09.2025).

ности могут оказаться не всегда эффективными, часто дают разные выводы при исследовании одних и тех же цифровых изображений документов. Поэтому использование функциональных возможностей инструментов ИИ может оказать ощутимую помощь в ситуациях исследования цифровых изображений документов, когда иные методы малоэффективны.

Так, с помощью инструментария ИИ можно:

1. Выполнять анализ характеристик пикселей изображений, таких как яркость, контрастность, цвет. Таким образом инструменты ИИ позволяют выявлять области с необычными, аномальными значениями, сигнализирующими о наличии признаков редактирования изображений. Например, область цифрового изображения документа, подвергшаяся изменению или вставке другого фрагмента, может отличаться от других областей этого документа резкостью границ, размытыми переходами цветов, несовпадением в цветах и яркости.

2. Обнаруживать следы сжатия, к которым относятся показатели шума, ошибок, особенности сегментации, распределения частот, трансформации и т. д. Например, если изображение документа было обработано в графическом редакторе, оно может содержать признаки повторного сжатия, что можно обнаружить в ходе применения разноплановых анализов на конкретные показатели изображения документа.

3. Изучать метаданные посредством извлечения и анализа EXIF-данных изображений, что позволяет, например: устанавливать устройство, применяемое для первоначального изготовления цифрового изображения документа; определять ПО, применяемое для обработки документа, временные штампы и другие скрытые следы, сохраняемые в цифровых изображениях документов.

4. Исследовать мельчайшие детали цифровых изображений документов. Изображения документов нередко сохраняют уникальную структуру материального носителя, на котором был выполнен изначально документ до перевода его в цифровой вид. Этот материал содержит многочисленные неровности и повреждения, обусловленные, с одной стороны, технологией его изготовления (признаки производственного происхождения), а с другой – дальнейшего взаимодействия с устройствами, с помощью которых наносятся реквизиты документов (признаки эксплуатации). В ряде работ упоминается возможность использования таких особенностей в качестве важных групповых и индивидуализирующих признаков, с помощью которых можно решать различные задачи по установлению технической подделки документов [5; 6].

5. Существенным образом экономить время, необходимое для изучения цифрового изображения документа, поиска и последующего анализа признаков, которые могут указывать на редактирование цифровых изображений документов с помощью инструментов ИИ.

Для исследования цифровых изображений документов рекомендуется использовать комплекс различных методов и средств, поскольку универсальных инструментов не существует. Одним из таких комплексных решений является специальное ПО, позволяющее в автоматическом режиме осуществлять работу

[1] Amped Authenticate. URL: https://ampedsoftware.com/authenticate (дата обращения: 10.09.2025).

с цифровыми изображениями документов и выявлять в них признаки внесения изменений (редактирования, монтажа и т. д.). При создании данного ПО первоочередное внимание было уделено нейросетевым методам, методам анализа изображений (ELA, Noiseprint, PRNU, Copy-Move) и др. [7] Предлагаемая к практическому применению программа создана на языке программирования Python с использованием следующего инструментария:

– OpenCV (Open Source Computer Vision Library) – библиотеки с открытым исходным кодом для компьютерного зрения, которая используется для предобработки изображений, а именно: фильтрации шума, коррекции контрастности и резкости;

– NumPy (Numerical Python) – базового пакета Python, используемого для вычислений и обработки изображений. Он позволяет эффективно представлять изображение как матрицу чисел (пикселей);

– Pillow (Python Imaging Library) – библиотеки для базовой обработки и манипуляции изображениями в Python, которая предоставляет инструменты для открытия, преобразования и сохранения изображений во множестве форматов. Pillow применяется на этапе предобработки изображений;

– PyTesseract – библиотеки, предназначенной для оптического распознавания символов на изображениях. Она позволяет извлекать и «читать» текст, встроенный в изображения, переводя его в электронный вид;

– PyTorch – библиотеки, применяемой при решении задач анализа изображений посредством построения и обучения нейронных сетей, включая специализированные модули для обработки изображений (сверточные слои, средства увеличения данных и др.);

– Tkinter – инструмент Python для создания настольных приложений с графическим интерфейсом.

Архитектура предлагаемой программы модульная – каждый метод анализа реализован отдельной функцией, возвращающей как визуальный результат (тепловую карту[1]), так и текстовый вывод с интерпретацией результатов. После применения всех выбранных методов программа позволяет сформировать объединенный вывод, содержащий следующий набор сведений: выявленные метаданные, статистики по шуму, списки обнаруженных аномалий (например, координаты подозрительных интервалов текста) и т. д. Кроме того, в программе реализована функция построения объединенной тепловой карты – путем наложения результатов нескольких методов. Если разные методы указывают на один и тот же участок изображения как сфальсифицированный, то на объединенной карте такая область изображения подсвечивается наиболее интенсивно.

Интерфейс программы представлен двумя блоками:

1. Основное окно просмотра, включающее:

– область визуализации изображения с возможностью масштабирования (уменьшение / увеличение масштаба);

– область с поддержкой прокрутки и масштабирования, позволяющая удобно исследовать детали изображения, перемещаясь по изображению.

[1] Тепловая карта представляет собой визуальный результат реализации метода.

2. Панель управления, которая содержит клавиши:

1) «Загрузка файла»: возможно изучение файлов форматов JPG, PNG и PDF;

2) «Метаданные», с ее помощью можно проводить:

– просмотр и анализ EXIF, XMP и других скрытых служебных данных;

– проверку временных меток, редакторов, сведений об изготовлении изображения документа;

3) «Метод анализа изображения». Под каждый встроенный в программу метод предусмотрена отдельная клавиша. Например: ELA, Noise, Copy-Move и др. При запуске определенного метода открывается окно с текстовым результатом анализа и / или тепловой картой изученного изображения. В последующем каждая карта сохраняется в памяти для дальнейшей агрегации;

4) «Комплексный анализ». Эта клавиша последовательно запускает все доступные методы, встроенные в программу, а по результатам их применения формируется общий отчет, содержащий текстовый вывод по результатам исследования цифрового изображения с визуальной демонстрацией результатов;

5) «Объединенная карта». По результатам применения всех методов программы с помощью данной клавиши можно получить агрегированную тепловую карту, содержащую визуальные результаты применения всех методов, посредством которых выявлены участки на цифровом изображении документа, подверженные редактированию;

6) AI-модули: AI Patch Detector и CNN Forensics. Эти клавиши позволяют запустить методы, включающие в себя использование нейросетей. По результатам их выполнения осуществляется вывод классификации: «Изменен» или «Оригинал» с визуальной подсветкой центра изображения и отображением карт шумов в зависимости от обнаруженных признаков редактирования.

Алгоритм работы программы можно описать так:

1. Загружается файл изображения документа в графическом формате. Если это файл в формате PDF, извлекается растровое изображение. Затем выполняется предварительное считывание базовых метаданных (EXIF, XMP), которые сразу выводятся, так как они несут информацию о возможном редактировании (например, программа добавляет в список подозрительных меток наличие тега Software, указывающего на использование графического редактора).

2. Осуществляется применение следующих методов анализа, выведенных отдельными кнопками в программе (кнопки интерфейса ELA, «Анализ шума», Copy-Move и др.). Каждый из описанных методов при выполнении отображает свое окно результатов: либо текстовое (описание обнаруженных признаков), либо графическое. Все результаты также сохраняются внутри программы для возможного последующего изучения и проверки.

3. В разделе программы «AI-анализ» имеется кнопка запуска сверточной нейросети (CNN Forensics), которая проводит глубокий анализ шума (Noiseprint) или классификационный анализ (AI Patch) загруженного изображения документа. Для улучшения эффективности обнаружения метод дополнен более наглядной маской, которая позволяет выделять области с превышением порога шумового отпечатка.

4. После применения отдельных методов формируется «Объединенная тепловая карта»: программа использует накопленные изображения-результаты,

полученные в ходе применения ряда методов, и интерпретирует результат в цветовую карту, где синий означает отсутствие признаков редактирования и монтажа, красный – наличие признаков редактирования и монтажа, обнаруженных в процессе исследования представленных объектов.

5. Итоговый вывод формируется на основе совокупности выявленных признаков. Например, если несколько методов (ELA, CNN Forensics, Copy-Move) дали положительные результаты в части наличия признаков редактирования цифрового изображения документа, то программа отметит изображение как «вероятно измененное». Если же ни один из методов не выявил отклонений, будет сформирован вывод об отсутствии видимых следов редактирования. Окончательное решение принимает эксперт, исходя из результатов, полученных с помощью всех методов, примененных им в процессе проведенного исследования.

Представляется, что комбинация обозначенных нами методов позволяет всесторонне изучать цифровое изображение документа. Даже при тщательной обработке цифрового изображения документа скрыть все следы редактирования весьма затруднительно. Если применяется определенный метод для сокрытия следов редактирования, например удаления метаданных, то одновременно образуются шумовые следы, которые будут определены посредством применения метода анализа изображений (ELA). В случае если удаляется шум, останутся следы, которые можно обнаружить посредством использования методов градиентного анализа либо PRNU-анализа. Тем не менее, применяя ПО, основанное на технологиях ИИ, необходимо учитывать, что любая нейронная сеть имеет определенный уровень доверия и может быть подвержена ошибкам первого и второго рода, которые не всегда удается распознать. Поэтому, разрабатывая такое ПО, следует руководствоваться алгоритмами, позволяющими понять механизм принятия решений, что ложатся в основу формируемых выводов эксперта. Основанное на технологиях ИИ ПО не является универсальным средством решения экспертных задач, а выступает как вспомогательный инструмент и должно использоваться в совокупности с другими методами и средствами производства экспертизы.

Список источников

1. Бессонов А. А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О. Е. Кутафина (МГЮА). 2021. № 2 (78). С. 48–51.

2. Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–9.

3. Новакова К. А., Кузьмин М. Н. Перспективы использования искусственного интеллекта при составлении заключения эксперта и оформлении иллюстративного материала // Судебная экспертиза. 2025. № 2 (82). С. 117–127.

4. Купин А. Ф., Коваленко А. С. К вопросу о возможностях применения систем искусственного интеллекта при криминалистическом исследовании документов и их реквизитов // Теория и практика судебной экспертизы. 2023. Т. 18, № 4. С. 28–35.

5. Четверкин П. А., Ефименко А. В. Технико-криминалистическое исследование следов зубчатых колес бумагопроводящих механизмов капельно-струйных принтерных устройств // Вестник Московского университета МВД России. 2016. № 5. С. 97–101.

6. Шведова Н. Н., Досова А. В. О возможностях установления фактов подделки документов, выполненной с использованием цифровых электрофотографических печатающих устройств // Судебная экспертиза. 2022. № 2 (70). С. 48–55.

7. Купин А. Ф. Методы криминалистического изучения документов на электронных носителях информации: монография. Тула: Изд-во ТулГУ, 2025. 178 с.

References

1. Bessonov A. A. The use of artificial intelligence algorithms in the forensic study of criminal activity (on the example of serial crimes). Courier of the Kutafin Moscow State Law University (MSAL), 48–51, 2021. (In Russ.).

2. Bakhteev D. V. Artificial intelligence in investigative activities: tasks and problems. Russian Investigator, 3–9, 2020. (In Russ.).

3. Novakova K. A., Kuzmin M. N. Prospects for the use of artificial intelligence in drawing up an expert opinion and preparing illustrative material. Forensic examination, 117–127, 2025. (In Russ.).

4. Kupin A. F., Kovalenko A. S. On the possibilities of applying artificial intelligence systems in the forensic examination of documents and their details. Theory and practice of forensic expertise, 28–35, 2023. (In Russ.).

5. Chetverkin P. A., Efimenko A. V. Technical and forensic study of traces of gear wheels of paper-conducting mechanisms of drop-jet printer devices. Vestnik of Moscow University of the Ministry of Internal Affairs of Russia, 97–101, 2016. (In Russ.).

6. Shvedova N. N., Dosova A. V. On the possibilities of establishing the facts of document forgery performed using digital electro-photographic printing devices. Forensic examination, 48–55, 2022. (In Russ.).

7. Kupin A. F. Methods of forensic examination of documents on electronic information media. Monograph. Tula: Publishing house of Tula State University; 2025: 178. (In Russ.).

Купин Алексей Федорович,
старший инспектор управления
научно-исследовательской деятельности
(научно-исследовательского института криминалистики)
Главного управления криминалистики
(Криминалистического центра)
Следственного комитета Российской Федерации,
доцент кафедры «Безопасность в цифровом мире»
Московского государственного технического университета
имени Н. Э. Баумана,
кандидат юридических наук, доцент;
alexcrim@rambler.ru

Kupin Alexey Fedorovich,
senior inspector of the research directorate
(research institute of criminalistics)
of the Chief Criminalistic Directorate
(Criminalistic Center) of the Investigative Committee
of the Russian Federation,
associate professor at the department
"Security in the digital world"
Bauman Moscow State Technical University,
candidate of juridical sciences, docent;
alexcrim@rambler.ru

Статья поступила в редакцию 02.09.2025; одобрена после рецензирования 15.09.2025; принята к публикации 14.11.2025.

The article was submitted 02.09.2025; approved after reviewing 15.09.2025; accepted for publication 14.11.2025.

* * *