УДК 004.932 https://doi.org/10.33619/2414-2948/126/16

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИНСТРУМЕНТОВ СОЗДАНИЯ И ОБНАРУЖЕНИЯ ПОДДЕЛЬНЫХ ИЗОБРАЖЕНИЙ И ПРЕДСТАВЛЕНИЕ ГИБРИДНОГО МЕТОДА

©Утепкалиев М. А., *ORCID: 0009-0005-0605-6405, Национальный университете обороны; Институт стратегических исследований и послевузовского образования имени Ататюрка, г. Стамбул, Турция, marat.utepkaliyev@gmail.com*
©Бояджы А., *ORCID: 0000-0003-1016-3439, Национальный университет обороны; Военно-воздушная академия, г. Стамбул, Турция, aytug.boyaci@msu.edu.tr*

COMPARATIVE ANALYSIS OF TOOLS FOR CREATING AND DETECTING FAKE IMAGES AND PRESENTATION OF A HYBRID METHOD

©Utepkaliyev M., *ORCID: 0009-0005-0605-6405, National Defense University; Atatürk Strategic Studies and Graduate Institute, Istanbul, Türkiye, marat.utepkaliyev@ gmail.com*
©Boyaci A., *ORCID: 0000-0003-1016-3439, National Defence University; Air Force Academy, Istanbul, Türkiye, aytug.boyaci@msu.edu.tr*

Аннотация. Развитие генеративных моделей, основанных на методах глубокого обучения, таких как генеративно-состязательные сети (Generative Adversarial Networks, GAN) и диффузионные модели, привело к возможности создания синтетических изображений чрезвычайно высокого уровня реалистичности. Данное обстоятельство создает серьезные трудности в области выявления поддельного мультимедийного контента, особенно в условиях, когда подобные инструменты становятся доступными широкому кругу пользователей, не обладающих специализированными знаниями. В настоящем исследовании представлен сравнительный анализ бесплатных инструментов для генерации и обнаружения поддельных изображений, а также предложен гибридный метод, направленный на повышение эффективности их выявления. В практической части работы были использованы и сопоставлены десять инструментов для генерации поддельных изображений (FaceApp, FaceSwapper.ai, DALL·E 3, Gemini и др.) и десять инструментов для их обнаружения (Illuminarty, Syntheticeye, модели HuggingFace). Проведена их оценка по показателям точности (от 42,14% до 81,13%), скорости работы и удобства использования. На основе выявленных ограничений предложен и реализован комбинированный подход к обнаружению поддельных изображений, основанный на интеграции анализа метаданных (EXIF), анализа уровня ошибок сжатия (Error Level Analysis, ELA) и базовой модели глубокой сверточной нейронной сети (Convolutional Neural Network, CNN), обученной на расширенном наборе данных, содержащем 7180 изображений. Предложенный подход позволил достичь точности обнаружения на уровне 79%. Полученные результаты свидетельствуют о необходимости стандартизации инструментов обнаружения поддельного контента и регулярного обновления используемых моделей с целью противодействия быстро развивающимся средствам генерации синтетических изображений.

Abstract. The rapid development of generative models based on deep learning, such as Generative Adversarial Networks (GANs) and diffusion models, has enabled the creation of highly realistic synthetic images. This development poses significant challenges for the field of forgery

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

detection, particularly in situations where such tools are easily accessible to non-expert users. This study presents a comparative analysis of freely available tools for generating and detecting fake images and proposes a hybrid approach aimed at improving detection effectiveness. In the experimental section, ten tools for fake image generation (including FaceApp, FaceSwapper.ai, DALL·E 3, Gemini, etc.) and ten tools for fake image detection (including Illuminarty, Syntheticeye, and models available on Hugging Face) were utilized and comparatively evaluated. The tools were assessed in terms of detection accuracy (ranging from 42.14% to 81.13%), processing speed, and usability. Based on the identified limitations, a combined approach for fake image detection was proposed and implemented. The method integrates metadata analysis (EXIF), Error Level Analysis (ELA), and a baseline Convolutional Neural Network (CNN) trained on an extended dataset containing 7,180 images. The proposed approach achieved a detection accuracy of 79%. The results highlight the necessity of standardizing fake-detection tools and regularly updating detection models in order to effectively counter the rapidly evolving capabilities of synthetic image generation technologies.

Ключевые слова: глубокое обучение, глубокие подделки, искусственный интеллект, манипуляция, обнаружение поддельных изображений.

Keywords: deep learning, deepfake, artificial intelligence, manipulation, fake images detection.

За последние десять лет развитие генеративных моделей, основанных на методах глубокого обучения, достигло чрезвычайно высокого уровня, позволяя создавать высокореалистичный контент в различных модальностях, таких как текст, изображения, аудио и видео [1].

Модели типа GAN на протяжении длительного времени занимали ведущие позиции в данной области и широко применялись для задач синтеза изображений, а также преобразования текстовых описаний в изображения [2-4].

Впоследствии появились и другие мощные подходы, в частности диффузионные модели, которые значительно расширили возможности генеративных систем [5-6].

В настоящее время инструменты для создания поддельного мультимедийного контента становятся все более доступными и простыми в использовании. В результате даже пользователи, не обладающие специализированными знаниями, могут создавать высокореалистично манипулированные изображения лиц, используя как готовые мобильные приложения, например FakeApp или Reface [7], так и специализированное программное обеспечение, такое как DeepFaceLab и FaceSwap [8].

Быстрое распространение подобного контента, особенно на платформах социальных сетей, существенно усложняет задачу установления его достоверности [9]. Несмотря на то, что в настоящее время разработано значительное количество методов обнаружения поддельного контента, постоянно возрастающий уровень реалистичности и сложность синтезируемых материалов, а также такие факторы, как шум, степень сжатия и изменение размеров изображений, значительно затрудняют способность моделей обнаружения к обобщению при столкновении с ранее неизвестными типами атак и реальными условиями эксплуатации [10].

Целью настоящего исследования является тестирование бесплатных инструментов генерации и обнаружения поддельного мультимедийного контента, а также разработка эффективного комбинированного подхода к решению данной задачи.

Во втором разделе работы рассматриваются основные понятия и технологии, связанные с созданием и обнаружением поддельного мультимедийного контента.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

В практической части исследования демонстрируется, каким образом с использованием бесплатных и удобных для пользователя инструментов можно относительно легко осуществлять различные манипуляции с изображениями, а также генерировать реалистичные изображения различных тематик и типов на основе текстовых описаний. Кроме того, учитывая стремительное развитие инструментов генерации визуального контента, были проанализированы и протестированы существующие решения для выявления поддельных или модифицированных изображений. В результате проведенного исследования осуществлено сравнительное оценивание указанных инструментов, а также предложены наиболее эффективные и простые в использовании сервисы и решения, требующие от пользователя лишь базовых технических знаний.

Основные понятия

Широкое распространение инструментов для генерации поддельного контента и одновременное усложнение процессов его обнаружения создают серьезные угрозы в различных сферах, включая деятельность правоохранительных органов, работу средств массовой информации и системы национальной безопасности. В частности, манипулирование видео- и аудиофайлами приводит к тому, что поддельные материалы становятся практически неотличимыми от подлинных, что подрывает доверие к цифровым платформам и создает значительные риски для общественной безопасности и политической стабильности.

Учитывая стремительные изменения в данной области, разработка специализированных инструментов для выявления поддельного мультимедийного контента, а также проведение дальнейших научных исследований приобретают критически важное значение для обеспечения достоверности информации и безопасности в цифровой среде. Понятие «поддельный» (fake) используется для обозначения цифрового контента, который создается или модифицируется с целью обмана или введения в заблуждение и может включать различные виды мультимедийных данных, такие как изображения, видео и аудио [11].

Истоки мультимедийной фальсификации восходят к XIX веку, когда начали применяться методы манипулирования фотографиями. В XX веке подобные практики получили широкое распространение в кинематографе и печатных средствах массовой информации. В настоящее время данная область претерпела значительную трансформацию благодаря развитию программного обеспечения, компьютерной графики и технологий искусственного интеллекта [12].

Особенно важную роль в этом процессе сыграло развитие методов глубокого обучения и генеративных моделей, прежде всего GAN, которые позволили автоматизировать процесс создания поддельного контента, сделав его более быстрым и реалистичным [11, 13].

В отличие от традиционных методов ручного редактирования, при которых нередко возникали заметные визуальные несоответствия, современные подходы, основанные на глубоком обучении, существенно снижают вероятность обнаружения подобных артефактов [6-7].

Предложенная в 2014 году архитектура GAN основана на состязательном процессе обучения между генеративной и дискриминаторной нейронными сетями, что позволяет создавать поддельный контент высокого качества [14-15].

В Таблице 1 представлена классификация различных типов моделей GAN и их основные характеристики.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Таблица 1

КЛАССИФИКАЦИЯ И ОСОБЕННОСТИ РАЗЛИЧНЫХ ТИПОВ GAN

Типы GAN	*Краткое описание*	*Применение*	*Особенности*
cGAN [16-18]	Расширение GAN с помощью дополнительных условных входов включает в себя такие элементы, как классы меток, текстовые или визуальные параметры.	Контроль генерирования	Позволяет генерировать данные для определенных классов, повышая точность и контроль над процессом генерирования.
DCGAN [19-22]	В архитектуре генератора и дискриминатора вместо полностью связанных слоев используются сверточные нейронные сети.	Создание изображений	Он отличается более стабильным обучением и простой структурой приложения для создания реалистичных данных.
WGAN [18, 23-25]	Разработан на основе расстояния Вассерштейна (Earth Mover’s Distance), которое повышает мотивацию к обучению.	Создание изображений и видео	Решает проблемы нестабильного обучения и обеспечивает лучшую сходимость благодаря изменениям в функции потерь.
CycleGAN [15, 17, 18, 26-30]	Для преобразования изображений между различными областями обучаются две модели генератора и две модели дискриминатора.	Создание изображений, видео и звука	Позволяет выполнять преобразования, такие как изменение стиля или преобразование голоса, без необходимости использования парных наборов данных.
StarGAN [14, 26]	Представляет собой модель, способную выполнять преобразование изображений между несколькими доменами (мультидоменная трансформация).	Преобразование изображений	Для выполнения преобразований используется один генератор, что обеспечивает повышенную эффективность.
StyleGAN [4, 31-33]	Архитектура, предназначенная для генерации изображений с использованием стилей (деконволюции и скрытых представлений)	Фотореалистичные изображения	Предоставляет пользователю полный контроль над структурой изображения, обеспечивая генерацию четких и высокодетализированных визуальных данных..
StyleGAN2 [4]	Является усовершенствованной версией StyleGAN, в которой устранены визуальные артефакты.	Создание изображений и видео	Усовершенствованная архитектура устраняет эффект «перекрестных текстур», делая генерируемые данные более фотореалистичными.
Pix2PixHD [34, 35]	Высококачественная модель для преобразования изображений, включающая синтез реалистичных объектов.	Преобразование изображений	Сосредоточен на синтезе высококачественных объектов и работает с соответствующими обучающими данными.
BigGAN [27, 33]	Архитектура, ориентированная на высокую степень детализации и цветового баланса при создании изображений.	Создание изображений	Позволяет работать с более крупными наборами данных и может одновременно содержать несколько классов объектов.
PGGAN [19, 36]	Это модель, в которой разрешение постепенно	Создание изображений	Постепенно возрастающая сложность помогает

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Типы GAN	*Краткое описание*	*Применение*	*Особенности*
	увеличивается в процессе обучения.		предотвратить проблемы на ранних этапах обучения и улучшить конечный результат.
StackGAN [30, 37]	Двухэтапный процесс создания изображения: на первом этапе создается черновой набросок, на втором этапе добавляются детали.	Создание изображений	Используется для создания изображений на основе текстовых описаний и повышает уровень детализации на каждом этапе.
MelGAN [38]	На основе обученной модели генерирует высокочастотные и реалистичные звуковые данные.	Создание звука	Простая архитектура, не содержащая сложных функций потери, что ускоряет речевую и звуковую генерацию.
HiFi-GAN [39]	Высококачественный синтез звука, ориентированный на реалистичность и скорость.	Синтез музыки и речи	Оптимизирует быструю производительность, повышая реалистичность и применимость в приложениях реального времени.
SAGAN [40]	Для повышения согласованности между различными частями наборов данных применяется механизм самоконтроля.	Создание музыки, изображений и звука	Разработан для обработки данных с длительными повторениями, например, сложных музыкальных композиций.

В результате этих технологических достижений технология «глубоких подделок» (deepfake) с 2017 года начала стремительно распространяться и оказала значительное влияние во многих областях – от индустрии развлечений до кибербезопасности [9, 41].

После 2017 года методы и инструменты создания и обнаружения deepfake также начали быстро развиваться, чему способствовал общий прогресс в области технологий. Процесс замены лиц позволил значительно упростить создание высококачественных изображений и видеоматериалов, что, в свою очередь, усложнило выявление следов манипуляций [42].

В Таблице 2 представлена классификация типов и функциональных особенностей deepfake контента.

Таблица 2

КЛАССИФИКАЦИЯ ТИПОВ И ФУНКЦИЙ DEEPFAKE КОНТЕНТА [43]

Типы deepfake	*Классификация функций*
Deepfake изображений	Изменение внешнего вида лица и тела, модификация черт лица, замена лица одного человека лицом другого и/или комбинирование этих элементов.
Deepfake видео	Замена лица человека, присутствующего в видеоматериале, лицом другого человека, а также перенос визуального поведения одного человека на лицо и тело другого.
Deepfake звуки	Изменение или имитация голосовых характеристик, а также синтез речи целевого лица на основе вновь созданных текстовых входных данных.
Deepfake звуки и видео	Изменение движений губ и артикуляции говорящего человека с синхронизацией с исходным контентом для обеспечения липсинхронизации, что позволяет привести речевые высказывания в видеоматериале в соответствие с целевым языком или текстом.

Параллельно с этими достижениями появились такие приложения, как FakeApp и DeepFaceLab, благодаря чему технология deepfake стала доступной для широкой аудитории пользователей и получила возможность применения в злонамеренных целях. Данные

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

приложения используют автокодировщики (autoencoders) и GAN для выполнения операций по замене лиц [8, 15].

В Таблице 3 представлены программные средства и приложения, используемые для создания deepfake-контента. Deepfake-материалы, созданные с использованием технологий искусственного интеллекта, могут быстро распространяться через социальные сети и достигать миллионов пользователей. Это создает серьезную угрозу в виде распространения фейковых новостей, дезинформации и мошенничества. При этом объектами подобных атак могут становиться не только известные личности и политики, но и обычные граждане [44].

Таблица 3

ИНСТРУМЕНТЫ И ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ В СОЗДАНИИ DEEPFAKE [45]

Инструменты	*Типы*	*Характеристика*
Классические инструменты создания подделок		
Adobe Premiere	Коммерческое десктопное программное обеспечение	Редактирование звука и видео, изменение кадра видео с помощью искусственного интеллекта
Corel VideoStudio	Коммерческое десктопное программное обеспечение	Запатентованная технология искусственного интеллекта
Синхронизация губ		
Dynalips	Коммерческое вэб приложение	Запатентованная технология
Crazytalk	Коммерческое вэб приложение	Запатентованная технология
Wav2Lip	Приложение с открытым исходным кодом	GAN с предварительно обученной дискриминационной сетью и функцией потерь, ориентированной на визуальное качество.
Манипуляция атрибутами лица		
FaceApp	Мобильное приложение	CNN
Adobe	Коммерческое десктопное программное обеспечение	Глубокая нейронная сеть (DNN) + Фильтры
Rosebud	Коммерческое вэб приложение	Запатентованная технология искусственного интеллекта
Изменение лица		
ZAO	Мобильное приложение	Запатентованная технология
RPEACE	Мобильное приложение	Запатентованная технология
Reflect	Мобильное приложение	Запатентованная технология
Impressions	Мобильное приложение	Запатентованная технология
FakeApp	Десктопное приложение	GAN
FaceSwap	Приложение с открытым исходным кодом	Две пары кодировщиков-декодировщиков (с общими параметрами)
Dräker	Приложение с открытым исходным кодом	Функция потери DSSIM для реконструкции лица. Приложение на основе библиотеки Keras.
DeepFaceLab	Приложение с открытым исходным кодом	Предоставляет различные методы распознавания лиц, такие как dlib, MTCNN, S3FD и т. д. Расширяет различные модели Faceswap, такие как H64, H128, LIAEF128, SAE и т. д.
FaceSwapGAN	Приложение с открытым исходным кодом	Автоматический кодировщик использует две функции потерь: противоположные потери и воспринимаемые потери.
DeepFake-tf	Приложение с открытым исходным кодом	Аналогичен DFaker, однако для реализации приложения используется TensorFlow.
Faceswapweb	Коммерческое вэб приложение	GAN

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

	Оживляние лица	
Face2Face	Приложение с открытым исходным кодом	Применяет трехмерную морфологическую модель лица (3DMM) в сочетании с методами машинного обучения.
Dynamixyz	Коммерческое десктопное программное обеспечение	Методы машинного обучения
FaceIT3	Приложение с открытым исходным кодом	GAN
	Создание лица	
Generated Photos	Коммерческое вэб приложение	StyleGAN
	Синтез звука	
Overdub	Коммерческое вэб приложение	Запатентованная технология искусственного интеллекта
Respeccher	Коммерческое вэб приложение	Сочетает традиционные алгоритмы цифровой обработки сигналов с запатентованными методами глубокого генеративного моделирования
SV2TTS	Приложение с открытым исходным кодом	Обобщенная сквозная (end-to-end) LSTM с функцией потерь.
ResembleAI	Коммерческое вэб приложение	Запатентованная технология искусственного интеллекта
Volcery	Коммерческое вэб приложение	Запатентованная технология искусственного интеллекта и глубокого обучения
VoiceApp	Мобильное приложение	Запатентованная технология искусственного интеллекта

Материал и методы исследования

Настоящее исследование направлено на определение степени эффективности существующих инструментов обнаружения поддельных изображений, созданных с использованием технологий искусственного интеллекта. В настоящее время широко распространяются такие технологии, как замена лица (face swapping), генерация фотореалистичных изображений на основе текстовых описаний, а также цифровая реставрация и улучшение старых фотографий. Однако данные технологические достижения одновременно повышают риск создания и распространения поддельного мультимедийного контента. В связи с этим разработка надежных и эффективных методов обнаружения фейковых изображений становится актуальной и необходимой задачей.

Создание, обнаружение и анализ изображений. В рамках данного исследования поддельные изображения были сгенерированы с использованием различных инструментов, после чего полученные материалы были проанализированы с применением открытых средств обнаружения подделок в рамках поэтапного исследовательского процесса. Общая схема реализованного методологического подхода представлена на Рисунке 1.

В статье процесс создания и обнаружения поддельных изображений рассматривается в рамках двухэтапной экспериментальной методологии. На первом этапе были созданы поддельные изображения с использованием десяти различных инструментов с открытым исходным кодом, выбранных с учетом их доступности и способности выполнять различные типы визуальных манипуляций. В ходе данного этапа, включающего три основные категории – генерацию и замену лиц, создание фотореалистичных изображений на основе текстовых описаний, а также редактирование изображений – был сформирован набор данных, состоящий из 130 изображений, что позволило обеспечить разнообразие исследуемого контента.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

На втором этапе сгенерированные изображения были проанализированы с использованием десяти широко применяемых инструментов обнаружения поддельных изображений с открытым исходным кодом. В процессе анализа были оценены такие параметры, как точность классификации инструментов, их производительность и удобство использования, ограничения доступа, а также технические и алгоритмические особенности применяемых решений. Благодаря проведенному комплексному сравнительному анализу предполагается выявить эффективность существующих методов обнаружения, а также определить сильные и слабые стороны используемых инструментов в зависимости от применяемых технологий генерации изображений. Ожидается, что полученные результаты будут способствовать разработке более надежных и эффективных подходов к обнаружению поддельных изображений.

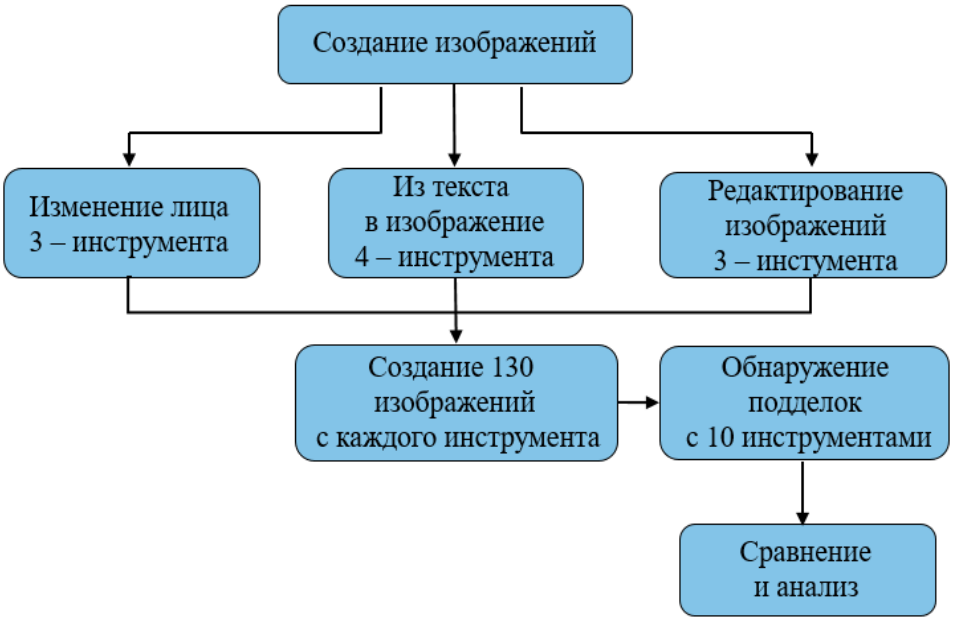

Рисунок 1. Схема реализации методологического подхода

По результатам данного исследования предполагается провести сравнительный анализ уровня обнаруживаемости изображений, созданных различными методами генерации. Кроме того, ставится задача выявить виды подделок, которые характеризуются повышенной устойчивостью к обнаружению, а также определить инструменты, демонстрирующие наибольшую эффективность при выявлении подобного контента. Предполагается, что полученные результаты внесут вклад в разработку более точных и надежных систем автоматического обнаружения поддельных изображений и будут иметь ориентирующее значение для дальнейших научных исследований в данной области.

Для изменения лиц использовались инструменты FaceApp, FaceSwapper.ai и Photo Lab. Генерация изображений на основе текстовых описаний осуществлялась с использованием платформ искусственного интеллекта, таких как ChatGPT (DALL·E 3), Gemini, Leonardo AI и Fusionbrain-Kandinsky. Для восстановления и цветизации черно-белых фотографий применялись такие платформы как Remini, RestoreFoto и ColorizePro.

Выбранные инструменты охватывают основные методы модификации изображений, что позволяет оценить возможности и ограничения современных технологий создания синтетического визуального контента.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

На втором этапе практической части исследования проведена эмпирическая оценка эффективности десяти инструментов открытого доступа, предназначенных для обнаружения поддельных изображений. Среди исследуемых решений – пять веб-платформ: Illuminarty, Rufakeapp, Aidetectcontent, Syntheticeye (Aletheia), Aiimagedetector, а также пять моделей платформы HuggingFace (Gourieff/AI-image-detector, Parth-2703/AI-Image-Detection-2, datxy/AI-Image-Detector, Sleepyriizi/AI-Fake-detector и FaceOnLive/Deepfake-Detector [36-43].

Валидация проводилась с использованием 50 реальных изображений и 130 модифицированных или сгенерированных изображений, полученных с помощью наиболее известных инструментов создания поддельных изображений.

Результаты и обсуждение

Полученные результаты показывают наличие существенных различий в точности обнаружения между протестированными системами. Согласно результатам анализа, средний показатель успешности обнаружения варьируется в диапазоне от 42,14% (Illuminarty) до 81,13% (Syntheticeye). Такой широкий диапазон, свидетельствует об отсутствии единых стандартов в области обнаружения поддельных изображений, а также о значительных различиях в степени зрелости применяемых алгоритмических подходов.

Среди протестированных инструментов наивысшие показатели точности продемонстрировали Syntheticeye (Aletheia) (81,13%), FaceOnLive/Deepfake-Detector (76,42%) и Sleepyriizi/AI-Fake-Detector (71,16%). Средние показатели обнаружения для используемых инструментов представлены в Таблице 4. Относительно высокая эффективность данных решений объясняется использованием современных архитектур глубокого обучения, таких как CNN, EfficientNet и Swin-V2, а также тем, что результаты анализа формируются в более интерпретируемой форме. Эти особенности делают указанные инструменты перспективными решениями для применения в задачах цифровой криминалистики и экспертного анализа визуального контента.

Таблица 4

СРЕДНИЙ КОЭФФИЦИЕНТ ОБНАРУЖЕНИЯ

Генерация	*Illuminarty*	*Rufakeapp*	*Aidetectcontent*	*Syntheticeye (ALETHEIA)*	*Aiimage Detector*	*Gourieff/AI-image-detector*	*Parth-2703/AI-Image-Detection-2*	*datxy/AI-Image-Detector*	*Sleepyriizi/ AI-Fake-detector*	*FaceOnLive/ Deepfake-Detector*
FaceApp	11,03	41,17	44,1	80,5	44,38	34,8	37,4	69,2	19,51	29,3
FaceSwapper.ai	18,25	45,47	44,65	83,36	49,11	33	39,7	69,95	50,33	94
Photo Lab	26,29	42,54	57,93	95,34	52,63	50,57	62,87	51,77	91,6	46,7
ChatGPT (DALL-E3)	65,77	54,38	30,8	92,7	50,05	40,4	32,8	53,8	97,9	99
Gemini	84,26	52,97	67,7	68,16	31,96	52,7	52,4	60,5	74,69	95,8
Leonardo AI	97,44	55,3	73,9	92,75	43,65	57,9	56,3	61,6	100	99
Fusionbrain-Kandinsky	94,6	53,18	54,6	89,11	48,54	54,3	68,2	39,3	99,94	99
Remini	11,55	44,63	49,6	52,25	55,6	50,2	62,6	69,5	0,1	69,6
RestoreFoto	5	45,81	49,2	55,64	55,36	54,3	61,5	71,6	10	79,4
ColorizePro	7,18	34,04	49,3	52,68	61,37	57,9	61,4	83,4	0,45	52,4
ИТОГО:	**42,14**	47,05	52,18	**81,13**	49,61	48,51	53,42	71,16	54,45	76,42

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

В ходе исследования также привлекло на себя внимание сложность обнаружения контента, созданного с использованием современных и широко распространенных инструментов генерации изображений. Изображения, сгенерированные такими системами, как DALL-E 3, Gemini, Leonardo AI и Kandinsky, в ряде случаев достигают высокого уровня фотореалистичности, при котором их трудно отличить от подлинных изображений. В частности, изображения, созданные с помощью Leonardo AI, были классифицированы как поддельные лишь в 42,14% случаев системой Illuminarty и в 55,3% случаев системой Rufakeapp. В то же время те же изображения были обнаружены системой Syntheticeye с точностью 92,75%. Данный результат указывает на то, что использование более продвинутых архитектур играет ключевую роль в выявлении поддельного контента с высоким уровнем реалистичности.

Сравнительный анализ также выявил значительные различия между инструментами не только по показателю точности, но и по таким параметрам, как время обработки, удобство пользовательского интерфейса, интерпретируемость результатов, а также поддержка языков и форматов. С точки зрения времени обработки наиболее быстрыми инструментами оказались Illuminarty (примерно 4 сек) и Rufakeapp (примерно 10 сек), однако данное преимущество сопровождается относительно низкой точностью обнаружения.

В противоположность этому решения, использующие более сложные модели, такие как datxy и Sleepyriizi, хотя и требуют до 90 секунд на один анализ, демонстрируют существенно более высокую точность обнаружения.

Относительно пользовательского опыта инструменты AiImageDetector, AiDetectContent, Sleepyriizi/AI-Fake-Detector и FaceOnLive/Deepfake Detector получили наиболее высокие оценки благодаря простому и понятному интерфейсу, поддержке нескольких языков и наглядному представлению результатов анализа. В то же время инструмент Parth-2703/AI Fake Image Detector, несмотря на высокие алгоритмические возможности, получил более низкую оценку из-за ограниченного удобства и простоты в использовании. Подробная оценка инструментов с точки зрения производительности, технических характеристик и удобства применения представлена в Таблице 5.

Таблица 5

ОЦЕНКА ЭФФЕКТИВНОСТИ, ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК
И УДОБСТВА ИСПОЛЬЗОВАНИЯ СРЕДСТВ ОБНАРУЖЕНИЯ ПОДДЕЛЬНЫХ ИЗОБРАЖЕНИЙ

Время обработки (сек.)	*Ограничения*	*Простота в использовании (с 1 по 5 баллов)*	*Языковая поддержка*	*Метод обнаружения подделок*	*Форматы изображений и размер*	*Объявление результатов*	*Тип результата (%)*
Illuminarty.ai (вэб приложение)							
~ 4	Да	4	En	-	png, jfif, jpg, pjpig, jpeg, webp.	Нет	Вероятность, что является подлинным или созданным ИИ.
RuFakeApp (вэб приложение)							
~ 10	Нет	4	En	CNN	png, jpg. Размер до 10 мб	Нет	Определение подлинности изображения.
Aidetectcontent (вэб приложение)							

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Время обработки (сек.)	*Ограничения*	*Простота в использовании (с 1 по 5 баллов)*	*Языковая поддержка*	*Метод обнаружения подделок*	*Форматы изображений и размер*	*Объявление результатов*	*Тип результата (%)*
~ 20	Нет	5	En	-	jpeg, jpg, png. Размер до 5 мб	Да	Вероятность, что является подлинным или созданным ИИ, размер и разрешение, EXIF данные.
SyntheticEye (вэб приложение)							
~ 15	Да	4	En	CNN	png, jpg, jpeg, webp.	Да, и в платной версий более детальней	Вероятность, что является подлинным или созданным ИИ, использования моделей GAN и CGAN.
AIImageDetector (вэб приложение)							
~ 10	Нет	5	12 языков	-	Все форматы	Нет	Вероятность, что является подлинным или созданным ИИ.
Gourieff (Hugging Face)							
~ 35	Нет	4	En	ViT	png, gif, jfif, jpg, pjpig, jpeg.	Нет	Вероятность, что является подлинным или созданным ИИ.
Parth-2703 (Hugging Face)							
~ 15	Нет	3	En	Fine Tuned	Все форматы	Нет	Вероятность, что является подлинным или созданным ИИ.
Datxy (Hugging Face)							
~ 90	Нет	4	En	Swin-tiny-patch4-window7-224, ViT	Все форматы	Нет	Анализ результатов, вероятность, что является подлинным или созданным ИИ.
Sleepyriizi (Hugging Face)							
~ 70	Нет	5	En	Swin-V2, SuSy, GLCM	Все форматы	Нет	Вероятность, что является подлинным или созданным ИИ.
FaceOnLive (Hugging Face)							
~ 30	Да	5	En	EfficientNet	Все форматы	Да	Анализ наличия ИИ, манипуляций с лицом, итоговая вероятностная оценка.

Результаты исследования показали, что при анализе фотореалистичного поддельного контента, созданного с использованием таких приложений, как FaceApp, FaceSwapper.ai и PhotoLab, большинство бесплатных средств обнаружения демонстрируют критически низкий уровень точности. Кроме того, разные показатели обнаружения одного и того же изображения различными инструментами наглядно указывает на отсутствие методологических стандартов в данной области.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Наконец, установлено, что при анализе изображений, содержащих лишь незначительные изменения например, ретушь или небольшие модификации черт лица точность обнаружения резко снижается. Это свидетельствует о том, что существующие решения обладают ограниченной адаптивностью к тонким и реалистичным манипуляциям. Данное обстоятельство подчеркивает необходимость разработки более устойчивых, обобщаемых и контекстно-чувствительных подходов к обнаружению поддельных изображений.

Комбинированный подход к обнаружению поддельных изображений (EXIF + ELA + CNN). В предыдущих абзацах данного раздела было представлено сравнительное исследование, касательно создания и обнаружения поддельных изображений с использованием бесплатных инструментов, в рамках которого были определены наиболее эффективные решения. Однако данное исследование не охватывает глубокие технические вопросы и внутреннюю логику алгоритмов обнаружения, а также не включает комплексную оценку качества изображений на различных уровнях их обработки.

В этом контексте целесообразным представляется применение комбинированного подхода, основанного на использовании нескольких методов анализа. Такая необходимость особенно актуальна ввиду высокой вероятности возникновения ложных результатов, поскольку ни один из существующих инструментов обнаружения не является полностью надежным.

В рамках данной работы был предложен и протестирован комбинированный метод обнаружения поддельных изображений. Предложенный подход основан на интеграции трех методов: анализа метаданных (EXIF), анализа уровня ошибок изображения (ELA) и сверточных нейронных сетей (CNN).

Данный метод позволяет не только осуществлять первичную фильтрацию изображений путтм выявления следов редактирования на уровне файловых метаданных, но и проводить более детальный анализ пиксельных и структурных искажений, возникающих в результате различных манипуляций с изображениями. Кроме того, использование CNN обеспечивает возможность выявления более сложных и труднообнаруживаемых искажений в визуальном содержании изображения [46, 47].

Каждый этап предложенного метода был реализован с использованием соответствующих библиотек языка программирования Python [48].

Анализ метаданных EXIF. Метаданные EXIF представляют собой встроенные структуры данных, которые автоматически формируются цифровыми устройствами в момент съемки. Эти данные содержат такие параметры, как модель камеры, дата и время съемки, фокусное расстояние, параметры экспозиции, а также информация об используемом программном обеспечении. В контексте цифровой криминалистики метаданные EXIF являются важным источником информации, позволяющим определить, подвергалось ли изображение редактированию или было ли оно создано искусственным способом. В частности, наличие в поле Software указаний на программы редактирования изображений (например, Adobe Photoshop) либо отсутствие ключевых параметров съемки может свидетельствовать о возможной фальсификации изображения.

В ходе исследования анализ EXIF-данных был проведен на выборке из 20 изображений, включая 10 подлинных и 10 поддельных. Полученные результаты показали, что ни одно из поддельных изображений не содержало EXIF-метаданных, что соответствует распространенной практике, при которой большинство программ редактирования автоматически удаляют подобную информацию. Вместе с тем было установлено, что у двух подлинных изображений также отсутствовали EXIF-данные. Это свидетельствует о том, что анализ EXIF может эффективно использоваться в качестве первичного инструмента

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

фильтрации, однако не является достаточным методом для окончательной верификации подлинности изображения.

Метод ELA (Error Level Analysis). Данный метод направлен на выявление локальных аномалий, возникающих вследствие неоднородного сжатия изображения. Если в определенных областях изображения выполнялось редактирование (например, добавление объектов, ретушь и т. д.), уровень ошибок в этих областях после повторного применения JPEG-сжатия будет отличаться от остальных участков. Визуализация этих различий позволяет локализовать зоны вмешательства.

В ходе работы все изображения были преобразованы в формат JPEG и повторно сохранены для последующего вычисления разницы. Результаты показали, что изображения, классифицированные как поддельные, демонстрируют выраженные артефакты в областях лица и фона, тогда как большинство оригинальных изображений сохраняют однородность уровня ошибок [49, 50].

Для повторного сохранения изображения и вычисления разницы в данном исследовании был использован скрипт на языке программирования Python с библиотекой Pillow. Пример результата анализа ELA представлен на рисунке 2 для одного из изображений.

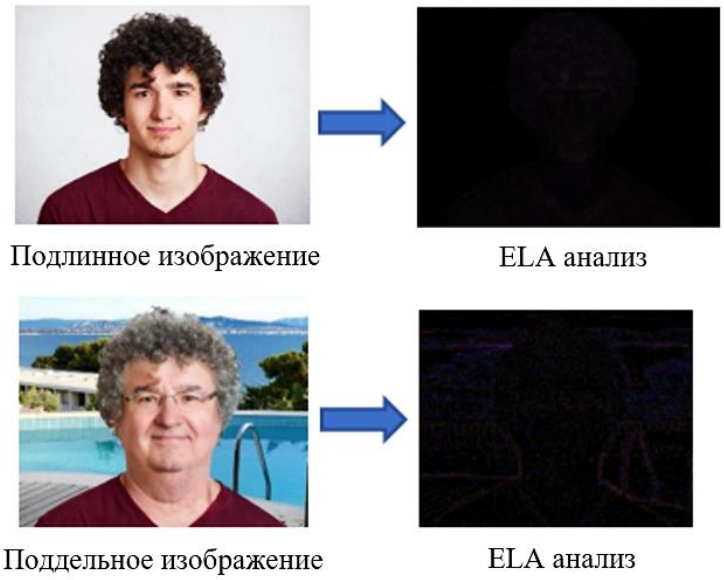

Рисунок 2. Результаты анализа методом ELA

Реализация базовой архитектуры CNN. В рамках данного исследования была реализована модель CNN для бинарной классификации изображений на подлинные (“real”) и поддельные (“fake”). Выбор архитектуры CNN обоснован ее доказанной эффективностью в задачах компьютерного зрения, в частности при выявлении различных видов манипуляции на изображениях.

Для построения модели использовались технологии TensorFlow/Keras, для оценки метрик Scikit-learn, а для обработки изображений библиотека Pillow, при этом вся работа проводились в среде Google Colab. Изначально использовался локальный набор данных, включающий 50 подлинных и 130 поддельных изображений. Однако данный объем оказался недостаточным для эффективного обучения нейронной сети. В связи с этим был дополнительно использован открытый набор данных с платформы Kaggle (https://www.kaggle.com/datasets/sachchitkunichetty/rvf10k), часть изображений которого была включена в исследование. После объединения данных итоговый набор выборки составил:

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

подлинные изображения 3550, поддельные изображения 3630, что обеспечило сбалансированное распределение классов и минимизировало риск смещения модели в сторону доминирующего класса. Простейшая архитектура CNN, примененная для бинарной классификации подлинных и поддельных изображений в данном исследовании, представлена на Рисунке 3.

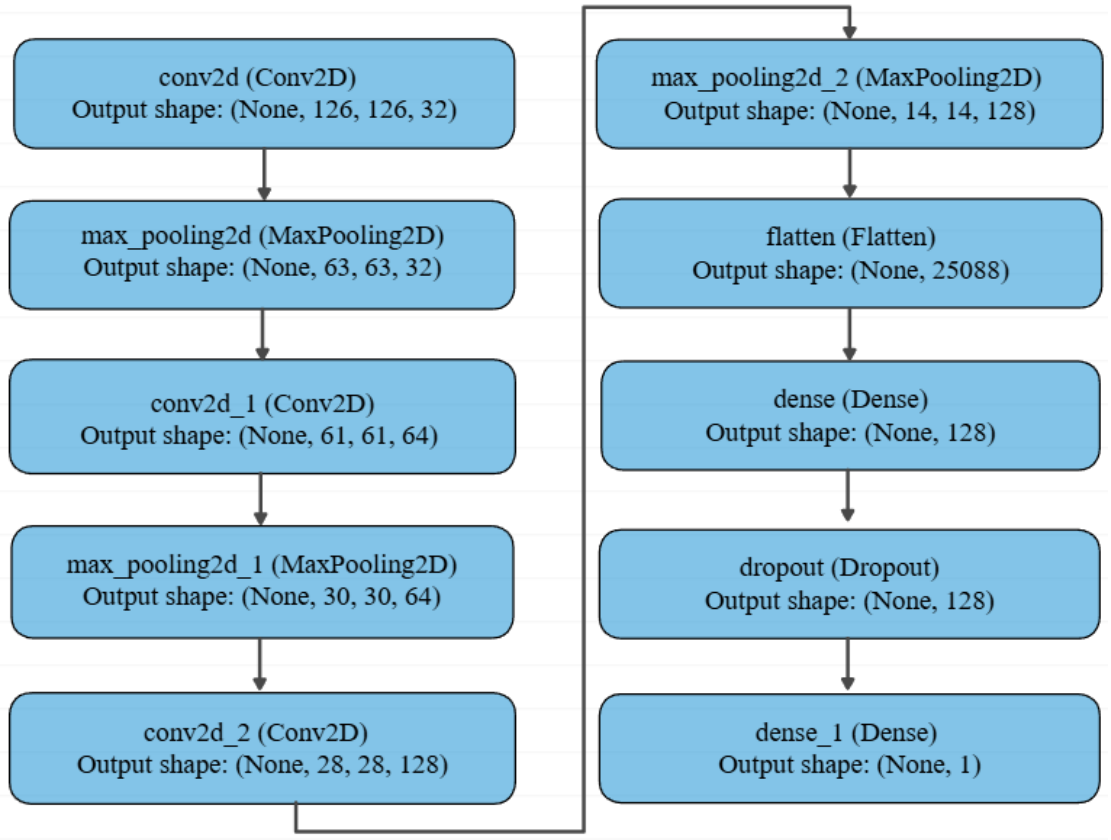

Рисунок 3. Базовая архитектура CNN, примененная для бинарной классификации подлинных и поддельных изображений

После серии экспериментов была выбрана следующая архитектура:

Слой Conv2D с 32 фильтрами размером (3, 3) и функцией активации ReLU: этот слой выполняет свертку входного изображения с 32 различными фильтрами, извлекая такие признаки, как границы, текстуры и узоры.

Слой MaxPooling2D с размером окна (2, 2): этот слой подвыборки (pooling), применяемый после каждого сверточного слоя, уменьшает размеры карт признаков, сохраняя при этом важные признаки и снижая вычислительную сложность.

Повторение слоев свертки и подвыборки: данная последовательность повторяется еще дважды, при этом количество фильтров в сверточных слоях увеличивается до 64 и 128 соответственно. Каждое последующее сочетание сверточного и pooling-слоя позволяет модели извлекать более абстрактные и сложные признаки из изображений.

Слой Flatten: после последнего слоя подвыборки выполняется операция выпрямления, преобразующая трехмерный тензор признаков в одномерный вектор, пригодный для передачи в полносвязные слои.

Полносвязные слои (Dense): далее следуют два полносвязных слоя. Первый слой содержит 128 нейронов с функцией активации ReLU и выполняет более глубокое извлечение

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

сложных комбинаций признаков. Для уменьшения переобучения (overfitting) после первого полносвязного слоя применяется Dropout с коэффициентом 0,5. Второй полносвязный слой состоит из одного нейрона с sigmoid-активацией, предсказывающего наличие deepfake на входном изображении.

Сигмоидная функция активации на выходе преобразует результат в значение от 0 до 1, интерпретируемое как вероятность принадлежности изображения к одному из классов (подлинное или поддельное).

Обучение модели. Для оптимизации параметров нейронной сети был использован адаптивный стохастический градиентный спуск (Adam). В качестве функции потерь применялась binary_crossentropy, что соответствует задаче бинарной классификации. В качестве основной метрики оценки качества модели использовалась точность (accuracy), поскольку обучающий набор данных был сбалансирован по классам.

Обучение проводилось с размером батча 32 на протяжении 45 эпох. Данные были разделены на обучающую и тестовую выборки в пропорции 70% / 30% соответственно.

В ходе обучения отслеживались значения точности и функции потерь как на обучающей, так и на проверочной (валидационной) выборке. Динамика изменения точности в процессе обучения представлена на Рисунке 4.

```
Epoch 30/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 132s 835ms/step - accuracy: 0.7740 - loss: 0.4813 - val_accuracy: 0.7595 - val_loss: 0.5291
Epoch 31/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 130s 822ms/step - accuracy: 0.7724 - loss: 0.4781 - val_accuracy: 0.7474 - val_loss: 0.5250
Epoch 32/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 134s 847ms/step - accuracy: 0.7881 - loss: 0.4528 - val_accuracy: 0.7516 - val_loss: 0.5320
Epoch 33/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 131s 824ms/step - accuracy: 0.7959 - loss: 0.4399 - val_accuracy: 0.7498 - val_loss: 0.5204
Epoch 34/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 130s 820ms/step - accuracy: 0.7765 - loss: 0.4653 - val_accuracy: 0.7558 - val_loss: 0.5150
Epoch 35/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 130s 822ms/step - accuracy: 0.8031 - loss: 0.4348 - val_accuracy: 0.7586 - val_loss: 0.4978
Epoch 36/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 129s 818ms/step - accuracy: 0.8030 - loss: 0.4293 - val_accuracy: 0.7679 - val_loss: 0.4991
Epoch 37/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 137s 870ms/step - accuracy: 0.8030 - loss: 0.4250 - val_accuracy: 0.7651 - val_loss: 0.5088
Epoch 38/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 162s 994ms/step - accuracy: 0.8054 - loss: 0.4185 - val_accuracy: 0.7660 - val_loss: 0.5090
Epoch 39/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 156s 990ms/step - accuracy: 0.8141 - loss: 0.4031 - val_accuracy: 0.7669 - val_loss: 0.4793
Epoch 40/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 148s 935ms/step - accuracy: 0.8173 - loss: 0.4033 - val_accuracy: 0.7702 - val_loss: 0.5146
Epoch 41/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 138s 875ms/step - accuracy: 0.8179 - loss: 0.4137 - val_accuracy: 0.7776 - val_loss: 0.4869
Epoch 42/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 134s 845ms/step - accuracy: 0.8152 - loss: 0.3989 - val_accuracy: 0.7665 - val_loss: 0.5425
Epoch 43/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 139s 878ms/step - accuracy: 0.8107 - loss: 0.4064 - val_accuracy: 0.7660 - val_loss: 0.4952
Epoch 44/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 134s 846ms/step - accuracy: 0.8227 - loss: 0.3970 - val_accuracy: 0.7795 - val_loss: 0.4955
Epoch 45/45
158/158 ━━━━━━━━━━━━━━━━━━━━ 133s 843ms/step - accuracy: 0.8360 - loss: 0.3685 - val_accuracy: 0.7892 - val_loss: 0.5316
```

Рисунок 4. Динамика изменения точности (accuracy) в процессе обучения

Модель продемонстрировала стабильный процесс обучения на протяжении 45 эпох. Начальная точность на обучающей выборке составляла около 50%, а к концу обучения достигла 83%. Точность на валидационной выборке аналогично увеличилась и стабилизировалась на уровне 79%. Изменение точности модели на обучающей и валидационной выборках во времени представлено на Рисунке 5. С точки зрения функции потерь, как на обучающей, так и на валидационной выборках наблюдается устойчивое снижение значения потерь, при этом признаков переобучения (overfitting) не выявлено. Динамика изменения функции потерь в ходе эпох представлена на Рисунке 6.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

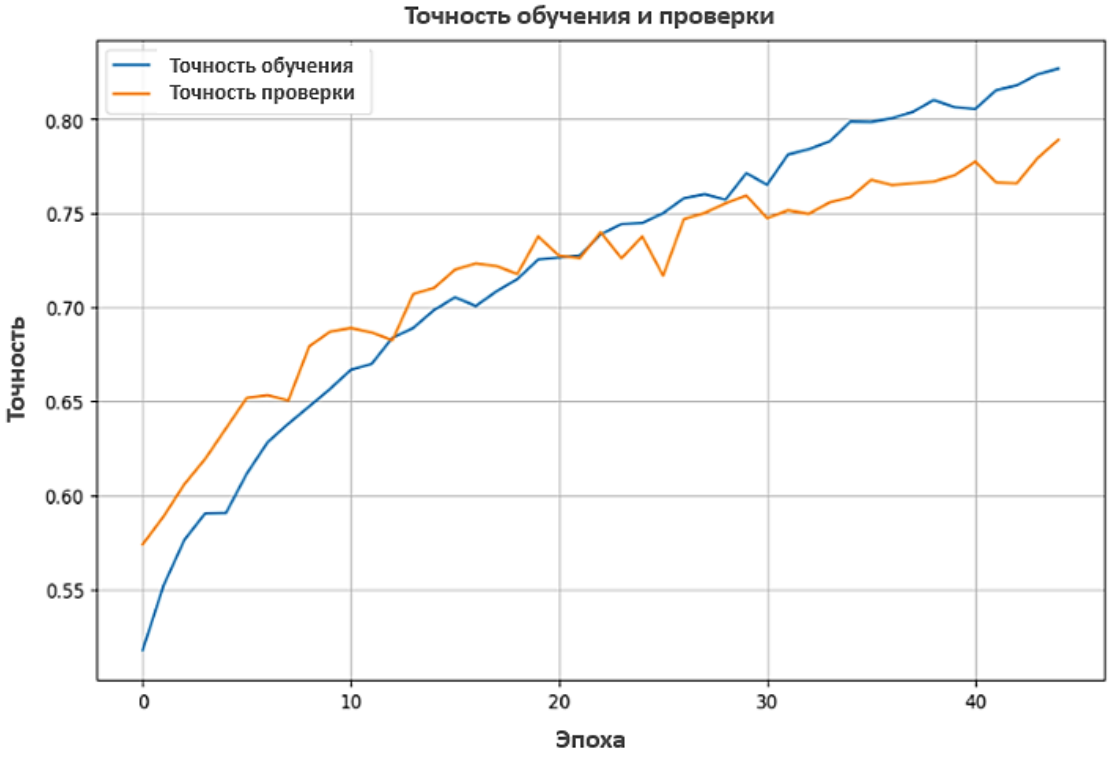

Рисунок 5. График изменения точности

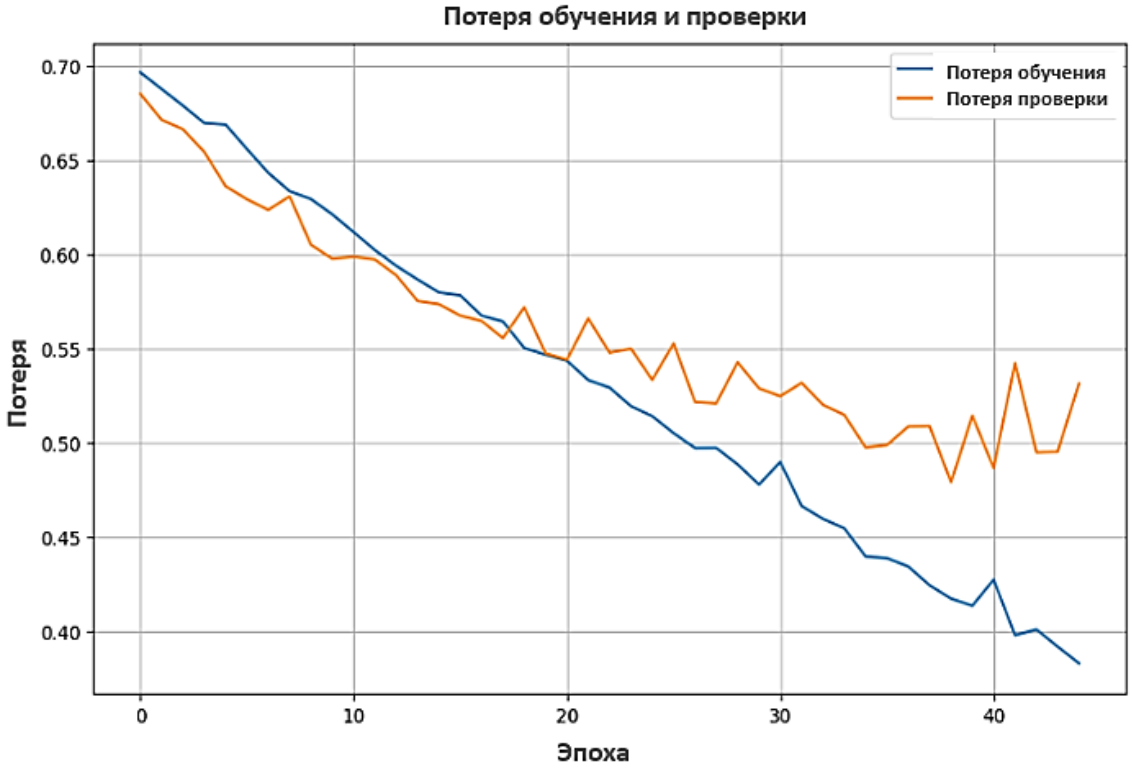

Рисунок 6. Изменения функции потерь

При оценке классификационной эффективности модели для класса “fake” значения метрик составили: precision – 0,81, recall – 0,76, F1-score – 0,78. Для класса “real” показатели были следующими: precision – 0,77, recall – 0,81, F1-score – 0,79. Общая точность (accuracy) модели составила 79%. Классификационный отчет с представленными метриками показан на Рисунке 7.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

	precision	recall	f1-score	support
fake	0.76	0.79	0.77	1089
real	0.78	0.74	0.76	1065
accuracy			0.77	2154
macro avg	0.77	0.77	0.77	2154
weighted avg	0.77	0.77	0.77	2154

Рисунок 7. Класификационный отчет

Несмотря на относительно простую архитектуру модели, при бинарной классификации поддельных и реальных изображений были получены удовлетворительные и сбалансированные результаты. Модель продемонстрировала сбалансированные метрики по всем классам и стабильную сходимость. Это подтверждает применимость сверточных нейронных сетей даже без использования предварительно обученных весов, несмотря на относительную простоту архитектуры.

Вместе с тем использованная архитектура CNN обладает ограниченной сверточной глубиной. Предполагается, что для выявления более сложных случаев подделки производительность модели может быть повышена за счет применения более глубоких архитектур или моделей, предварительно обученных на крупных наборах данных (например, EfficientNet, Xception).

Хотя используемый в исследовании набор данных был расширен, он все еще не охватывает все возможные вариации синтетически созданного мультимедийного контента. Поэтому на последующих этапах планируется проведение сравнительного анализа с моделями, обученными на более обширных и разнообразных наборах данных.

Тем не менее данное исследование представляет собой значимый вклад как с точки зрения методологического подхода, так и с позиции демонстрации практической применимости базовой модели в наглядной и доступной форме, что соответствует исследовательским и образовательным целям статьи.

Заключение

Проведенное исследование выявило существенные различия в эффективности бесплатных инструментов, используемых для обнаружения поддельных изображений, создаваемых современными средствами генерации фейковых изображений. Установлено, что точность обнаружения напрямую связана с архитектурой применяемых алгоритмов и их способностью адаптироваться к новым генеративным моделям. Особое внимание привлекает то, что такие популярные системы, как DALL·E 3, Gemini, Leonardo AI и Fusionbrain-Kandinsky, способны генерировать изображения, которые визуально практически неотличимы от подленных. Данная ситуация ставит под сомнение надежность устаревших или недостаточно обученных систем автоматического обнаружения подделок и показывает, что в условиях реальной эксплуатации такие системы могут демонстрировать ограниченную эффективность. Архитектуры компьютерного зрения, такие как EfficientNet, Swin-V2 и Vision Transformer (ViT), продемонстрировали наиболее высокую производительность при анализе изображений. Однако даже эти модели столкнулись с трудностями при обработке изображений, подвегнутых к минимальной манипуляции, что подчеркивает необходимость регулярного обновления обучающих данных в условиях стремительного развития генеративных технологий. В рамках исследования был предложен комбинированный подход, основанный на анализе EXIF-метаданных, использовании метода ELA и применении базовой

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

архитектуры CNN. Данный метод показал практическую эффективность даже при ограниченном объеме обучающих данных. Первичные этапы анализа (EXIF и ELA) могут использоваться для выявления явно аномальных объектов и предварительной оценки достоверности изображения, тогда как модуль нейронной сети обеспечивает более глубокий анализ. На основе набора данных, расширенного реальными и поддельными изображениями, полученными с платформы Kaggle, была разработана и протестирована простая архитектура CNN. Модель достигла точности около 79%, что сопоставимо или в ряде случаев превосходит результаты существующих бесплатных инструментов обнаружения подделок. В качестве практического решения предлагается интегрированная онлайн-система, объединяющая три метода анализа: EXIF, ELA и CNN-модуль. Такой подход может расширить потенциал применения системы в областях цифровой криминалистики, информационной безопасности и расследований различного характера. Кроме того, в ходе анализа были рассмотрены и сопоставлены различные методы обнаружения поддельных изображений. Определены возможные направления их дальнейшего совершенствования, включая расширение и диверсификацию обучающих наборов данных, оптимизацию архитектуры моделей (количество слоев, размеры фильтров, использование различных функций активации), а также применение предварительно обученных моделей, что особенно важно при работе в условиях ограниченных вычислительных ресурсов. Таким образом, результаты исследования подтверждают потенциал гибридного и интегрированного подхода в процессе выявления и обнаружения изображений. Данное исследование вносит вклад в развитие технологий обеспечения достоверности мультимедийного контента и подчеркивает важность повышения уровня цифровой грамотности.

Интернет-ресурсы:

AI Image Detector. https://aiimagedetector.org
ChatGPT (OpenAI). https://chatgpt.com
ColorizePro Photo Restoration. https://colorizepro.ru
DeepFake Detector. https://faceonlive.com/deepfake-detector
Face Swapper. https://faceswapper.ai
FaceApp: Face Editor. https://clc.li/wPcas
Google Gemini. https://gemini.google.com
Illuminarty AI Detector. https://app.illuminarty.ai
Kandinsky Image Generator Platform. https://fusionbrain.ai
Leonardo AI Image Generator. https://leonardo.ai
Maybe’s AI Art Detector. https://clc.li/QOnOT
Photo Lab Photo Editor and Art. https://clc.li/ZNWRn
Remini Photo Enhancement. https://clc.li/BWndN
RestoreFoto AI Restoration. https://restorefoto.ru
RUFake Image Authentication System. https://www.rufakeapp.com
Synthetic Eye AI Detector. https://syntheticeye.dev
Trusted AI Generated Image Detector. https://clc.li/nGHaO
Two Stage AI Fake Detector. https://clc.li/FgnbG

Список литературы:

1. Alhabeeb S. K., Al-Shargabi A. A. Text-to-image synthesis with generative models: Methods, datasets, performance metrics, challenges, and future direction // IEEE Access. 2024. V. 12. P. 24412-24427. https://doi.org/10.1109/ACCESS.2024.3365043

2. Sharma H., Das S. A brief study of generative adversarial networks and their applications in image synthesis // Multimedia Tools and Applications. 2024. V. 83. №7. P. 21551-21581. https://doi.org/10.1007/s11042-023-16175-2

3. Porkodi S. P., Sarada V., Maik V., Gurushankar K. Generic image application using GANs (generative adversarial networks): A review // Evolving Systems. 2023. V. 14. №5. P. 903-917. https://doi.org/10.1007/s12530-022-09464-y

4. Liu M., Wei Y., Wu X., Zuo W., Zhang L. Survey on leveraging pre-trained generative adversarial networks for image editing and restoration // Science China Information Sciences. 2023. V. 66. №5. P. 151101. https://doi.org/10.1007/s11432-022-3679-0

5. Полежаева М. В., Кенжина Д. С., Нерпин Е. С., Сафонова Т. В., Мокряк А. В. Использование нейронной сети для генерации изображений // Международный журнал информационных технологий и энергоэффективности. 2024. Т. 9. №8 (46). С. 97.

6. Bushey J. AI-generated images as an emergent record format //2023 IEEE International Conference on Big Data (BigData). IEEE, 2023. P. 2020-2031. https://doi.org/10.1109/BigData59044.2023.10386946

7. Luo A. et al. Beyond the prior forgery knowledge: Mining critical clues for general face forgery detection //IEEE Transactions on Information Forensics and Security. – 2023. – Т. 19. – С. 1168-1182. https://doi.org/10.1109/TIFS.2023.3332218

8. Chauhan R., Popli R., Kansal I. A systematic review on fake image creation techniques // 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2023. P. 779-783.

9. Dang M., Nguyen T. N. Digital face manipulation creation and detection: A systematic review // Electronics. 2023. V. 12. №16. P. 3407. https://doi.org/10.3390/electronics12163407

10. Yoo Y., Na D., Nathanson S., Cao Y., Watkins L. Disinformation at scale: detecting ai-human composite images via convolution ensembles // MILCOM 2024-2024 IEEE military communications conference (milcom). IEEE, 2024. P. 621-626. https://doi.org/10.1109/MILCOM61039.2024.10773642

11. Ромашов В. А., Еремук В. В., Чернов Р. Масштабирование систем оптической связи в свободном пространстве // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации. 2023. С. 53-56.

12. Русин М. И., Вайнштейн В. И. Методы поиска синтетических изменений в видеозаписи // Информационная безопасность: сборник докладов Всероссийской Школы молодых ученых. Новосибирск, 2022. С. 24.

13. Alanazi S., Asif S. Exploring deepfake technology: creation, consequences and countermeasures // Human-Intelligent Systems Integration. 2024. V. 6. №1. P. 49-60. https://doi.org/10.1007/s42454-024-00054-8

14. Patel Y., Tanwar S., Bhattacharya P., Gupta R., Alsuwian T., Davidson I. E., Mazibuko T. F. An improved dense CNN architecture for deepfake image detection // IEEE Access. 2023. V. 11. P. 22081-22095. https://doi.org/10.1109/ACCESS.2023.3251417

15. Shahzad H. F., Rustam F., Flores E. S., Luis Vidal Mazon J., De la Torre Diez I., Ashraf I. A review of image processing techniques for deepfakes // Sensors. 2022. V. 22. №12. P. 4556. https://doi.org/10.3390/s22124556

16. Mehmood R., Bashir R., Giri K. J. Text conditioned generative adversarial networks generating images and videos: A critical review // SN Computer Science. 2024. V. 5. №7. P. 935. https://doi.org/10.1007/s42979-024-03289-z

17. Li J., Li T., Lin R., Nie Q. GAN-based models and applications // 2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE, 2022. P. 848-852. https://doi.org/10.1109/ICISCAE55891.2022.9927647

18. Li J., Zhang C., Zhu W., Ren Y. A comprehensive survey of image generation models based on deep learning // Annals of Data Science. 2025. V. 12. №1. P. 141-170. https://doi.org/10.1007/s40745-024-00544-1

19. Khatri A., Gupta N. A Study on Analyzing Deepfake through various Facial Regions-A Review // 2023 6th International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2023. V. 6. P. 1133-1138. https://doi.org/10.1109/IC3I59117.2023.10397658

20. Di Giammarco M., Santone A., Cesarelli M., Martinelli F., Mercaldo F. Evaluating deep learning resilience in retinal fundus classification with generative adversarial networks generated images // Electronics. 2024. V. 13. №13. P. 2631. https://doi.org/10.3390/electronics13132631

21. Chang Y. H., Chung P. H., Chai Y. H., Lin H. W. Color face image generation with improved generative adversarial networks // Electronics. 2024. V. 13. №7. P. 1205. https://doi.org/10.3390/electronics13071205

22. Айрапетов А. Э., Коваленко А. А. Виды генеративно-состязательных сетей // Достижения науки и образования. 2019. №4 (45). С. 7-13.

23. Oubara A., Wu F., Maleki R., Ma B., Amamra A., Yang G. Enhancing adversarial learning-based change detection in imbalanced datasets using artificial image generation and attention mechanism //ISPRS International Journal of Geo-Information. 2024. V. 13. №4. P. 125. https://doi.org/10.3390/ijgi13040125

24. Chen C., Liu D., Ma S., Nepal S., Xu C. Private image generation with dual-purpose auxiliary classifier // Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2023. P. 20361-20370.

25. Wu S., Liu Z., Zhang B., Zimmermann R., Ba Z., Zhang X., Ren K. Do as i do: Pose guided human motion copy //IEEE Transactions on Dependable and Secure Computing. 2024. V. 21. №6. P. 5293-5307. https://doi.org/10.1109/TDSC.2024.3371530

26. Raza S. A., Habib U., Usman M., Cheema A. A., Khan M. S. MMGANGUARD: a robust approach for detecting fake images generated by GANS using multi-model techniques // IEEE Access. 2024. V. 12. P. 104153-104164. https://doi.org/10.1109/ACCESS.2024.3393842

27. Kumari R., Garg H. Image splicing forgery detection: A review //Multimedia Tools and Applications. 2025. V. 84. №8. P. 4163-4201. https://doi.org/10.1007/s11042-024-18801-z

28. Elnabawy R. H., Abdennadher S., Hellwich O., Eldawlatly S. ClipArtGAN: An Application of Pix2Pix Generative Adversarial Network for Clip Art Generation // Multimedia Tools and Applications. 2025. V. 84. №25. P. 30281-30305. https://doi.org/10.1007/s11042-024-20361-1

29. Emara M. M., Farouk M., Fakhr M. W. Parent gan: image generation model for creating parent's images using children's images // Multimedia Tools and Applications. 2025. V. 84. №24. P. 28643-28665. https://doi.org/10.1007/s11042-024-20186-y

30. Arif D., Mehmood Z., Ullah A., Winberg S. High-definition image formation using multi-stage cycle generative adversarial network with applications in image forensic // Arabian Journal for Science and Engineering. 2024. V. 49. №3. P. 3887-3896. https://doi.org/10.1007/s13369-023-08193-x

31. Convertini V. N., Impedovo D., Lopez U., Pirlo G., Sterlicchio G. Discrete fourier transform in unmasking deepfake images: A comparative study of stylegan creations // Information. 2024. V. 15. №11. P. 711. https://doi.org/10.3390/info15110711

32. Kumar L., Singh D. K. Pose image generation for video content creation using controlled human pose image generation GAN // Multimedia Tools and Applications. 2024. V. 83. №20. P. 59335-59354.

33. Qiao T., Chen Y., Zhou X., Shi R., Shao H., Shen K., Luo X. CSC-Net: Cross-color spatial co-occurrence matrix network for detecting synthesized fake images // IEEE Transactions on Cognitive and Developmental Systems. 2023. V. 16. №1. P. 369-379. https://doi.org/10.1109/TCDS.2023.3274450

34. Alrowais F., Hassan A. A., Almukadi W. S., Alanazi M. H., Marzouk R., Mahmud A. Boosting deep feature fusion-based detection model for fake faces generated by generative adversarial networks for consumer space environment // IEEE Access. 2024. V. 12. P. 147680-147693. https://doi.org/10.1109/access.2024.3470128

35. Alamayreh O., Fascella C., Mandelli S., Tondi B., Bestagini P., Barni M. Just Dance: detection of human body reenactment fake videos // EURASIP Journal on Image and Video Processing. 2024. V. 2024. №1. P. 21. https://doi.org/10.1186/s13640-024-00635-2

36. Камилов Э. М., Егоров А. А. Генерация пористых сред с использованием генеративно-состязательной нейронной сети // Вестник кибернетики. 2020. №3(39). С. 79-86..

37. Zhang H., Xu T., Li H., Zhang S., Wang X., Huang X., Metaxas D. N. Stackgan++: Realistic image synthesis with stacked generative adversarial networks // IEEE transactions on pattern analysis and machine intelligence. 2018. V. 41. №8. P. 1947-1962. https://doi.org/10.1109/TPAMI.2018.2856256

38. Kumar K., Kumar R., De Boissiere T., Gestin L., Teoh W. Z., Sotelo J., Courville A. C. Melgan: Generative adversarial networks for conditional waveform synthesis // Advances in neural information processing systems. 2019. V. 32.

39. Kong J., Kim J., Bae J. Hifi-gan: Generative adversarial networks for efficient and high fidelity speech synthesis // Advances in neural information processing systems. 2020. V. 33. P. 17022-17033.

40. Zhang H., Goodfellow I., Metaxas D., Odena A. Self-attention generative adversarial networks // International conference on machine learning. PMLR, 2019. P. 7354-7363.

41. Джуров А. А., Черкесова Л. В., Ревякина Е. А. Программное средство, определяющее феиковый видеоконтент с помощью технологии Deepfake алгоритма GAN // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. №4. С. 60-67.

42. Tampubolon M. Digital face forgery and the role of digital forensics // International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique. 2024. V. 37. №3. P. 753-767. https://doi.org/10.1007/s11196-023-10030-1

43. Karakoç E., Zeybek B. Görmek inanmaya yeter mi? Görsel dezenformasyonun ayirt edici biçimi olarak siyasi deepfake içerikler // Öneri Dergisi. 2022. V. 17. №57. P. 50-72. https://doi.org/10.14783/maruoneri.908542

44. Chaitra B., Reddy P. V. B. Digital image forgery: taxonomy, techniques, and tools–a comprehensive study // International Journal of System Assurance Engineering and Management. 2023. V. 14. №Suppl 1. P. 18-33. https://doi.org/10.1007/s13198-022-01829-5

45. Masood M., Nawaz M., Malik K. M., Javed A., Irtaza A., Malik H. Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward: Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward // Applied intelligence. 2023. V. 53. №4. P. 3974-4026. https://doi.org/10.1007/s10489-022-03766-z

46. Nagm A. M., Moussa M. M., Shoitan R., Ali A., Mashhour M., Salama A. S., AbdulWakel H. I. Detecting image manipulation with ELA-CNN integration: a powerful framework for

authenticity verification // PeerJ Computer Science. 2024. V. 10. P. e2205. https://doi.org/10.7717/peerj-cs.2205

47. Vadrevu A., Rajeshwari R., Pabbathi L., Sirimalla S., Vodnala D. Image forgery detection using metadata analysis and ELA processor // Innovations in Computer Science and Engineering: Proceedings of the Ninth ICICSE, 2021. Singapore: Springer Singapore, 2022. P. 579-586. https://doi.org/10.1007/978-981-16-8987-1_62

48. Шустова Е. П. Введение в анализ изображений на Python. Казань, 2020. 88 с.

49. Aggarwal G., Srivastava A. K., Jhajharia K., Sharma N. V., Singh G. Detection of deep fake images using convolutional neural networks // 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS). IEEE, 2023. P. 1083-1087. https://doi.org/10.1109/ICTACS59847.2023.10389973

50. Kar P., Xue Z., Ardakani S. P., Kwong C. F. Are fake images bothering you on social network? Let us detect them using recurrent neural network // IEEE Transactions on Computational Social Systems. 2022. V. 10. №2. P. 783-794. https://doi.org/10.1109/TCSS.2022.3159709

References:

1. Alhabeeb, S. K. & Al-Shargabi, A. A. (2024). Text-to-image synthesis with generative models: Methods, datasets, performance metrics, challenges, and future direction. *IEEE Acces, 12*, 24412-24427. https://doi.org/10.1109/ACCESS.2024.3365043

2. Sharma, H., & Das, S. (2024). A brief study of generative adversarial networks and their applications in image synthesis. *Multimedia Tools and Applications*, *83*(7), 21551-21581. https://doi.org/10.1007/s11042-023-16175-2

3. Porkodi, S. P., Sarada, V., Maik, V., & Gurushankar, K. (2023). Generic image application using GANs (generative adversarial networks): A review. *Evolving Systems*, *14*(5), 903-917. https://doi.org/10.1007/s12530-022-09464-y

4. Liu, M., Wei, Y., Wu, X., Zuo, W., & Zhang, L. (2023). Survey on leveraging pre-trained generative adversarial networks for image editing and restoration. *Science China Information Sciences*, *66*(5), 151101. https://doi.org/10.1007/s11432-022-3679-0

5. Polezhaeva, M. V., Kenzhina, D. S., Nerpin, E. S., Safonova, T. V., & Mokryak, A. V. (2024). Ispol′zovanie nejronnoj seti dlya generatsii izobrazhenij. *Mezhdunarodnyj zhurnal informatsionnykh tekhnologij i energoeffektivnosti, 9*(8 (46)), 97.

6. Bushey, J. (2023, December). AI-generated images as an emergent record format. In *2023 IEEE International Conference on Big Data (BigData)* (pp. 2020-2031). IEEE. https://doi.org/10.1109/BigData59044.2023.10386946

7. Luo, A., Kong, C., Huang, J., Hu, Y., Kang, X., & Kot, A. C. (2023). Beyond the prior forgery knowledge: Mining critical clues for general face forgery detection. *IEEE Transactions on Information Forensics and Security*, *19*, 1168-1182. https://doi.org/10.1109/TIFS.2023.3332218

8. Chauhan, R., Popli, R., & Kansal, I. (2023, March). A systematic review on fake image creation techniques. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 779-783). IEEE.

9. Dang, M., & Nguyen, T. N. (2023). Digital face manipulation creation and detection: A systematic review. *Electronics*, *12*(16), 3407. https://doi.org/10.3390/electronics12163407

10. Yoo, Y., Na, D., Nathanson, S., Cao, Y., & Watkins, L. (2024). Disinformation at scale: detecting ai-human composite images via convolution ensembles. In *MILCOM 2024-2024 IEEE military communications conference (milcom)* (pp. 621-626). IEEE. https://doi.org/10.1109/MILCOM61039.2024.10773642

11. Romashov, V. A., Eremuk, V. V., & Chernov, R. (2023). Masshtabirovanie sistem opticheskoj svyazi v svobodnom prostranstve. In *Fundamental'nye i prikladnye nauchnye issledovaniya: aktual'nye voprosy, dostizheniya i innovatsii* (pp. 53-56).

12. Rusin, M. I., & Vajnshtejn, V. I. (2022). Metody poiska sinteticheskikh izmenenij v videozapisi. In *Informatsionnaya bezopasnost': sbornik dokladov Vserossijskoj Shkoly molodykh uchenykh, Novosibirsk,* 24.

13. Alanazi, S., & Asif, S. (2024). Exploring deepfake technology: creation, consequences and countermeasures. *Human-Intelligent Systems Integration*, *6*(1), 49-60. https://doi.org/10.1007/s42454-024-00054-8

14. Patel, Y., Tanwar, S., Bhattacharya, P., Gupta, R., Alsuwian, T., Davidson, I. E., & Mazibuko, T. F. (2023). An improved dense CNN architecture for deepfake image detection. *IEEE Access*, *11*, 22081-22095. https://doi.org/10.1109/ACCESS.2023.3251417

15. Shahzad, H. F., Rustam, F., Flores, E. S., Luis Vidal Mazon, J., De la Torre Diez, I., & Ashraf, I. (2022). A review of image processing techniques for deepfakes. *Sensors*, *22*(12), 4556. https://doi.org/10.3390/s22124556

16. Mehmood, R., Bashir, R., & Giri, K. J. (2024). Text conditioned generative adversarial networks generating images and videos: A critical review. *SN Computer Science*, *5*(7), 935. https://doi.org/10.1007/s42979-024-03289-z

17. Li, J., Li, T., Lin, R., & Nie, Q. (2022, September). GAN-based models and applications. In *2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE)* (pp. 848-852). IEEE. https://doi.org/10.1109/ICISCAE55891.2022.9927647

18. Li, J., Zhang, C., Zhu, W., & Ren, Y. (2025). A comprehensive survey of image generation models based on deep learning. *Annals of Data Science*, *12*(1), 141-170. https://doi.org/10.1007/s40745-024-00544-1

19. Khatri, A., & Gupta, N. (2023, September). A Study on Analyzing Deepfake through various Facial Regions-A Review. In *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 6, pp. 1133-1138). IEEE. https://doi.org/10.1109/IC3I59117.2023.10397658

20. Di Giammarco, M., Santone, A., Cesarelli, M., Martinelli, F., & Mercaldo, F. (2024). Evaluating deep learning resilience in retinal fundus classification with generative adversarial networks generated images. *Electronics*, *13*(13), 2631. https://doi.org/10.3390/electronics13132631

21. Chang, Y. H., Chung, P. H., Chai, Y. H., & Lin, H. W. (2024). Color face image generation with improved generative adversarial networks. *Electronics*, *13*(7), 1205. https://doi.org/10.3390/electronics13071205

22. Ajrapetov, A. E., & Kovalenko, A. A. (2019). Vidy generativno-sostyazatel′nykh setej. *Dostizheniya nauki i obrazovaniya*, (4 (45)), 7-13.

23. Oubara, A., Wu, F., Maleki, R., Ma, B., Amamra, A., & Yang, G. (2024). Enhancing adversarial learning-based change detection in imbalanced datasets using artificial image generation and attention mechanism. *ISPRS International Journal of Geo-Information*, *13*(4), 125. https://doi.org/10.3390/ijgi13040125

24. Chen, C., Liu, D., Ma, S., Nepal, S., & Xu, C. (2023). Private image generation with dual-purpose auxiliary classifier. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 20361-20370).

25. Wu, S., Liu, Z., Zhang, B., Zimmermann, R., Ba, Z., Zhang, X., & Ren, K. (2024). Do as i do: Pose guided human motion copy. *IEEE Transactions on Dependable and Secure Computing*, *21*(6), 5293-5307. https://doi.org/10.1109/TDSC.2024.3371530

26. Raza, S. A., Habib, U., Usman, M., Cheema, A. A., & Khan, M. S. (2024). MMGANGUARD: a robust approach for detecting fake images generated by GANS using multi-model techniques. *IEEE Access*, *12*, 104153-104164. https://doi.org/10.1109/ACCESS.2024.3393842

27. Kumari, R., & Garg, H. (2025). Image splicing forgery detection: A review. *Multimedia Tools and Applications*, *84*(8), 4163-4201. https://doi.org/10.1007/s11042-024-18801-z

28. Elnabawy, R. H., Abdennadher, S., Hellwich, O., & Eldawlatly, S. (2025). ClipArtGAN: An Application of Pix2Pix Generative Adversarial Network for Clip Art Generation. *Multimedia Tools and Applications*, *84*(25), 30281-30305. https://doi.org/10.1007/s11042-024-20361-1

29. Emara, M. M., Farouk, M., & Fakhr, M. W. (2025). Parent gan: image generation model for creating parent's images using children's images. *Multimedia Tools and Applications*, *84*(24), 28643-28665. https://doi.org/10.1007/s11042-024-20186-y

30. Arif, D., Mehmood, Z., Ullah, A., & Winberg, S. (2024). High-definition image formation using multi-stage cycle generative adversarial network with applications in image forensic. *Arabian Journal for Science and Engineering*, *49*(3), 3887-3896. https://doi.org/10.1007/s13369-023-08193-x

31. Convertini, V. N., Impedovo, D., Lopez, U., Pirlo, G., & Sterlicchio, G. (2024). Discrete fourier transform in unmasking deepfake images: A comparative study of stylegan creations. *Information*, *15*(11), 711. https://doi.org/10.3390/info15110711

32. Kumar, L., & Singh, D. K. (2024). Pose image generation for video content creation using controlled human pose image generation GAN. *Multimedia Tools and Applications*, *83*(20), 59335-59354.

33. Qiao, T., Chen, Y., Zhou, X., Shi, R., Shao, H., Shen, K., & Luo, X. (2023). CSC-Net: Cross-color spatial co-occurrence matrix network for detecting synthesized fake images. *IEEE Transactions on Cognitive and Developmental Systems*, *16*(1), 369-379. https://doi.org/10.1109/TCDS.2023.3274450

34. Alrowais, F., Hassan, A. A., Almukadi, W. S., Alanazi, M. H., Marzouk, R., & Mahmud, A. (2024). Boosting deep feature fusion-based detection model for fake faces generated by generative adversarial networks for consumer space environment. *IEEE Access*, *12*, 147680-147693. https://doi.org/10.1109/access.2024.3470128

35. Alamayreh, O., Fascella, C., Mandelli, S., Tondi, B., Bestagini, P., & Barni, M. (2024). Just Dance: detection of human body reenactment fake videos. *EURASIP Journal on Image and Video Processing*, *2024*(1), 21. https://doi.org/10.1186/s13640-024-00635-2

36. Kamilov, E. M., & Egorov, A. A. (2020). Generatsiya poristykh sred s ispol′zovaniem generativno-sostyazatel′noj nejronnoj seti. *Vestnik kibernetiki*, (3 (39)), 79-86.

37. Zhang, H., Xu, T., Li, H., Zhang, S., Wang, X., Huang, X., & Metaxas, D. N. (2018). Stackgan++: Realistic image synthesis with stacked generative adversarial networks. *IEEE transactions on pattern analysis and machine intelligence*, *41*(8), 1947-1962. https://doi.org/10.1109/TPAMI.2018.2856256

38. Kumar, K., Kumar, R., De Boissiere, T., Gestin, L., Teoh, W. Z., Sotelo, J., ... & Courville, A. C. (2019). Melgan: Generative adversarial networks for conditional waveform synthesis. *Advances in neural information processing systems*, *32*.

39. Kong, J., Kim, J., & Bae, J. (2020). Hifi-gan: Generative adversarial networks for efficient and high fidelity speech synthesis. *Advances in neural information processing systems*, *33*, 17022-17033.

40. Zhang, H., Goodfellow, I., Metaxas, D., & Odena, A. (2019, May). Self-attention generative adversarial networks. In *International conference on machine learning* (pp. 7354-7363). PMLR.

41. Dzhurov, A. A., Cherkesova, L. V., & Revyakina, E. A. (2023). Programmnoe sredstvo, opredelyayushchee feikovyj videokontent s pomoshch′yu tekhnologii Deepfake algoritma GAN. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli, 15*(4), 60-67.

42. Tampubolon, M. (2024). Digital face forgery and the role of digital forensics. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *37*(3), 753-767. https://doi.org/10.1007/s11196-023-10030-1

43. Karakoç, E., & Zeybek, B. (2022). Görmek inanmaya yeter mi? Görsel dezenformasyonun ayirt edici biçimi olarak siyasi deepfake içerikler. *Öneri Dergisi*, *17*(57), 50-72. https://doi.org/10.14783/maruoneri.908542

44. Chaitra, B., & Reddy, P. B. (2023). Digital image forgery: taxonomy, techniques, and tools–a comprehensive study. *International Journal of System Assurance Engineering and Management*, *14*(Suppl 1), 18-33. https://doi.org/10.1007/s13198-022-01829-5

45. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward: Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward. *Applied intelligence*, *53*(4), 3974-4026. https://doi.org/10.1007/s10489-022-03766-z

46. Nagm, A. M., Moussa, M. M., Shoitan, R., Ali, A., Mashhour, M., Salama, A. S., & AbdulWakel, H. I. (2024). Detecting image manipulation with ELA-CNN integration: a powerful framework for authenticity verification. *PeerJ Computer Science*, *10*, e2205. https://doi.org/10.7717/peerj-cs.2205

47. Vadrevu, A., Rajeshwari, R., Pabbathi, L., Sirimalla, S., & Vodnala, D. (2022). Image forgery detection using metadata analysis and ELA processor. In *Innovations in Computer Science and Engineering: Proceedings of the Ninth ICICSE, 2021* (pp. 579-586). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-8987-1_62

48. Shustova, E. P. (2020). Vvedenie v analiz izobrazhenij na Python. Kazan′. (in Russian).

49. Aggarwal, G., Srivastava, A. K., Jhajharia, K., Sharma, N. V., & Singh, G. (2023, November). Detection of deep fake images using convolutional neural networks. In *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)* (pp. 1083-1087). IEEE. https://doi.org/10.1109/ICTACS59847.2023.10389973

50. Kar, P., Xue, Z., Ardakani, S. P., & Kwong, C. F. (2022). Are fake images bothering you on social network? Let us detect them using recurrent neural network. *IEEE Transactions on Computational Social Systems*, *10*(2), 783-794. https://doi.org/10.1109/TCSS.2022.3159709

Поступила в редакцию
12.03.2026 г.

Принята к публикации
19.03.2026 г.

Ссылка для цитирования:

Утепкалиев М. А., Бояджы А. Сравнительный анализ инструментов создания и обнаружения поддельных изображений и представление гибридного метода // Бюллетень науки и практики. 2026. Т. 12. №5. С. 131-155. https://doi.org/10.33619/2414-2948/126/16

Cite as (APA):

Utepkaliyev, M., & Boyaci, A. (2026). Comparative Analysis of Tools for Creating and Detecting Fake Images and Presentation of a Hybrid Method. *Bulletin of Science and Practice, 12*(5), 131-155. (in Russian). https://doi.org/10.33619/2414-2948/126/16