

УДК 004.056.2:77

ПРОБЛЕМА ИДЕНТИФИКАЦИИ ФАЛЬСИФИКАЦИИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Г. А. Аптюкова, А. В. Никифоров, Т. В. Гавриленко

*Сургутский государственный университет,
aptjukova@rambler.ru, klgdante@gmail.com, taras.gavrilenko@gmail.com.*

В настоящее время благодаря разнообразному инструментарию программ очень просто модифицировать файлы. В данной статье авторами рассматриваются проблемы идентификации подлинности фото-, видео- или аудиофайлов.

Ключевые слова: цифровое изображение, фотография, видеозапись, фальсификация, идентификация.

IDENTIFICATION PROBLEM OF DIGITAL IMAGE ADULTERATION

G. A. Aptjukova, A. V. Nikiforov, T. V. Gavrilenko

*Surgut State University,
aptjukova@rambler.ru, klgdante@gmail.com, taras.gavrilenko@gmail.com.*

There are various tools currently helping to easily alter files. This paper considers genuineness identification problems of photo, video and audio files.

Keywords: digital image, photograph, video, adulteration, identification.

Развитие цифровых технологий повлекло за собой изменение формы жизни, трансформацию социальных отношений с новыми способами коммуникации, такими как социальные сети. Например, статистика показывает, что каждый день в Instagram публикуется 85 млн фото и видео [1].

Возрастающее количество производимых фотографий и видео связано с доступностью и распространением различных устройств для их создания: смартфоны, фотоаппараты, видеокамеры, веб-камеры, видеорегистраторы и т. д. Создание фотографии перестало быть чем-то, требующим специальных познаний и навыков, став неотъемлемой составляющей жизни современного человека.

Вместе с постоянным совершенствованием устройств для создания фотографий, совершенствуются и инструменты обработки изображений, которые имеют свою негативную сторону, поскольку упрощают процесс подделки изображений сторонними лицами.

Фальсификация цифрового изображения может производиться в политических, рекламных, зачастую корыстных целях. Известны примеры фальсификаций исторических фотографий (рис. 1) [2].



Рис. 1. Фальсификация исторических фотографий

Ретуширование фотографий можно встретить и на фотографиях современных мировых изданий. На рис. 2 в Иране запускают ракеты. На фальсифицированной фотографии одна из ракет дорисована (рис. 2) [3].



Рис. 2. Фальсификация современных фотографий

Фото-, видеозаписи могут служить поводом к возбуждению дела об административном правонарушении. К примеру, каждый гражданин Российской Федерации вправе обратиться с жалобой в ГИБДД на нарушителя правил дорожного движения, при этом доказательством нарушения является фотография или видеозапись. Существующие программные средства позволяют в цифровом изображении перенести объект, в данном случае автомобиль, на другой фон, к примеру, на тротуар. И такая фальсифицированная фотография, направленная в ГИБДД, в соответствии со статьей 12.19 Кодекса Российской Федерации об административных правонарушениях повлечет наложение административного штрафа в размере одной тысячи рублей на владельца автомобиля.

При этом, установленный Федеральным законом от 2 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и приказом МВД России от 12 сентября 2013 года № 707 «Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации» порядок рассмотрения обращений граждан не предусматривает проверку фотографий на подлинность.

В данном случае, проведение фототехнической экспертизы будет нецелесообразно для владельца автотранспорта, поскольку стоимость экспертизы значительно превышает стоимость административного штрафа. Доказательством недостоверности фото-, видеозаписи будет опять же фотография или видеозапись, что автомобиль в указанный период времени находился в другом месте.

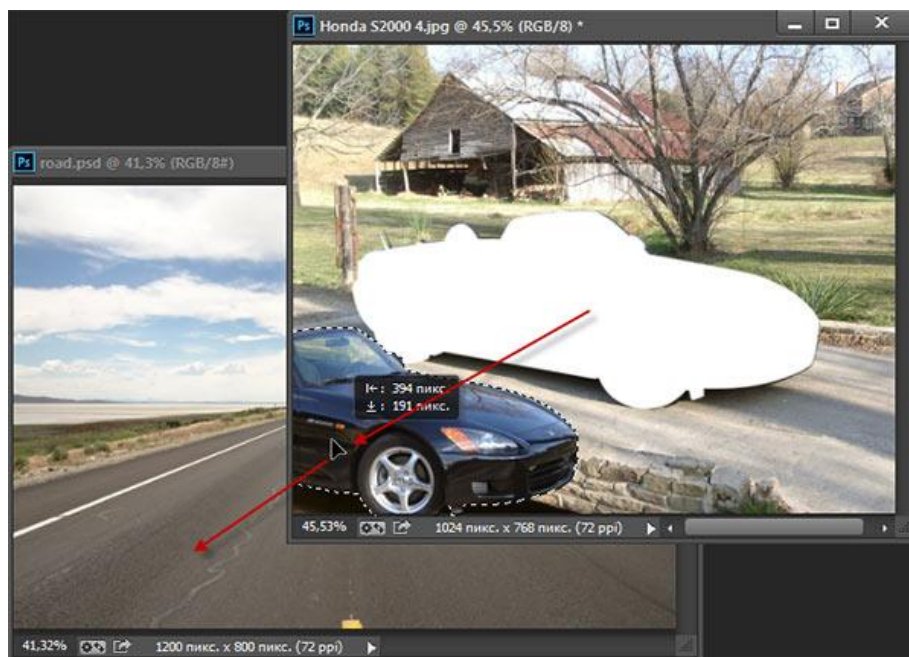


Рис. 3. Наложение автомобиля на другое изображение в Photoshop [4]

Записи с видеорегистратора автомобиля могут быть также изменены. На рис. 4 пример изменения видеозаписи, где убран дорожный знак «Уступите дорогу». Без знака перекресток становится равнозначным [5].



Рис. 4. Изменение видеозаписи

Компания Nvidia разработала алгоритм, использующий элементы искусственного интеллекта и способный значительно видеоизменять фотографии и видео. Эксперимент провели на роликах, полученных с автомобильных видеорегистраторов. Так, одно из исходных видео снималось зимой, а на обработанной версии алгоритм успешно превратил зиму в лето (рис. 5). Еще одно демонстрационное видео показывает, как день превратился в ночь (рис. 6) [6].

Для того, чтобы недобросовестные граждане не смогли отредактировать, изменить время и координаты съемки с видеорегистратора, будет создано приложение, на разработку которого правительство России выделит 2,5 млрд рублей. Правительство одобрило внесение в Госдуму проекта закона, который позволит гражданам самостоятельно фиксировать нарушения ПДД с помощью мобильного приложения. Материалы будут передаваться по мобильной связи в МВД для возбуждения дела [7].

Фотографии, изготовленные в ходе проведения следственных действий и оформленные в соответствии с требованиями действующего законодательства, могут иметь доказательственное значение в уголовном процессе. Каждое лицо, вовлеченное в процесс раскрытия и расследования преступления должно помнить и осознавать, что фотографии, фигурирующие по делу, могут быть фальсифицированы или подвергнуты сомнению [8].



Рис. 5. Изменение сезона на видео



Рис. 6. Искусственный интеллект меняет видео

И здесь ситуация обратная – есть доказательство виновности или невиновности в виде фото, видео- или аудиоинформации, но оно исключается из рассмотрения в деле, поскольку не удостоверяется подлинность представленных доказательств.

Именно фотографии являются основным доказательством, которое рассматривается страховыми компаниями в процессе возмещения ущерба застрахованных объектов. На сегодняшний день чаще всего с фальсификациями сталкивается сфера автомобильного страхования. Мошенники с помощью графических редакторов могут создать вполне реальное доказательство того, что их автомобиль разбит в ДТП. И наоборот, страхование разбитого автомобиля «задним числом», когда для страхования предоставляются фотографии автомобиля, измененные графическими редакторами в первоизданном виде (рис. 7) [9].

В 2011 г. для выявления фотомошенничества международной группой разработчиков, входящих в компанию SMTDP Tech, была создана программа Picture Manipulation Inspector. Однако этот проект не взлетел: вскоре выяснилось, что большинство страховых компаний собирают данные в непригодном для анализа формате (как правило, фото слишком сильно сжаты), а, чтобы организовать процедуру верификации, надо сначала перестроить всю систему работы с данными. В итоге бизнес по проверке документов для автостраховщиков так и не был запущен.

Для идентификации подлинности фото-, видео- или аудиофайлов классические способы, используемые в криптографии, не подходят. Это связано с тем, что при пересылке фото-,

видео- или аудиофайла через Интернет, происходит перекодирование исходного файла. Процесс перекодирования применяется для более эффективной передачи файла через Интернет. Однако после пересылки мы получаем не оригинальный файл, а его измененную копию. Далее на примере фотографии будет разобрано, какие проблемы создает перекодирование при идентификации фотографии и как оно влияет на характеристики исходного изображения.



Рис. 7. Страхование автомобиля задним числом

Первая проблема, возникающая при перекодировании, состоит в том, что оригинальная фотография имеет палитру типа RGBA, а после пересылки по Интернету палитра меняется на HSLA или другую. И как следствие последовательность байт кодирующая, один и тот же цвет, изменяется. Это изменение приводит к различным значениям хэш-суммы. Поэтому становится невозможным применение алгоритма расчета хэш-суммы для подтверждения подлинности.

Вторая проблема заключается в изменении кодов цветов на границе соприкосновения. В качестве примера возьмем коды двух цветов с оригинальной фотографии (рис. 1). Первый код: RGBA (255,198,24,1) и второй код: RGBA (255,24,214,1). Два этих цвета соприкасаются друг с другом на границе. Границу соприкосновения можно представить в виде прямой или кривой линии (рис. 8).

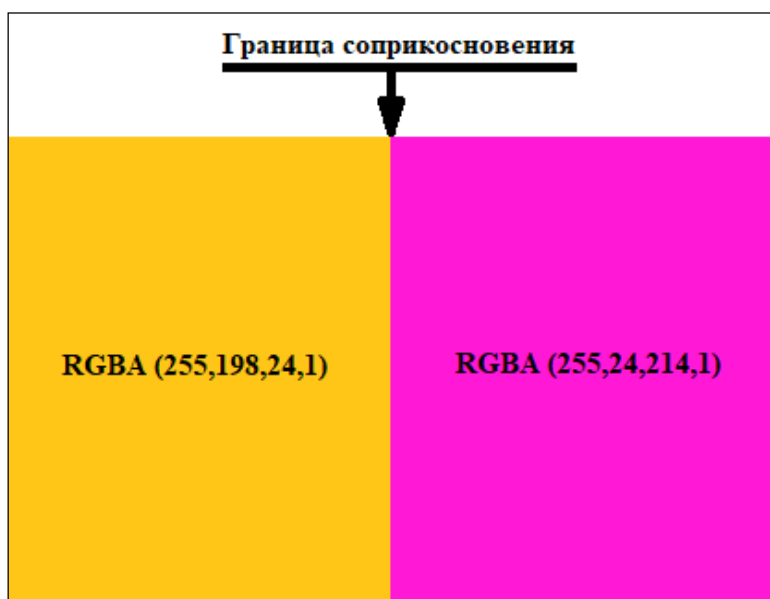


Рис. 8. Граница соприкосновения цветов

После пересылки и перекодирования фотографии по Интернету происходит изменение кодов цветов на границе соприкосновения. Первый код: RGBA (250,198,24,1) и второй код: RGBA (255,29,214,1). Становится очевидно, что один или несколько параметров, задающих цвет, были изменены в ходе перекодирования. Если изменяется только один параметр, то происходит создание нового оттенка на границе. При изменении нескольких параметров, то на границе соприкосновения может получиться даже новый цвет. Но для человеческого глаза все эти изменения останутся незамеченными. Достоверно рассчитать хэш-сумму также будет невозможно, так как в последовательности байт произошли изменения, не являющиеся посторонним вмешательством.

Третья проблема – это изменение общего размера исходного файла. Эта проблема является следствием первых двух. Возможное изменение типа палитры и количества байт, отводимых под один цвет, приводит к увеличению общего размера файла. Появляющиеся новые цвета на границе соприкосновения создают новые коды цветов, которые требуется хранить в исходном файле. Это также приводит к увеличению общего размера файла. Нельзя использовать хэш-сумму для идентификации подлинности фотографии, так как количество исходных байт для расчета хэш-суммы постоянно изменяется.

Из-за выше перечисленных проблем классические методы криптографии не будут корректно работать для определения достоверности фотографий. Поэтому требуется разработать новые методы идентификации, которые бы учитывали данные проблемы в процессе анализа фотографий на достоверность.

Литература

1. Интернет-статистика 2017 года: мобильный трафик, электронная коммерция, социальные сети, реклама и поисковые системы [Электронный ресурс]. URL: <https://sdvv.ru/articles/elektronnaya-kommertsiya/internet-statistika-2017-goda-mobilnyy-trafik-elektronnaya-kommertsiya-sotsialnye-seti-reklama-i-poi/> (дата обращения: 10.12.2017).
2. Глумов Н. И., Кузнецов А. В. Обнаружение на изображениях искусственных изменений локального происхождения // Автометрия. 2011. Т. 47. № 3. С. 4–12.
3. Самые известные фотофальсификации (51 фото + текст) [Электронный ресурс]. URL: <https://dezinfo.net/foto/6917-samyie-izvestnyie-fotofalsifikacii-51-foto-tekst.html> (дата обращения: 23.01.2018).
4. Наложение автомобилей на другое изображение в Photoshop [Электронный ресурс], URL: <https://rugraphics.ru/photoshop/nalozhenie-avtomobiley-na-drugoe-izobrazhenie> (дата обращения: 23.01.2018).
5. Улыбнитесь, вас снимает камера фиксации // Доброе утро. [Электронный ресурс]. URL: <https://www.1tv.ru/shows/dobroe-utro/reportazh/ulybnites-vas-snimaet-kamera-fiksacii-dobroe-utro-fragment-vypuska-ot-18-10-2017> (дата обращения: 23.01.2018).
6. Nvidia научила искусственный интеллект подделывать фотографии и видео [Электронный ресурс]. URL: <https://hitech.newsru.com/article/05dec2017/nvidia> (дата обращения: 23.01.2018).
7. Власти разрабатывают мобильное приложение для фиксации нарушений ПДД [Электронный ресурс]. URL: <https://og.ru/society/2017/10/06/91876> (дата обращения: 23.01.2018).
8. Криминалистическое обеспечение раскрытия и расследования преступлений : материалы X Всерос. науч.-практ. круглого стола, 26 февраля 2016. Ставрополь : СФ КрУ МВД России, 2016. Ч. 1. 258 с.
9. Северюхин Я. Осторожно, фотомошенничество! // Современные страховые технологии. 2014. № 1. С. 60–65.