

МЕТОДЫ ВЕРИФИКАЦИИ ПОЛЬЗОВАТЕЛЬСКОГО ФОТО- И ВИДЕОКОНТЕНТА В ЖУРНАЛИСТИКЕ

И. А. Королев

*Белорусский государственный университет,
ул. Кальварийская, 9, 220004, г. Минск, Республика Беларусь,
Iakorolev1996@gmail.com*

*Научный руководитель – В. П. Воробьев, кандидат филологических наук,
доцент*

Стремительное развитие социальных медиа и все возрастающие объемы пользовательского контента, представленного в основном в формате фотографий и видеозаписей, актуализируют значимость верификации журналистами визуальной информации. Выявление базовых методов верификации пользовательских фотографий и видеозаписей в значительной мере способствует стандартизации и повышению оперативности журналистской деятельности в данном направлении.

Ключевые слова: методы верификации; пользовательский контент; постобработка фотографий; анализ метаданных.

METHODS OF VERIFICATION OF USER-GENERATED PHOTO AND VIDEO CONTENT IN JOURNALISM

I. A. Korolev

*Belarusian State University,
9, Kalvariyskaya Str., 220004, Minsk, Republic of Belarus
Corresponding author: I. A. Korolev (Iakorolev1996@gmail.com)*

Research advisor – V. P. Vorobiev, candidate of Philology, associate professor

The rapid development of social media and the increasing volumes of user-generated content, presented mainly in the format of photographs and videos, actualize the importance of verification of visual content by journalists. The identification of basic methods for verifying user-generated photos and videos will vastly contribute to the standardization journalistic practice in this direction and increase in the speed of verification user-generated content.

Key words: verification methods; user-generated content; post-processing; metadata analysis.

В эпоху повсеместной технологизации и медиатизации общества у журналистов все реже возникает необходимость добывать информацию непосредственно с места событий. Роль журналистов постепенно смещается от информаторов к верификаторам новостного контента, создателями которого в основном выступают пользователи социальных медиа. Большие объемы пользовательского контента (user-generated content), основным форматом которого являются фотографии и видеозаписи, актуализируют необходимость разработки системы методов его верификации, способной стандартизировать задачи журналиста, помочь сотрудникам СМИ быстрее и качественнее устанавливать достоверность информации.

Анализ академической и специализированной литературы, среди которой «Руководство по верификации» (К. Силверман, Р. Цубаки), руководство для академической и профессиональной подготовки журналистов «Журналистика, “фейковые новости” и дезинформация» (Ш. Айртон, Дж. Позетти), «Расширенное руководство по верификации видеоматериалов» от Bellingcat, а также статьи «К проблеме верификации фотографий в современных медиа» (О. А. Бакулин, М. А. Ромакина), «Способы и средства обеспечения анонимности в глобальной сети Интернет» (Д. С. Карпов), «Как установить подлинность фото и понять, какая часть кадра была отфотошоплена. FotoForensics» (Л. Белая), «Debunking photo-fakes: Advice for image verification» (C. Albeanu), «Verifying Video» (M. Browne), «Spot faked photos using digital forensic techniques» (S. Horaczek), «Photojournalism in the Age of New Media» (J. Keller), позволяет выявить существующие методы проверки фотографий/видеозаписей и на их основании создать систему базовых методов верификации пользовательского контента.

1. Первичный анализ пользовательского контента.

Несмотря на то что верификация пользовательского контента зачастую предполагает использование технических инструментов, немаловажным фактором успешности установления достоверности фотографий/видеозаписей остается их первичный анализ. Данный метод позволяет журналисту уже на этапе ознакомления с материалом отыскать вызывающие сомнения в подлинности детали, среди которых «внутренняя согласованность любых видимых теней (т.е. находятся ли тени там, где мы их ожидаем, и соответствуют ли они источникам света» [1, с. 108], неестественные отражения в зеркалах, стеклах, лужах, зрачках или их отсутствие, а также несоответствие между визуальным контентом и комментарием к нему. Данный метод позволяет журналисту сконцентрировать свое внимание на анализе конкретных деталей, что способствует повышению скорости установления достоверности визуального контента.

2. Идентификация автора/создателя контента.

Одним из основных принципов работы с информацией является коммуникация с ее источником для получения подробностей. Непосредственный контакт с автором фотографии/видеозаписи в значительной мере способствует установлению ее подлинности. В случае верификации пользовательского контента журналист может не только связаться с загрузившим контент пользователем, но и прибегнуть к анализу его учетной записи: часто об онлайн-источнике доступно гораздо больше информации, чем, например, о традиционном источнике, звонящем по горячей линии [2]. Уже беглое изучение страницы пользователя, в частности, просмотр основной информации, анализ частоты публикаций и истории аккаунта, может не только дать представление о том, является ли страница «живой» или более походит на фейк, но и предоставить дополнительные контактные данные (телефон или аккаунты в других социальных сетях).

При коммуникации с автором контента журналист может выяснить: кто автор и где в данный момент находится; когда и при каких условиях он попал на место создания фотографии/видеозаписи; что он видел на месте создания фотографии/видеозаписи (и что показывает его снимок/видео). В случае верификации фотографии журналист резонно может попросить у источника предоставить дополнительные снимки, так как маловероятно, что в ситуации, заслуживающей освещения в СМИ, очевидец ограничится единственной фотографией. Точность и конкретность ответов на вопросы журналиста, а также готовность предоставить дополнительный материал – основные индикаторы того, что источник информации действительно является автором контента.

3. Поиск «интернет-следа» верифицируемого контента.

Следующим базовым методом верификации пользовательского контента является определение того, появлялась ли запрашиваемая фотография/видеозапись в Сети ранее, то есть поиск «интернет-следа» верифицируемого объекта.

В случае верификации фотографий осуществить данную задачу можно в программах, организующих поиск обратного изображения. Наиболее популярными в русскоязычном пространстве Сети инструментами, обладающими необходимым для решения данной задачи функционалом, являются относящиеся к поисковым системам сервисы Google Reverse Image Search и «Яндекс.Картинки», а также сервис TinEye, при помощи которого пользователь может не только найти более ранние версии изображения, но и определить, где оно появилось впервые.

Способы поиска «интернет-следа» видеозаписей в целом схожи с описанными выше способами анализа фотографий. Специалисты Bellingcat рекомендуют начинать поиск интернет-следа видеозаписи с обратного поиска изображений, представляющих собой скриншоты и миниатюры из видео, так как «в настоящее время в свободном доступе нет инструментов, которые позволили бы искать целиком все видео» [3]. Эффективность данного инструмента зависит от качества миниатюры: наиболее перспективным является поиск контрастных или имеющих характерную цветовую гамму изображений [2].

Вторым вариантом поиска видеозаписи является поиск по ключевым словам (например, именам, топонимам, акронимам) из названия или описания файла. При использовании данного метода удобным инструментом являются фильтры, которыми располагают основные видеохостинги (в частности, YouTube, Vimeo, YouKu), так как они позволяют найти самую раннюю версию искомого видео («миниатюры оригинального и “вырезанного” видео обычно совпадают» [2]).

4. Анализ метаданных визуального контента.

Метаданные, также называемые EXIF-данными (exchangeable image file format) представляют собой встроенную в файл информацию о его свойствах и признаках. Метаданные хранят информацию о том, когда было выполнено изображение или видеозапись, на какое устройство и при каких его настройках (в случае фотографий), а также могут содержать геоданные и информацию о том, «как изображение было отредактировано в редакторе» [4, с. 61]. Обладая неоспоримыми преимуществами, данный метод имеет и существенные ограничения, в частности, метаданные автоматически стираются у загружаемого в социальные медиа фото- и видеоконтента, а также поддаются редактированию в специализированных программах. Отметим, что проблема с очисткой метаданных может быть решена в том случае, если на этапе коммуникации с автором визуального контента журналисту удалось получить от него оригинальный, содержащий метаданные снимок или видеозапись.

5. Проверка фотографии/видеозаписи на предмет постобработки.

Распространенным методом анализа фотографий на предмет редактирования является анализ уровня ошибок (error level analysis): «если изображение не подвергалось постобработке, оно будет однородным, без ярко выраженных светлых, темных или радужных областей» [5]. Анализ уровня ошибок позволяет определить «наиболее измененные фрагменты изображения» [5], то есть найти места, которые, вероятно, подвергались фотомонтажу. Одним из популярных инструментов, позволяющих произ-

вести анализ уровня ошибок является сайт Fotoforensics.com (название переводится с английского как «фотокриминалистика»). По утверждению разработчиков, инструмент «стремится упростить процесс анализа. Он работает как микроскоп – выделяя артефакты и детали, которые человеческий глаз не в состоянии идентифицировать» [6]. При этом создатели сайта напоминают пользователям, что анализ изображений представляет собой сложную многоаспектную задачу, «нет решения с одной кнопкой, которое скажет вам, является ли изображение реальным или измененным» [6].

Важно отметить, что, как и в случае с метаданными снимков, социальные сети не сохраняют информацию об уровне ошибок, стирая ее при загрузке. Следовательно, журналисты, работающие с загруженными в социальные сети снимками, не имеют возможности установить их подлинность при помощи анализа уровня ошибок.

Наиболее популярными общедоступными инструментами анализа видеозаписей на предмет монтажа и иных манипуляций являются программы для редактирования видеозаписей Adobe Premier и Vegas. Например, сфальсифицированное канадскими студентами видео о том, как парящий в монреальском парке орел подхватывает когтями ребенка и несколько метров проносит его над землей, было опровергнуто путем разделения видео на отдельные кадры и обнаружения того факта, что на некоторых кадрах отсутствовала тень орла [2].

Таким образом, систему базовых методов верификации пользовательских фотографий/видеозаписей составляют следующие методы: первичный анализ; идентификация автора/создателя контента; поиск «интернет-следа»; анализ метаданных; установление факта постобработки фотографии/видеозаписи. Так как сегодня не существует единственно правильного подхода к установлению достоверности пользовательского контента, а работа над его проверкой представляет собой анализ совокупности доказательств правдивости/ложности рассматриваемого объекта и принятие на их основе решения о публикации/не публикации материала в СМИ, обращение к представленной системе методов является необходимым условием для реализации журналистом полноценного анализа достоверности пользовательского контента.

Библиографические ссылки

1. Ireton C., Posetti J. Journalism 'Fake News' & disinformation: handbook for journalism education and training UNESCO. 2018 [Electronic resource]. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000265552> (data of access: 01.12.2022).

2. *Browne M.* Verifying Video [Electronic resource]. DataJournalism.com. URL: <https://datajournalism.com/read/handbook/verification-1/verifying-video/5-verify-ing-video> (data of access: 01.12.2022).
3. Расширенное руководство по верификации видеоматериалов [Электронный ресурс]. Bellingcat.com. 2017. URL: <https://ru.bellingcat.com/materialy/putevoditeli/2017/07/18/advanced-video-verification-guide> (дата обращения: 01.12.2022).
4. *Карнов Д. С., Ибрагимова З. А.* Способы и средства обеспечения анонимности в глобальной сети // Правовая информатика. 2021. №. 3. С. 60–67.
5. *Белая Л.* Как установить подлинность фото и понять, какая часть кадра была отфотошоплена. FotoForensics [Электронный ресурс]. Sdelano.media. URL: <https://sdelano.media/fotoforensics>. 2018 (дата обращения: 01.12.2022).
6. Tutorial: Using FotoForensics [Electronic resource]. Fotoforensics.com. URL: <https://clck.ru/33JFaF> (data of access: 01.12.2022).