Издаётся с 1924 года

РАДИО®

9•2020

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Радиолюбитель"—"Радиофронт"—"Радио"

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.

Регистрационный ПИ № ФС77-50754

Главный редактор В. К. ЧУДНОВ

Редакционная коллегия:

А. В. ГОЛЫШКО, А. С. ЖУРАВЛЁВ, А. Н. КОРОТОНОШКО, К. В. МУСАТОВ, И. А. НЕЧАЕВ (зам. гл. редактора), Л. В. МИХАЛЕВСКИЙ, С. Л. МИШЕНКОВ, О. А. РАЗИН

Выпускающие редакторы: С. Н. ГЛИБИН

Обложка: В. М. МУСИЯКА

Вёрстка: Е. А. ГЕРАСИМОВА

Корректор: Т. А. ВАСИЛЬЕВА

Адрес редакции: 107045, Москва, Селивёрстов пер., 10, стр. 1

Тел.: (495) 607-31-18. Факс: (495) 608-77-13

E-mail: **ref@radio.ru**

Группа работы с письмами — (495) 607-08-48

Отдел рекламы — (495) 607-31-18; e-mail: **advert@radio.ru**

Распространение — (495) 607-77-28; e-mail: **sale@radio.ru**

Подписка и продажа — (495) 607-77-28

Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — ЗАО "Журнал "Радио", ИНН 7708023424,
р/сч. 40702810438090103159
Банк получателя — ПАО Сбербанк г. Москва
корр. счёт 30101810400000000225 БИК 044525225

Подписано к печати 24.08.2020 г. Формат 60×84 1/8. Печать офсетная.

Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.

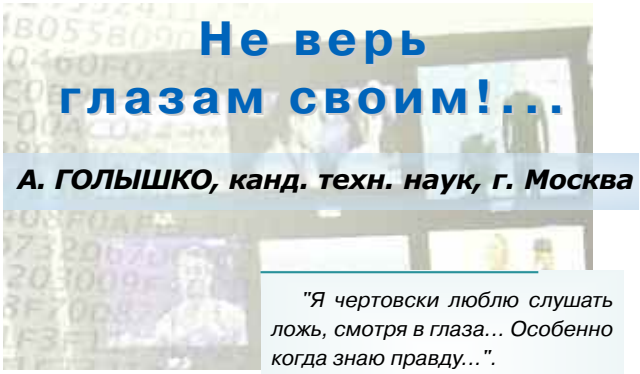
В розницу — цена договорная.

Подписной индекс:

Официальный каталог ПОЧТА РОССИИ — П4014;

КАТАЛОГ РОССИЙСКОЙ ПРЕССЫ — 89032.

Отпечатано в ОАО «Подольская фабрика офсетной печати»
142100, Моск. обл., г. Подольск, Революционный проспект, д. 80/42.
Зак. 02345-20.



Не верь глазам своим!..

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Я чертовски люблю слушать ложь, смотря в глаза... Особенно когда знаю правду...".

Адриано Челентано

Продолжая начатый в прошлом номере журнала разговор о видеотехнологиях и распознавании лиц, отметим один из последних трендов, направленный ровно в противоположную сторону. Компания IBM отказалась от разработки ПО и оказания услуг по распознаванию лиц на фоне массовых протестов в США. Глава IBM заявил, что компания не хочет развивать технологии, которые могут быть использованы "для массового наблюдения и нарушения базовых прав и свобод человека", и предложил обсудить возможность запрета на их использование правоохранителями. Американская корпорация Microsoft отказалась продавать полиции США свою технологию распознавания лиц, пока в стране не разработают соответствующее законодательство. Зато китайская компания LLVision Technology Co разработала солнечные смарт-очки для полицейских, которые внешне похожи на Google Glass, оборудованы камерой и связаны с базой данных правоохранительных органов. Чтобы проверить личность подозрительного человека, полицейскому надо посмотреть на него с расстояния не больше пяти метров и с ракурса, при котором видно не менее 70 % лица. Система распознавания лиц автоматически начнёт искать совпадения в базе данных. На поиск потребуется 2...3 мин. Если совпадение будет найдено, система сообщит имя и домашний адрес человека.

Таким образом, с одной стороны, появились некие сомнения в массовом использовании технологии распознавания лиц, а с другой — "поезд" продолжает идти вперёд. Всё это выглядит достаточно забавно, когда выясняется, что сегодня с помощью видеотехнологий лица можно не только распознавать, но и синтезировать. К примеру, как теперь многим понятно, широкополосный Интернет — это, прежде всего, видео в HD-качестве на распространённых платформах, которые постепенно заменяют для граждан новостные ленты, аналитику и просто развлекательное чтиво. А ещё это инструмент влияния на миллиарды людей, позволяющий создавать нужное в данный момент общественное мнение. Сегодня, когда планета плотно опутана информационными каналами, влиять можно с помощью новостей, причём, когда это необходимо, поддельных.

Сам термин fake news (поддельные новости) не нов, потому что поддельные новости существовали всегда. Ещё в XIII веке до н. э. цари Египта и Хеттского государства начертали на камнях своих дворцов сообщения о победе в битве, которая на самом деле завершилась вничью. Ну а в XX веке с поддельной новости о захвате радиостанции началась Вторая мировая война. Что же касается новостей дня сегодняшнего, то, как говорится, пробу ставить негде.

Фейковые новости влияют на политику больших стран, а их создатели зарабатывают немалые деньги, используя различные схемы монетизации. Fake news смогут сокрушать политиков и бизнесы. Но сейчас мы не будем изучать тех, кто создаёт фейковые новости, как организуют поддельные информационные кампании, и зачем им, собственно, это всё. Очевидно, вы и сами догадываетесь.

Однако на пике всех этих игр с гражданами может оказаться ещё более изощрённая технология deep fake, которая уже не раз доказала свою способность превратить каких-нибудь знаменитостей, к примеру, в звёзд порноиндустрии.

Deep fake (дипфейк) — это алгоритм, позволяющий моделировать поведение и внешность человека на видеозаписи. Имя технология получила от сочетания deep learning (глубокое обучение) и fake (подделка). Это реалистичная манипуляция аудио- и видеоматериалами с помощью искусственного интеллекта (ИИ). Последний использует синтез человеческого изображения, т. е. объединяет несколько картинок, на которых человек запечатлён с разных ракурсов и с разным выражением лица, и делает из них видео. Анализируя фотографии, специальный алгоритм учится тому, как выглядит и может двигаться человек. На самом деле работают две нейросети. Первая генерирует образцы изображения, а вторая отвечает за то, чтобы отличать настоящие образцы от поддельных. Технологию можно сравнить с работой двух фальшивомонетчиков, один из которых подделывает купюры, а второй пытается отличить эти подделки от оригиналов. В случае, если второй обнаруживает подделку, изображение отсылается первому, который улучшает свою работу, предлагая более реалистичную подделку.

Технология deep fake "заставляет" говорить человека то, что он не произносил, и делать то, что он никогда не делал. В её основе лежат нейронные сети, работающие по генеративно-состязательному принципу (Generative Adversarial Network — GAN). Это алгоритмы на базе машинного обучения, способные генерировать новый контент из заданного набора. Например, GAN может изучить тысячу фотографий Барака Обамы и создать свою, сохраняя все черты и мимику экс-президента. Алгоритмы, заложенные в базу программы, постоянно соревнуются друг с другом в двух процессах: обучение на представленных фотографиях с целью создания реальной подмены лица на копии и исключение негодных вариантов до тех пор, пока машина сама не начнёт путать оригинал и копию. В этой сложной схеме заключается основная цель работы deep fake — создание ложных фотографий и видеоконтента, в которых лицо оригинала замещается другим образом.

Различные методы манипулирования изображениями появились ещё в XIX веке и в XX веке применялись в кинофильмах. Эти методы стремительно улучшились с появлением цифрового видео. Технология deep fake возникла в 2014 г. в умелых руках студента Стэнфордского университета Яна Гудфеллоу. Ничего плохого Ян не имел в виду, однако через три года пользователь (кстати, его ник — Deepfakes) социального новостного сайта Reddit начал с помощью этой технологии заменять лица порноактрис знаменитостями. Тут и началось...

После этого Reddit ужесточил свои правила в распространении контента, а за всеми подобными роликами со звуковой и/или видеоманипуляцией закрепилось название дипфейки. Кстати, недавнее исследование показало, что 96 % дипфейков в Интернете — порноролики. Очевидно, фантазии у их создателей хватает преимущественно только на это. В последнее время подделки начали привлекать повышенное внимание благодаря использованию в финансовых махинациях, розыгрышах и, разумеется, фальшивых новостях.

Помимо порнографии, пользователи в Интернете интересуются ещё и политикой. В сети есть несколько дипфейков с политическими деятелями, где их выступления монтировали и меняли смысл высказывания. По Интернету гуляют якобы пьяная Нэнси Пелоси, якобы Трамп, выступающий против климатических инициатив, а также якобы Обама, который в одном из роликов называет Трампа complete dipshit (засранцем). Разумеется, в реальности никто из этих персонажей ничего подобного не делал, однако доказать, "что ты не верблюд", сразу не получается.

Распространение ложной информации, вторжение в частную жизнь, разрушение репутации — только малая часть того, к чему могут привести дипфейки. Именно поэтому, по мнению палаты представителей конгресса США, они представляют угрозу национальной безопасности страны. Законодатели обеспокоены тем, как эта технология повлияет и на очередную предвыборную кампанию, и на политическую обстановку в целом. Кстати, Калифорния стала первым штатом, где на законодательном уровне запретили распространение дипфейков с кандидатами во время предвыборной гонки.

Впрочем, любые технологии сами по себе не могут быть хорошими или плохими — главное, как их используют. В Интернете достаточно развлекательных роликов с дипфейками. К примеру, на YouTube-канале Ctrl Shift Face сменяются лица главных героев фильма на других известных голливудских актёров, где Сильвестр Сталлоне становится Терминатором, Брюс Ли исполняет роль Нео в "Матрице", а Джим Керри вместо Джека Николсона играет главную роль в "Сиянии". С распространением таких роликов появилась опасность дискредитации любого пользователя, фото которого есть в Интернете. Первыми под огонь попали публичные личности, изображений которых достаточно много в открытом доступе. Как очень точно высказался однажды Роберт Шекли: "Самое обидное, что в информационной войне всегда проигрывает тот, кто говорит правду. Он ограничен правдой, а лжец может нести что угодно".

Крупные корпорации Google, Facebook, Microsoft пытаются бороться с распространением фейковых видео, чтобы уметь отсекать нежелательные сразу же после появления. Создаются соответствующие инструменты, с помощью которых разработчики могут тренировать алгоритмы для обнаружения дипфейков. Вот Facebook не так давно анонсировала конкурс с призовым фондом 10 млн долл. на лучшую программу, распознающую фейковые видео.

Есть примеры использования дипфейков и в рекламе. В частности, Бекхэм снялся в социальном ролике об опасностях малярии, а технологии помогли ему заговорить на девяти разных языках. Носители языка произносили текст, а ИИ подстраивал видео под артикуляцию Бэкхема. Впрочем, авторы рекламы предпочитают называть это видео синтезом, а не дипфейком, чтобы избежать негативных сравнений. Кстати, пока тренда использования данной технологии в рекламе нет. В массовом сознании дипфейки — это информационное оружие. Именно поэтому для ведущих брендов использование дипфейков несёт серьёзный репутационный риск.

Разумеется, технология пока неидеальна. В частности, имеют место мимические артефакты — нереалистичные движения, монотонность речи. Поскольку все движения лица генерируются неидеальным ИИ, некоторые из них получаются неестественными. Впрочем, их можно скорректировать, но тогда, возможно, нереалистичными станут другие элементы мимики. Даже короткий видеоролик содержит огромное количество таких мимических движений, поэтому требуется очень качественно обученный ИИ, чтобы на большом объёме не допускать ошибок. Видео с применением дипфейков выглядят убедительно только в течение 2...3 с, но они (во всяком случае пока) далеки от того, чтобы обмануть пользователей. Если присмотреться к таким роликам внимательней, то можно заметить, что, например, подрисованные лица на видео не моргают. Эффект постоянно открытых глаз связан с недостатками процесса создания таких роликов. Дело в том, что среди картинок, по которым обычно учится нейросеть, не так много (на самом деле их почти нет) фотографий с закрытыми глазами. Пользователи вряд ли хранят или выкладывают в сеть неудачные фото, на которых они моргают. Но ведь ИИ постоянно совершенствуется и с морганием что-нибудь "придумает".

Чтобы уверенно распознать дипфейк, учёные из Университета Олбани провели эксперимент, в котором выявили, что в среднем люди моргают 17 раз в минуту. Это число увеличивается до 26 раз во время разговора и падает до 4,5 раза во время чтения. Эти же учёные предложили свой метод распознавания фейковых видеороликов, объединив две нейронные сети, для того чтобы более эффективно распознавать ненастоящие лица. Как выяснилось, нейронные сети часто упускают спонтанные и непроизвольные физиологические действия. Например, дыхание во время речи или движение глаз.

Несомненно, при росте числа дипфейков будет расти и чувствительность аудитории к различным несовершенствам. Возможно, благодаря этому идея найти дипфейк и станет основной для коммуникации ИТ-компании или новостного агрегатора. Впрочем, рядовому

пользователю всё сложнее отличить смонтированное видео от настоящего. Но, по мнению экспертов, уже очень скоро технологии достигнут такого уровня, что смонтированное видео уже будет невозможно отличить от оригинала и экспертам. Учитывая количество фото, которые граждане "заливают" в социальные сети, недостатка в материале для дипфейков не предвидится. Проблема в том, что в будущем пользователям, которые не смогут доказать, что их не было на определённом видео, может, например, грозить тюремный срок. К тому же подобные видео могут быть как безобидными, так катастрофически опасными с точки зрения появления оскорблений той или иной этнической или религиозной группы граждан. И даже рекламные сюжеты с нестареющими или вечно живыми звёздами используются сейчас не так часто отнюдь не из-за технологических проблем (наложением 3D-модели оригинала и пластическим гримом актёра можно сконструировать видео даже без всякого дипфейка), а из-за неразрешённых этических вопросов, не говоря уже о наследниках и пр.

Несмотря на все изложенные выше риски, технология дипфейк всё же имеет большой потенциал, если, конечно, её правильно использовать. Учитывая, что создать качественный дипфейк на обычном компьютере непросто, существует достаточно много инструментов, доступных в Интернете, чтобы помочь людям сделать это.

В частности, есть приложение Doublicat. Несколько секунд — и ваше лицо будет наложено на лицо Брэда Питта, Леонардо Ди Каприо или Тейлора Свифта, причём ваше наложенное лицо будет почти так же гримасничать, как и оригинал. По словам разработчиков приложения, само изображение удаляется с серверов сразу после его обработки.

Приложение FaceApp, разработанное российской компанией Wireless Lab, использует нейронные сети для генерации высокореалистичных преобразований лиц на фотографиях. Приложение может преобразить ваше лицо, чтобы заставить его улыбаться, выглядеть старше, выглядеть моложе или просто для смены пола, а также многих других занятных преобразований. Татуировки, виньетки, размытие объектива и наложение фона также являются частью FaceApp. В 2018 г. приложение привлекло много внимания со стороны трансгендерных и ЛГБТ-сообществ из-за его реалистичных преобразований гендерных изменений. Но приложение столкнулось с критикой как в социальных сетях, так и в прессе за нарушение конфиденциальности пользовательских данных.

С помощью инструмента Deepfakes web β можно создавать видео в Интернете за 2 долл. в час. Обучение здесь немного объёмнее, чем в других приложениях. Для начала нужно зарегистрироваться и загрузить свои видео. Всё остальное происходит в облаке, где используются мощные графические процессоры. На изучение видеоизображений и смену лиц уходит почти четыре часа. Также можно использовать обученную модель, чтобы менять лица, это занимает около 30 мин. Разумеется, доступ к своим видео и учебным данным можете получить только вы.

Приложение DeepFaceLab является ведущим ПО для создания подделок, которое использует новые нейронные сети для замены лиц в видео. Приложение размещено на GitHub и породило бесчисленное множество видео в Интернете. По словам его разработчиков, более 95 % глубоких подделок видео создаются с помощью DeepFaceLab. Его используют несколько популярных каналов YouTube, таких как Ctrl Shift Face, iFake и Shamook. DeepFaceLab работает с высоким качеством, но для его использования необходимо иметь технические знания.

FaceSwap похож на DeepFaceLab, но предоставляет больше возможностей, лучшую документацию и лучшую онлайн-поддержку. В отличие от вышеприведённых инструментов, рассчитанных на Android и iOS, он также доступен на Mac и Linux. Это инструмент с открытым исходным кодом, наполненный функциональностью для выполнения каждого шага процесса deep fake, от импорта первоначального видео до создания финального видео. Чтобы запустить этот инструмент, необходима мощная видеокарта, так как замена лица происходит крайне медленно. Работая на Python, Keras и Tensorflow, Faceswap имеет активное сообщество, поддерживающее и разрабатывающее ПО. Соответственно существует много учебников, которые помогут вам начать работу.

Технология глубокой подделки мультимедиа Zao позволяет модулировать голоса знаменитостей и накладывать своё лицо на тело актёра в сцене. Достаточно просто нажать на одну фотографию, чтобы попробовать тысячи модных причёсок, одежды и макияжа. Приложение предоставляет множество видеоклипов, нарядов и буквально неограниченные возможности для изучения. В 2019 г. Zao за короткое время приобрёл значительную популярность, позволив пользователям обмениваться лицами с любимыми актёрами в коротких клипах из телепередач и фильмов. За месяц он стал самым загружаемым бесплатным и во многом удовлетворяющим честолюбие приложением в Китае. С ростом популярности его разработчики также столкнулись с критикой политики конфиденциальности приложения. Всего несколько секунд понадобится, чтобы поменять ваше лицо, но так как алгоритм в основном обучен на китайских лицах, это может выглядеть не совсем так, как ожидается.

В целом все вышеприведённые инструменты демонстрируют, как быстро развивался базовый ИИ. То, что раньше требовало тысячи картинок, чтобы сделать достаточно убедительное глубокое поддельное видео, теперь требует наличия только одного изображения и при этом демонстрирует лучшие результаты.

Мировой рынок мультимедиа вплотную подошёл к предоставлению таких видеосервисов, как "герой по запросу" и "сюжет по запросу". Иначе говоря, сегодня потенциально каждый зритель по своему желанию может получить тех героев видеосюжета, которых захочет, и задать такие повороты сюжета, которые затронут тончайшие струны его души (естественно, при наличии последних). Даже при минимальном воображении нетрудно представить, какие сюжеты и какие замены действующих лиц при этом возможны (мы его не любим — заменим его лицом какого-нибудь отрицательного героя). Стоит заметить, что для появления указанных сервисов гораздо больше необходимы определённые вычислительные мощности и наличие соответствующего ИИ.

Что касается высочайшего качества, то это по-прежнему удел профессионалов. Скажем, ещё десять лет назад Джеймс Кэмерон, который занимает одно из ведущих мест в мировой кинофантастике, снял свой "Аватар", где около 80 % видеоряда было анимацией, тщательным образом подогнанной под реальность (в том числе и в 3D). Фильм снимался долго, но результат был весьма хорош и вызвал настоящий шок. И неспроста "Аватар" был выдвинут американской киноиндустрией на премию "Оскар" сразу по семи номинациям. Тем больший шок вызвало присуждение фильму лишь одного приза и отнюдь не за режиссуру и технологию изготовления, а за работу оператора. В чём дело?

Несколько лет назад об этом уже приходилось писать, но в данном случае неплохо и повторить в связи с развитием и продвижением в массы технологии deep fake. В тот момент Джеймс Кэмерон предвосхитил день сегодняшний и убедительно показал, что внешность киногероям может быть придана абсолютно любая без потери качества во всех смыслах, а это означает, что уже в скором времени не будет нужды в так называемых высокооплачиваемых "звёздах" с их капризами, скандалами, пластическими операциями и пр. Мужественные, нежные, соблазнительные, гадкие и смазливые будут созданы компьютером, в котором вместо Джеймса Кэмерона будет трудиться нужным образом ориентированный ИИ. Дело будет лишь в быстродействии и цене такого компьютера, но отнюдь не в сидящем за ним человеке. Учитывая стремительный прогресс, долго ждать коммерчески выгодных предложений не придётся. Что же касается американских киноакадемиков, это далеко неглупые люди, которые просто увидели в "Аватаре" смерть всего того, чем жила и живёт мировая киноиндустрия. Какой уж тут "Оскар", если завтра буквально каждая кухарка...

Ну вы понимаете...

По материалам ***new-science.ru, topwar.ru, informburo.kz, www.sostav.ru, millionstatusov.ru***