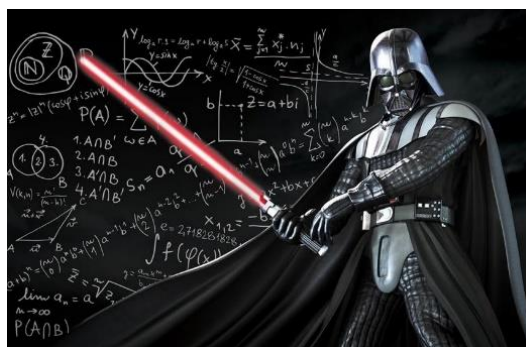


Эти нейросети

Уязвимости нейросетевых технологий



Афанасьев Сергей

КБ «Ренессанс Кредит»

24.10.2020

1. Как обмануть системы распознавания лиц?

Нейронные сети кажется уже навсегда вошли в нашу жизнь, являясь одновременно и нашими помощниками, и угрозами, и некоторой магией – а как же это все-таки работает? Наши смартфоны оснащаются различными системами биометрии, в основе которых лежат нейронные сети – распознавание лиц, отпечатки пальцев, распознавание радужки глаз и другие. Мы начинаем цикл постов, которых расскажем об уязвимостях нейросетевых технологий.

Известный писатель-фантаст Артур Кларк как-то сказал:

«Если знаменитый, но старый ученый утверждает, что нечто возможно, он почти определенно прав. Если он утверждает, что нечто невозможно, он, очень вероятно, ошибается»

Если перевести эту цитату на наш бизнес язык, то должно звучать примерно так:

«Если известные эксперты или крупные компании заявляют, что нечто невозможно – они, очень вероятно, ошибаются»

Собственно эту мысль мы будем эксплуатировать далее на практических примерах. Но сначала давайте попробуем разобраться – как работает фотобиометрия.

Пару лет назад в небольшой американском городе Ланкастер произошла необычная бытовая история. В полицию обратились пострадавшие покупатели, которых на местном рынке обманывал мошенник. Пока продавцы отлучались от своих прилавков, мошенник представлялся хозяином прилавка, брал деньги с покупателей и исчезал. Один из свидетелей нарисовал очень схематичный портрет мошенника, но уже на следующий день полиция поймала преступника.



В заявлении ведомства говорилось: «Хоть портрет, предоставленный свидетелем, мог показаться неумелым и карикатурным, он, вместе с описанием физических особенностей

подозреваемого, помог сотруднику полиции вспомнить его имя». Преступником оказался бездомный по имени Хунг Фыок Нгуен.



Да, возможно портрет преступника получился очень схематичным и не все черты лица похожи, но какое-то сходство с оригинальной фотографией все-таки есть.

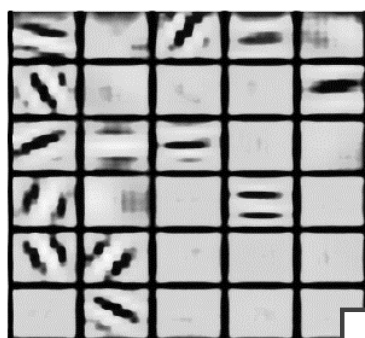
Примерно так работает наш мозг, когда распознает лица – нам не нужна глубокая детализация, достаточно каких-то неуловимых грубых паттернов. И примерно также работают фотобиометрические системы, в основе которых лежат сверточные нейронные сети.

**Если вы можете прочесть это,
вы можете прочитать хошу рбту
с всякой зрпль!**

Принципы работы сверточных нейронных сетей достаточно простые – есть слои сверток и есть слои пулинга, с помощью которых выделяются контрастные участки на фотографиях. За счет такой архитектуры нейросеть обрабатывает контуры на изображении лица, не вдаваясь в глубокую детализацию.

В результате обработки изображения нейросеть формирует несколько карт признаков. Первая карта содержит набор простых черточек. Вторая – более сложных линий. Следующая карта, более высокого уровня, выделяет целые формы – глаз, ухо, нос и прочее. И так далее до полных лиц.

Карта признаков 1



Карта признаков 2



Карта признаков 3



Такая архитектура нейронной сети позволяет добиться очень высокой точности распознавания лиц за счет двух основных свойств:

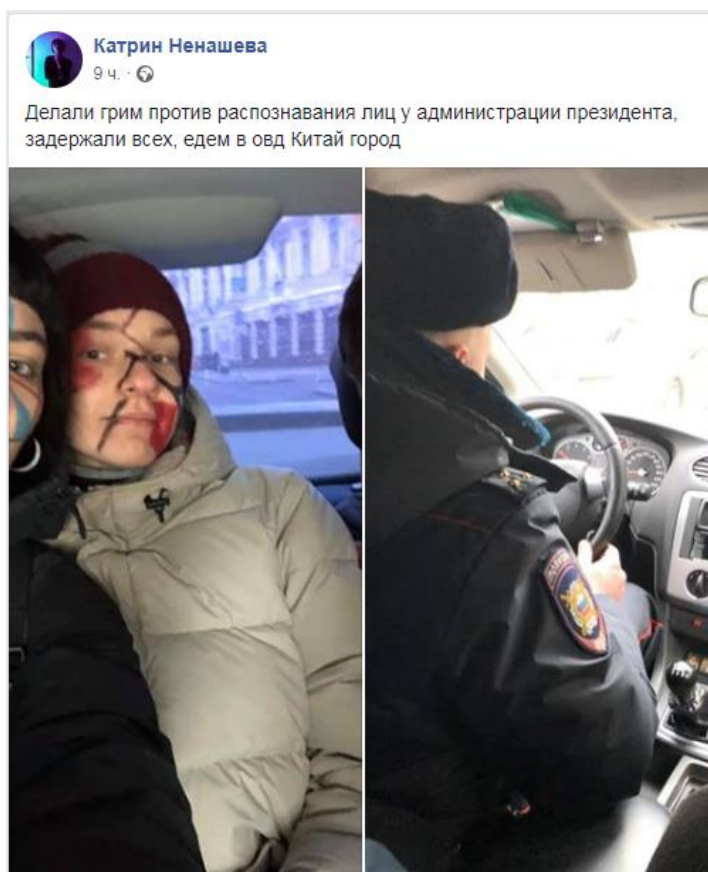
1. Первое свойство – это иерархичность. Операция «свертки» позволяет создавать иерархичные карты признаков: от черточек к сложным объектам;
2. Второе свойство – это отсеивание шумов с помощью операции «пулинг».

Итак, подытоживая, мы теперь знаем, что сверточная нейронная сеть обрабатывает контуры на изображении лица, не вдаваясь в глубокую детализацию.

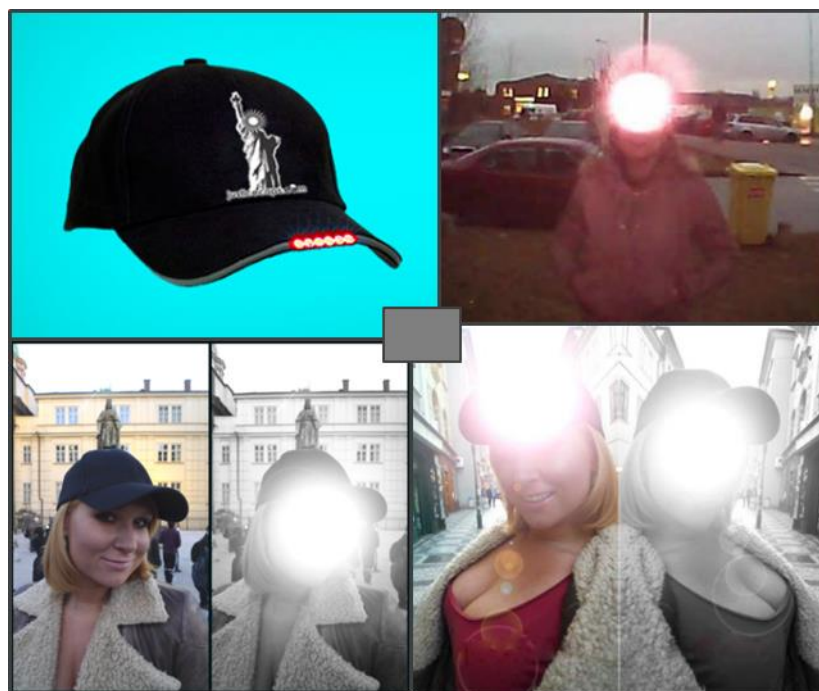
Григорий Бакунов из компании Яндекс, хорошо понимающий эти принципы, придумал алгоритм, генерирующий случайный макияж, который ломает системы распознавания лиц. Принципы работы алгоритма те же, что у сверточных нейронных сетей – на лицо добавляется несколько ярких полосок или точек, которые нейросеть считает за контуры лица. В результате нейронка не может сравнить разрисованное лицо с базовой фотографией.






Таким способом Григорий Бакунов продемонстрировал, что системы распознавания лиц уязвимы и легко обходятся. Но с таким макияжем вы вряд ли придете в банк, и вам вряд ли одобряют кредит. Более того, такой макияж уже стал объектом внимания полицейских и скоро возможно станет вне закона.



Способы обмана систем распознавания лиц были придуманы еще до Григория Бакунова. Например, в 2014 году в продаже появилась бейсболка Justice Cap, оснащенная светодиодами, которые засвечивали лицо для фото и видео камер. Это очень простой и эффективный способ скрыться от видеонаблюдения. И стоила такая кепка всего 15\$ долларов.

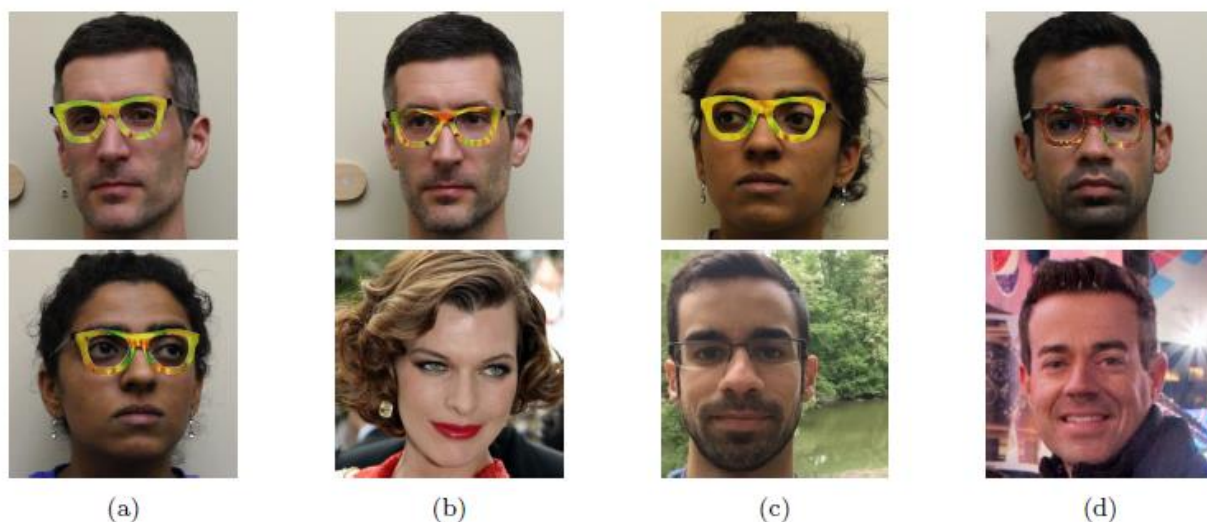


В 2015 году американский математик Ян Гудфелоу разработал алгоритм для атаки на нейронные сети, распознающие объекты на фотографиях. Он добавил к фотографии панды специально сгенерированный шум и получил изображение, которое нейронная сеть распознавала как гиббона, хотя человеку по-прежнему видел панду на обработанной фотографии.

	$+ .007 \times$		$=$	
x		$\text{sign}(\nabla_x J(\theta, x, y))$		$x + \epsilon \text{sign}(\nabla_x J(\theta, x, y))$
“panda”		“nematode”		“gibbon”
57.7% confidence		8.2% confidence		99.3 % confidence

Этот пример стал хрестоматийным для научных исследований и показал темную сторону генеративно-сопоставительных нейронных сетей (которые, кстати, тоже придумал Гудфелоу).

Годом позже исследователи из Университета Карнеги-Меллона (США) продолжили развивать идеи Гудфелоу и предложили с помощью нейросетей генерировать специальный принт для оправы очков. Цель была та же – обойти системы распознавания лиц. Разработанная нейронная сеть позволила подбирать специальные принты, которые делают из человека любую выбранную знаменитость (или другого человека). Например, один из исследователей, надев такие очки, стал для фотобиометрической системы Милой Йовович.



Еще спустя год на одной из выставок дизайнер Дзинь-Цай Лю предложила надевать на голову портативный проектор, который проецирует на лицо человека другое лицо. И хотя это был арт-проект без практической реализации, эту идею позже подхватили китайские исследователи.



Проектор для лица (Источник: Jing-cai Liu)

В 2018 году инженеры из Фуданьского университета и компании Алибаба предложили использовать инфракрасные светодиоды для взлома систем распознавания лиц. Для этого они прикрепили светодиоды на нижнюю часть козырька обычной кепки. Принцип работы достаточно простой: инфракрасные лучи, падающие на лицо человека, образуют пятна, которые не видны человеческому глазу, но фотокамера их отлично ловит. В результате на систему распознавания лиц отправляется фотография с пятнами, которую нейросеть не может сравнить с базовой фотографией.

Кроме простого взлома, инженеры разработали сложный режим работы светодиодов. Они обучили модель, которая обманывает Open Source фотобиометрию FaceNet от компании Google. Разработанная учеными модель оптимизирует несколько параметров: яркость луча, угол наклона луча и диаметр пятна. В результате можно загрузить фотографию жертвы и алгоритм выдаст оптимальные параметры калибровки светодиодов, чтобы фотобиометрия FaceNet распознала на фото жертву, а не мошенника. Для людей с похожим типом внешности (раса, пол и т.д.) точность прохождения фотобиометрии за жертву составила около 70%.



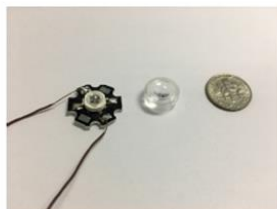
1. Кепка со светодиодами



2. Батарейка



4. ШИМ-плата для управления яркостью



3. Светодиод и линза



5. Три линзы для подбора диаметра луча

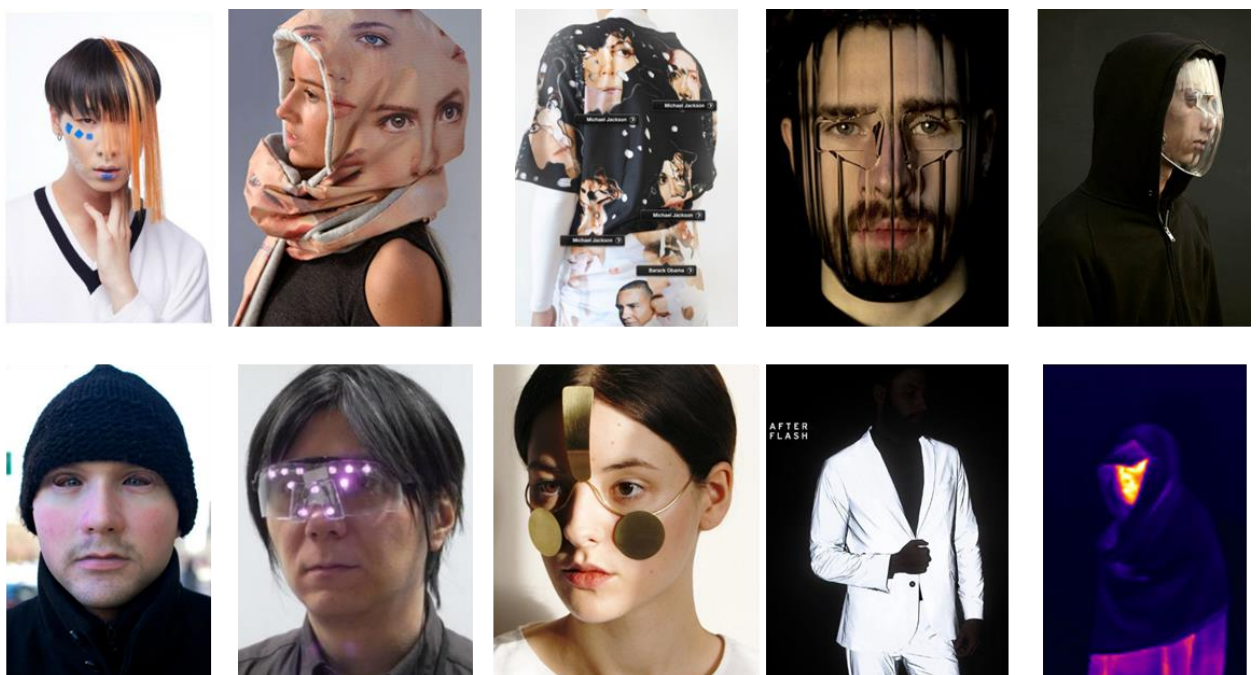
Такую кепку можно сделать и собственными руками, закупив комплектующие в обычном магазине электроники. Единственным неудобством такой кепки является то, что инфракрасный свет оставляет ожоги на коже человека. Поэтому исследователи не рекомендовали носить кепку с работающими светодиодами более одной минуты.

Несмотря на то, что атаки на нейронные сети могут использовать и преступники, ученые пытаются найти в этих разработках добрую миссию – например, использовать атаки на нейронные сети как борьбу с «Большим братом». Так, недавно чикагские инженеры бросили вызов технологическим компаниям, собирающим фотографии о пользователях в интернете с целью последующей перепродажи этих данных полицейским ведомствам и частным компаниям.



Ученые разработали инструмент под названием Fawkes (Фокс), который маскирует фотографии для защиты от фотобиометрических систем. Исследователи смогли обмануть системы распознавания лиц от Amazon, Microsoft и китайской технологической компании Megvii. Всего за месяц Fawkes скачали больше 50 тысяч раз с сайта для разработчиков. Сейчас инженеры работают над бесплатной версией для массового пользователя.

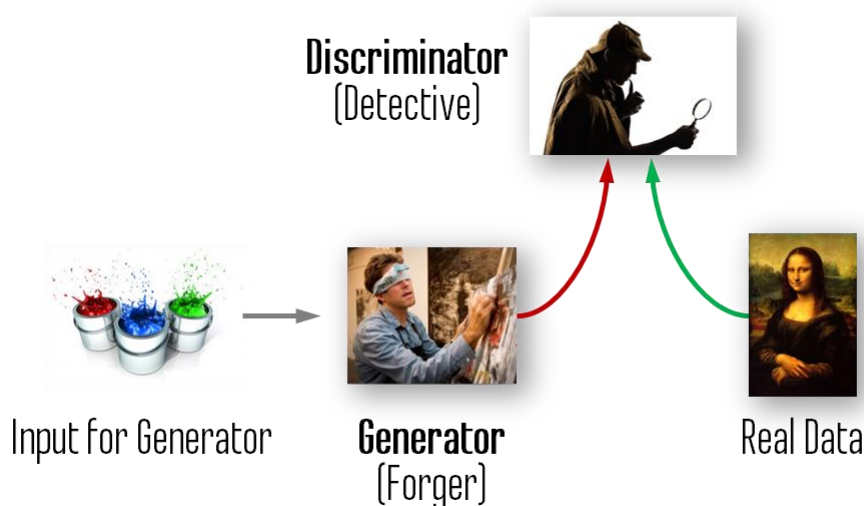
За несколько лет существования фотобиометрических систем было придумано множество способов их взлома: специальный макияж, платки и накидки с лицами других людей, стеклянные преломляющие маски, накладные маски с чужим лицом, очки со светодиодами и даже светоотражающая одежда (например, костюм с вкраплением светоотражающих нитей, из-за которых на фото виден только сам костюм).



Итак, обмануть системы распознавания лиц оказалось не очень сложно, если использовать специальный макияж, очки или кепку со светодиодами. Но макияж и очки – это все детские шалости по сравнению с тем, что умеют делать генеративно-состязательные сети.

Генеративно-состязательные сети (**GAN**) были предложены американским математиком Яном Гудфеллоу в 2014 году (который потом с помощью таких сетей сделал из панды гиббона). Принцип работы ГАНа достаточно простой: сеть состоит сразу из двух нейронных сетей – генератора и дискриминатора. Задача генератора создавать искусственные данные (фотографии, голоса, мелодии и т.п.), а задача дискриминатора попытаться отличить сгенерированные данные от настоящих. Таким образом при обучении ГАНа происходит некоторая антагонистическая игра – генератор пытается обмануть дискриминатор, а дискриминатор пытается выявить этот обман. За счет такой соревновательной концепции с помощью ГАНов получается генерировать данные очень высокого качества.

Generative Adversarial Network



ГАНы быстро стали популярными и нашли свое применение в таких приложениях как PRISMA, MSQRD, виртуальный макияж ModiFace, виртуальная примерочная Wannaby и другие.

Но также быстро проявилась и темная сторона ГАНов. В конце 2017 года на ресурсе Raddit пользователь под ником **Deepfakes** выложил несколько видео низкого социального содержания, в которых лица действующих героинь были заменены на голливудских звезд.

Всего через пару месяцев, в январе 2018 года, в интернете появилось приложение **FakeApp**, с помощью которого можно было подставлять лицо любого человека в любое видео. Причем для работы в приложении не нужно было обладать навыками программирования или специальными знаниями о нейронных сетях – любой пользователь мог создать свой дипфейк (почему-то больше всех в этих экспериментах досталось Николасу Кейджу).

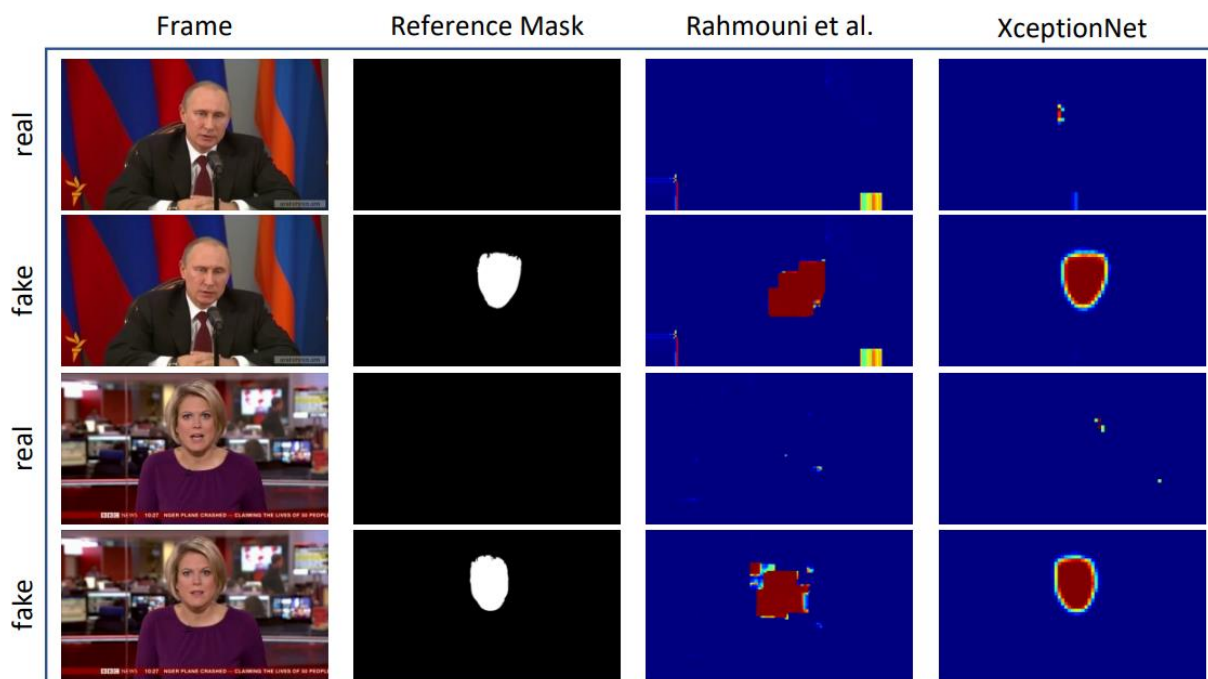


Однако в первой версии **FakeApp** для создания качественного дипфейка требовалось загружать несколько фотографий лица человека, снятого с разных ракурсов, а рендеринг видео мог отрабатывать всю ночь. При этом в любительских дипфейках было много графических артефактов.

В 2019 году израильские ученые решили проблему низкой скорости разработки дипфейков, предложив нейронную сеть **FSGAN**, которая позволяет в режиме реального времени заменять лица на видео, не требуя для этого длительной обработки. Авторы разработки утверждают, что в отличие от предыдущих подходов deepfakes их метод работает для любых двух лиц без какой-либо специальной обработки изображений (проверено на Николасе Кейдж!).



Сразу после появления дипфейков началась борьба снаряда и брони. В 2018 году немецкие и итальянские ученые разработали нейросеть **XceptionNet**, которая умеет выявлять подмену лиц на фото или видео. По точности распознавания XceptionNet превосходила существующие на тот момент алгоритмы в несколько раз даже при оценке на сжатых видео. Интересно, что это исследование спонсировалось агентством DARPA департамента обороны США.



Антидипфейк нейронки применяются и для защиты фотобиометрических систем как одна из разновидностей **Liveness Detection** – технологии, которая позволяет убедиться, что перед фотокамерой находится живой человек, а не заранее сделанная фотография или видеозапись.

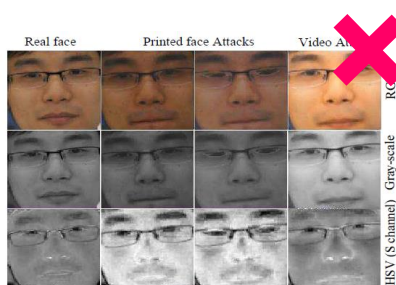
Есть несколько видов **Liveness Detection** для фотобиометрических систем:

1. **Интерактивное подтверждение** – когда человека просят подмигнуть на камеру, или улыбнуться, или покачать головой. Причем, чтобы это действие не было предварительно записано на видео, система просит выполнить его из случайно выбранных. Такая защита легко обходится, например, с помощью кепки с инфракрасными светодиодами, о которой я рассказывал в предыдущем посте: перед камерой будет стоять живой человек с инфракрасными пятнами на лице. Также интерактивное подтверждение можно обойти с помощью дипфейков, которые позволяют «приклеивать» лицо другого человека в реальном времени (аналог анимоджи для смартфонов).
2. **Анализ текстур** – позволяет выявлять дипфейки и распознавать, что фотография сделана с плоского изображения. Обходится с помощью все той же кепки со светодиодами.
3. **3D-камера** – тоже считается технологией Liveness Detection, хотя по сути является 3D-фотобиометрией, которой оснащены, например, iPhone X. Такую защиту сложнее обойти, чем интерактив или текстуры, но, к сожалению, 3D-камеры тоже уязвимы.

Интерактив



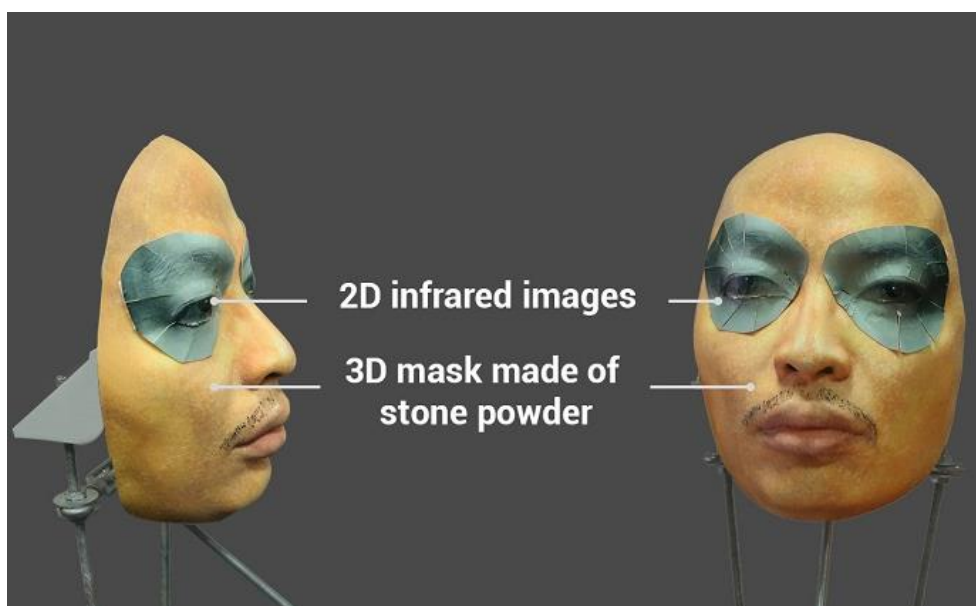
Текстуры



3D-камеры



Уязвимость 3D-фотобиометрии продемонстрировали вьетнамские инженеры из компании Вкав, занимающиеся технологиями кибербезопасности. Всего через пару недель после релиза iPhone X они продемонстрировали как можно взломать FaceID с помощью маски, напечатанной на 3D-принтере. Для этого понадобилось предварительно отсканировать лицо владельца смартфона с помощью 3D-сканера. Первая версия маски состояла из четырех компонент: напечатанная на 3D-принтере основа, 2D изображение глаз, силиконовый нос и специально рассчитанные области лица. Вторая версия маски была упрощена до двух компонент: каменная 3D-основы и 2D-изображение глаз.



После публикации этой новости некоторые специалисты по кибербезопасности утверждали, что такой подход не масштабируем, поскольку нужно долго сканировать лицо владельца смартфона. И возможно они действительно были бы правы, если бы к тому моменту не придумали ГАНы.

В 2016 году инженеры из Массачусетского технологического института (MIT) разработали нейронную сеть **3D-GAN**, которая позволяет восстанавливать 3D-модели высокого качества по 2D-изображению. Если обучить такую нейросеть на фотографиях лиц, можно создать 3D-маску любого человека, фотографию которого можно достать, например, из социальных сетей.

Learning a Probabilistic Latent Space of Object Shapes via 3D Generative-Adversarial Modeling

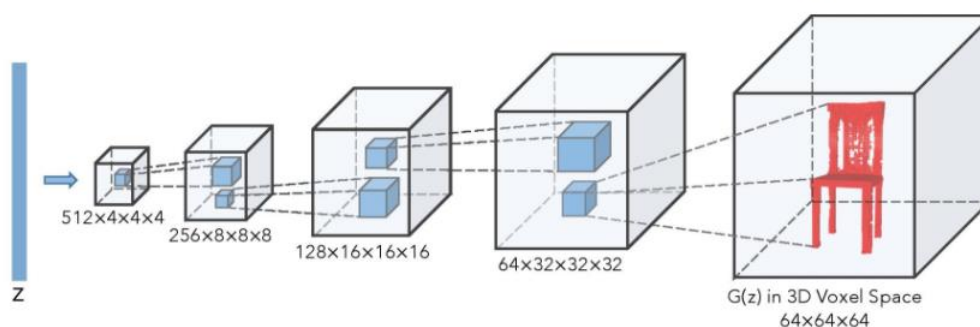
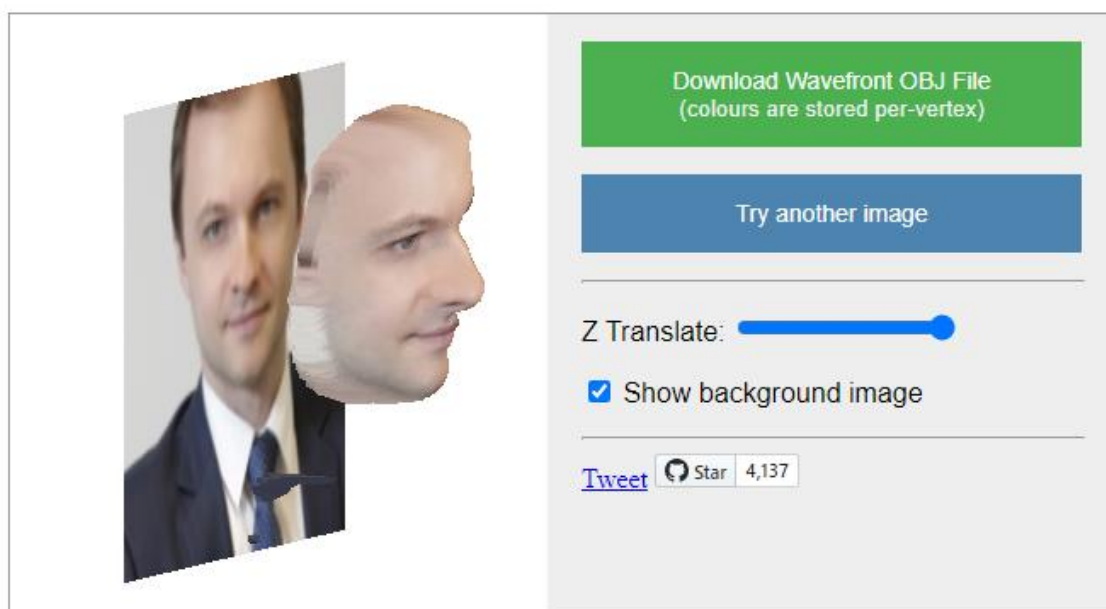


Figure 1: The generator of 3D Generative Adversarial Network (3D-GAN)



Figure 2: Shapes synthesized by 3D-GAN

Уже в 2017 году британские ученые развили эту идею и разработали нейронную сеть **VRN**, которая создает 3D-маску человека всего по одной фотографии. Разработку выложили в открытый доступ, а демо-версию работы этой нейросети можно протестировать по этой ссылке: <http://www.cs.nott.ac.uk/~psxasi/3dme/>



Возможно, что восстановленные с помощью нейронных сетей 3D-маски пока еще не достаточно точные по сравнению с масками, созданными с помощью 3D-сканеров. Но мы помним, что свёрточные нейронные сети, лежащие в основе фотобиометрии, выделяют

очень грубые признаки без глубокой детализации (иначе человек не смог бы пройти фотобиометрию повторно).

После взлома FaceID специалисты из компании Вкав в своем блоге описали другой способ масштабирования взлома 3D-биометрии: 3D-маску можно воссоздавать, снимая фотографию с двух камер, расположенных со сдвигом (стереосъемка). Примерно так и работает большинство 3D-сканеров.

На этом можно закончить с обзором методов взлома систем распознавания лиц. В следующей части узнаем, как можно обойти голосовую биометрию.

Источники:

1. <https://lancaster.crimewatchpa.com/lbop/node/57727>
2. <https://novayagazeta.ru/articles/2017/07/18/73156>
3. <https://oddtymall.com/justice-caps-hide-your-face-from-surveillance-cameras>
4. <https://arxiv.org/pdf/1412.6572.pdf>
5. <https://www.cs.cmu.edu/~sbhagava/papers/face-rec-ccs16.pdf>
6. <http://jingcailiu.com/wearable-face-projector/>
7. <https://arxiv.org/pdf/1803.04683.pdf>
8. <http://sandlab.cs.uchicago.edu/fawkes/>
9. <https://gagadget.com/how-it-works/56165-bolshoj-brat-ne-usledit-kak-v-mire-nauchilis-obmanyivat-sistemyi-raspoznavaniya-lits/>
10. https://meduza.io/news/2020/02/09/u-administratsii-prezidenta-zaderzhali-chetyreh-chelovek-s-grimom-protiv-raspoznayuschih-litsa-kamer?utm_source=facebook&utm_medium=main
11. <https://fakeapp.site/>
12. <https://arxiv.org/pdf/1908.05932.pdf>
13. <https://arxiv.org/pdf/1803.09179.pdf>
14. <https://arxiv.org/pdf/1511.06316.pdf>
15. http://www.bkav.com/dt/top-news/-/view_content/content/103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions
16. http://3dgan.csail.mit.edu/papers/3dgan_nips.pdf
17. <http://www.cs.nott.ac.uk/~psxasj/3dme/>

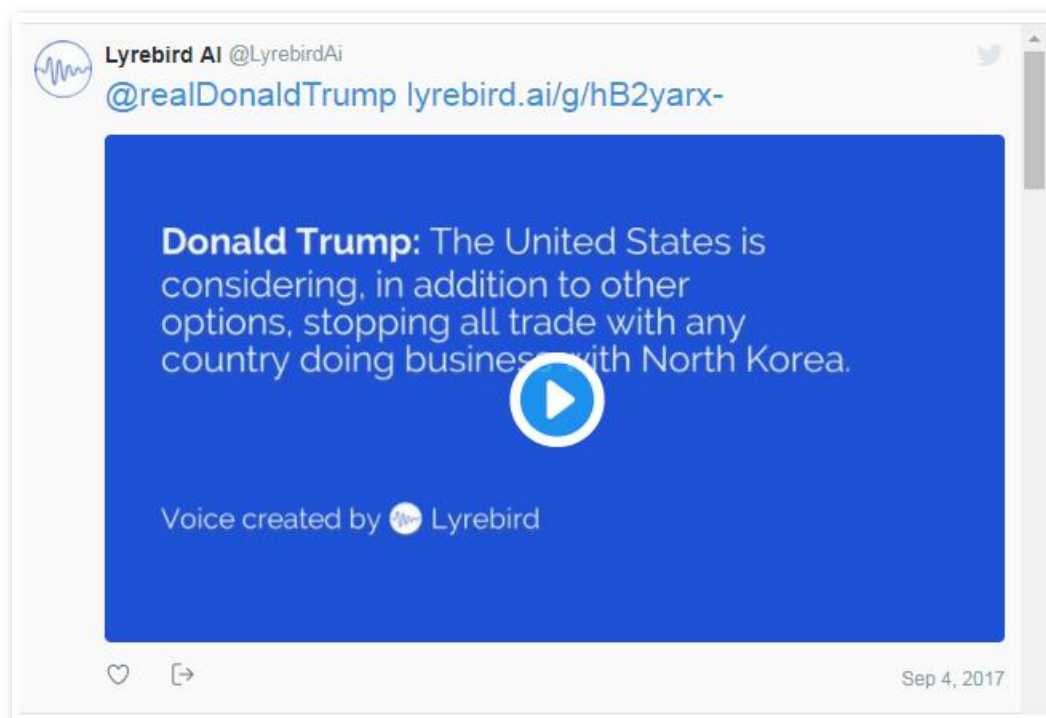
2. Как взломать голосовую биометрию?

В предыдущей части было показано как обойти защиту систем распознавания лиц, а также была немного затронута тема дипфейков. Создать свой дипфейк может сейчас любой человек, используя, например, мобильное приложение Reface. Хочется предупредить безнадежных романтиков – дипфейки уже начинают регулироваться законом, поэтому официальные приложения работают по принципу fair use (добросовестное использование) и имеют ряд ограничений и защит – например, запрет на анонимное использование, наличие вотермарок, скрытых меток и т.п.

В этом разделе узнаем как взламываются системы распознавания голоса. Вообще взломом чужого голоса начали заниматься еще до появления нейронных сетей. Среди российских экспертов по клонированию чужого голоса самими известными считаются Владимир Винокур и Максим Галкин. Но мы поговорим о более современных технологиях, которые можно легко масштабировать.

В 2017 году в интернете появился проект **Lyrebird AI**, который позволяет генерировать речь по загруженному слепку голоса. Через год разработчики открыли доступ к API проекта и воспользоваться этой технологией мог уже любой желающий. Григорий Бакунов из Яндекса (который придумал специальный макияж для взлома фотобиометрии) в своем телеграмм-канале тогда писал:

«TNW с испугом пишет о потенциале проекта Lyrebird для преступников. Эта система позволяет загрузить минуту своего голоса, а потом получить текст-тупич с голосом, похожим на ваш. Автор прав, сделать из, скажем, 2-3 часов речи очень приличный TTS можно, причем для этого подойдут уже готовые опенсорсные технологии.»



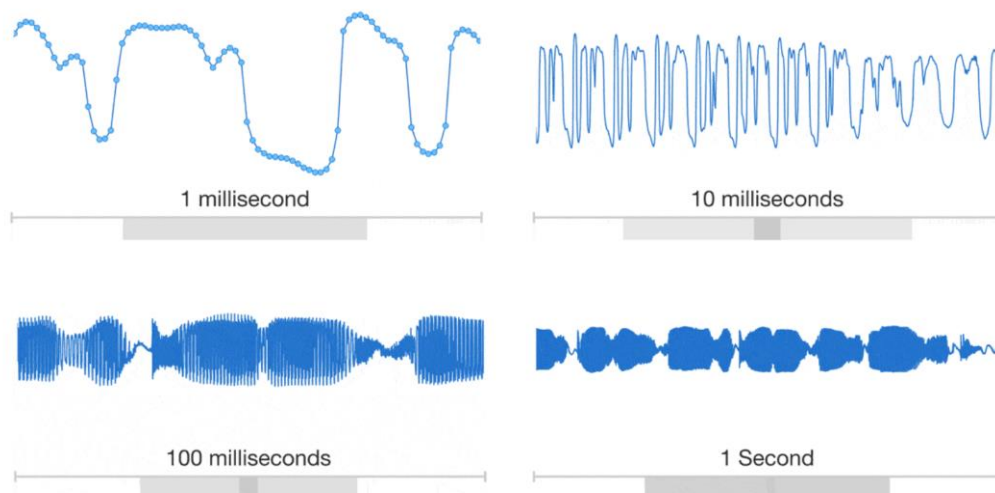
Сейчас на рынке есть уже несколько проектов, позволяющих клонировать чужой голос:

- [Resemble.AI](#) – предоставляется демоверсия программы;
- [iSpeech](#) – есть демоверсия для 27 языков, включая русский;
- [Lyrebird AI](#) – можно загрузить демоверсию на 3 часа речи;
- [Vera Voice](#) – проект от компании Screenlife Technologies и команды проекта «Робот Вера».

Технология клонирования голоса может стать реальной угрозой для систем голосовой биометрии – когда по загруженному слепку голоса человека мошенники смогут генерировать любую речь: например, ответы на вопросы оператора банка где используется голосовая биометрия. И хотя голосовые слепки сложнее достать, чем, например, фотографии из социальных сетей, такие технологии будут использоваться в различных мошеннических схемах.

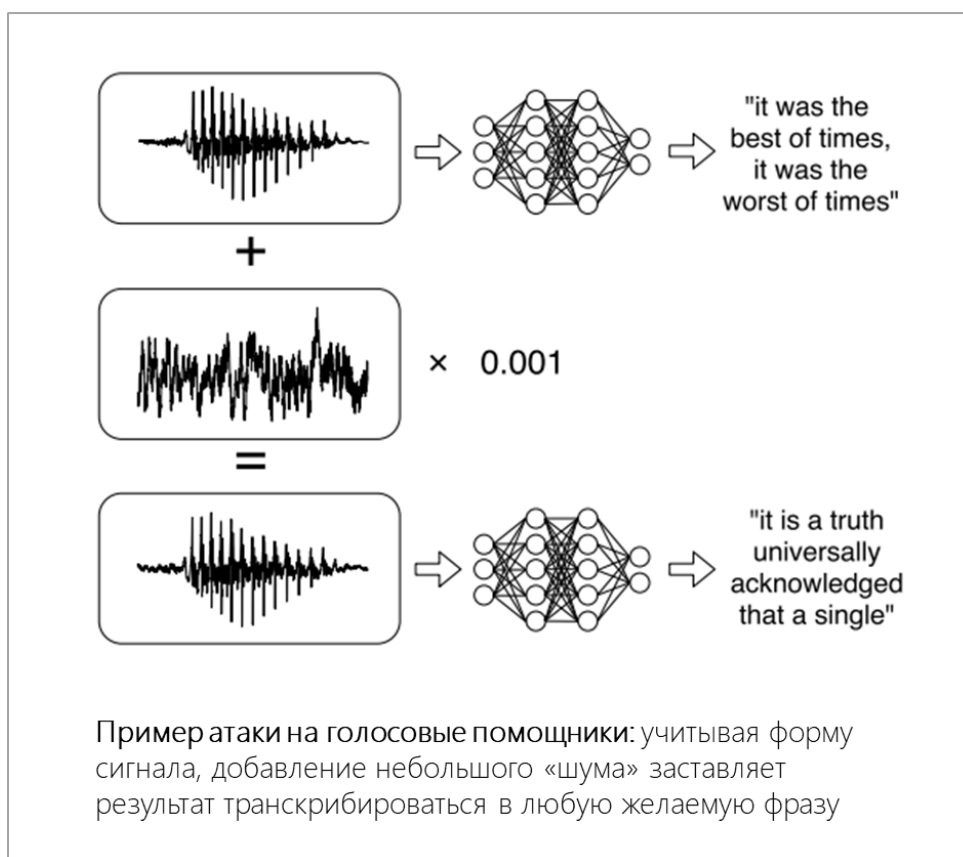
Для защиты систем голосовой биометрии, как и для фотобиометрии, используют технологию **Liveness Detection**, которая позволяет убедиться, что на другом конце провода говорит живой человек, а не заранее записанный голос. Для голосовой биометрии обычно используется интерактивный Liveness Detection – это когда человека просят произнести случайно сгенерированную фразу. Текущие возможности нейронных сетей позволяют обходить интерактивный Liveness Detection путем генерации речи в режиме онлайн. В развитии этой технологии пионерами была компания DeepMind, принадлежащая Гуглу и известная благодаря своей программе AlphaGo, победившей чемпиона мира в игре го (китайский аналог шахмат и шашек).

Компания DeepMind прославилась не только своими игровыми ботами. В 2016 году они разработали порождающую нейронную **WaveNet**, которая умеет генерировать речь по технологии TTS (text-to-speech) в режиме онлайн. В основе WaveNet лежат разработанные в DeepMind свёрточная нейросеть PixelCNN и рекуррентная нейросеть PixelRNN. В первых релизах 2016 года разработчики DeepMind отмечали проблему высокой ресурсоемкости нейронной сети WaveNet – для генерации 1 секунды речи требовалось порядка 1-2 минут работы сети. Всего через год эту проблему решили, и WaveNet стала генерировать одну секунду речи всего за несколько миллисекунд. Позже WaveNet была встроена в голосовой помощник Google Assistant.



Со взломом голоса ученые активно экспериментируют и в других направлениях. В 2018 году исследователи из университета Беркли (США) показали как можно взламывать голосовые помощники: они отправляли на голосовые помощники Siri и Alexa набор звуков, находящиеся за пределами человеческой слышимости или замаскированные среди музыки, и смогли тайно активировать системы искусственного интеллекта на смартфонах – набирать номера телефонов, открывать веб-сайты и т.д.

Демонстрация этих уязвимостей поставила под сомнение надежность голосовой биометрии для ее использования в системах безопасности, например, при разблокировке дверей дома, переводе денег в мобильном банке, покупок в интернет-магазинах и т.д.

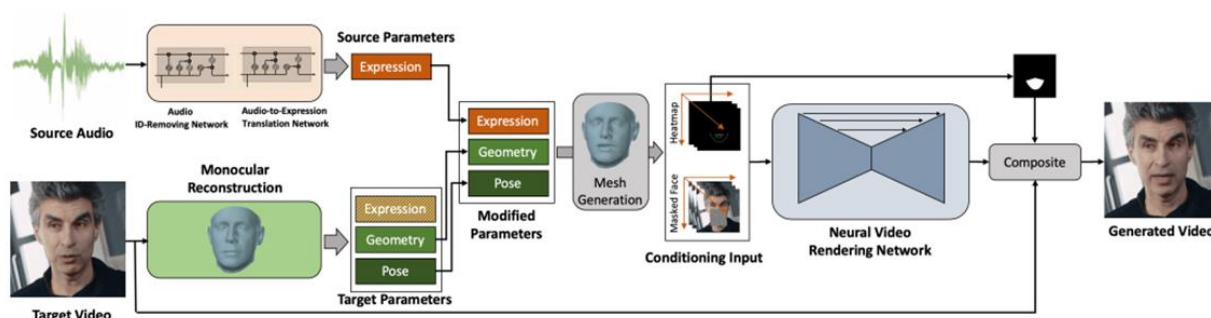


Инженеры по разработке систем безопасности понимают риски, связанные с уязвимостями биометрических систем, и начинают прибегать к мультимодальному подходу – когда в систему идентификации закладывается сразу несколько видов биометрии. Один из таких примеров Единая биометрическая система (ЕБС), запущенная в России в 2018 году для удаленной идентификации граждан на портале госуслуг. ЕБС использует 2 модальности для биометрической идентификации – распознавание лица по фотографии и голосовая идентификация пользователя. Разработчики ЕБС предполагали, что бимодальный подход позволит уменьшить долю ошибочных срабатываний, а также снизит риски взлома, поскольку злоумышленникам придется обходить сразу два типа биометрии – фото и голос.

Но совсем недавно в начале 2020 года китайские исследователи из SenseTime разработали генеративную нейронную сеть, которая позволяет принимать на вход изображение целевой персоны и аудиозапись с речью, а на выходе отдавать видеозапись с целевой персоной, на которой выражение лица персоны соответствует аудиодорожке. Таким

образом, с помощью этой технологии к любому человеку можно «приклеить» лицо другого человека с клонированным голосом. Это показало, что и бимодальные биометрические системы вообще говоря уязвимы.

Речь + Фото = Видео



На этом пока можно завершить короткий обзор уязвимостей голосовых технологий, а в следующей части обсудим разнообразные виды поведенческой биометрии.

Источники:

1. <https://www.descript.com/lyrebird-ai?source=lyrebird>
2. <https://www.resemble.ai/>
3. <https://www.ispeech.org/text.to.speech>
4. <https://veravoice.ai/>
5. <https://arxiv.org/pdf/1609.03499.pdf>
6. <https://arxiv.org/pdf/1801.01944.pdf>
7. <https://arxiv.org/pdf/2001.05201.pdf>

3. Она милого узнает по походке - можно ли обмануть поведенческую биометрию?

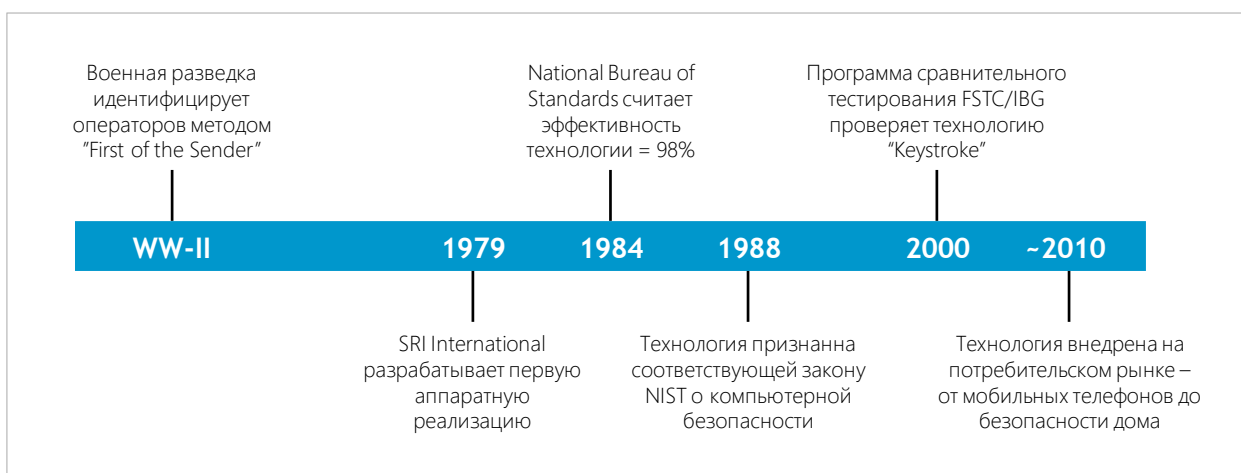
Итак, мы теперь знаем как обойти системы распознавания лиц и голосовую биометрию. Помимо фото и голоса есть и другие виды биометрий, например, поведенческая биометрия. Разновидностей поведенческой биометрии очень много – от самых старых и давно изученных, таких как клавиатурный почерк и биометрия по движению мышкой, до экзотических, таких как:

1. Биометрия по *морганию глаз* или *движению губ*;
2. *Стиль вождения* – можно встраивать в автомобили для защиты от угонов;
3. *Игровая стратегия* – можно выявлять мультиаккаунтинг в компьютерных играх, или использование одного аккаунта разными игроками. Данный вид биометрии может использоваться и в онлайн-казино;
4. *Сенсоры на рукоятке пистолета* – такой вид биометрии мы уже видели в научно-фантастических фильмах, когда оружием может пользоваться только его владелец, из чужих рук оно не стреляет;
5. *Сетевой трафик* – на этом работают различные деанонимизаторы (деанонимизация пользователей), например, для установки личности в сетях TOR;
6. *Стиль программирования* – с помощью этой биометрии выявляют хакеров, которые пишут вирусы и трояны. На этом основаны антивирусные программы, когда по базе уже известных сигнатур (кусков кода) определяют, что новый вирус был написан каким-то уже ранее известным хакером или группой хакеров;
7. *Авторский стиль* – этот вид биометрии используют, например, при проверке рукописей на антиплагиат. С помощью такого подхода ученые доказывали, что «Тихий Дон» писал сам Шолохов, а не кто-то из других известных писателей.

Classification of the various types of behavioural biometrics	Authorship	Direct human computer		Indirect human computer interaction	Motor skill	Purely behavioral	Properties of behavioural biometrics		
		Input device interaction based	Software interaction based				Enrollment time	Verification time	Required hardware
Audit logs							D	D	Computer
Biometric sketch							M	S	Mouse
Blinking (моргание)							M	S	Camera
Call-stack							D	H	Computer
Calling behaviour							D	D	Phone
Car driving style (стиль вождения)							H	M	Car sensors
Command line lexicon							H	H	Computer
Credit card use (транзакционное поведение)							D	D	Credit card
Dynamic facial features							M	S	Camera
E-mail behaviour							D	M	Computer
Gait/Stride (походка)							M	S	Camera
Game strategy (игровая стратегия)							H	H	Computer
GUI interaction							D	H	Computer
Handgrip (рукоятка пистолета)							M	S	Gun sensors
Haptic							M	M	Haptic
Keystroke dynamics							M	S	Keyboard
Lip movements (движение губ)							M	S	Camera
Mouse dynamics							M	S	Mouse
Network traffic (сетевой трафик)							D	D	Computer
Painting style							D	D	Scanner
Programming style (стиль программирования)							H	H	Computer
Registry Access							D	H	Computer
Signature/Handwriting							M	S	Stylus
Storage Activity							D	D	Computer
System Calls							D	H	Computer
Tapping							M	S	Sensor
Text Authorship (авторский стиль)							H	M	Computer
Voice/Speech/Singing							M	S	Microphone

Клавиатурный почерк (**Keystroke Dynamics**) можно отнести к одному из самых старых и давно изученных видов поведенческой биометрии. Биометрию по клавиатурному почерку начали использовать, когда появились печатные машинки и телеграфы. Например, во время второй мировой войны по клавиатурному почерку определяли операторов-шифровальщиков. Так можно было отличить настоящую шифровку от диверсанта.

Позже, когда появились пользовательские компьютеры, биометрию по клавиатурному почерку начали патентовать и совершенствовать. Сейчас этот вид биометрии используют в различных приложениях, где есть клавиатура, включая мобильные банки, ДБО и т.д.



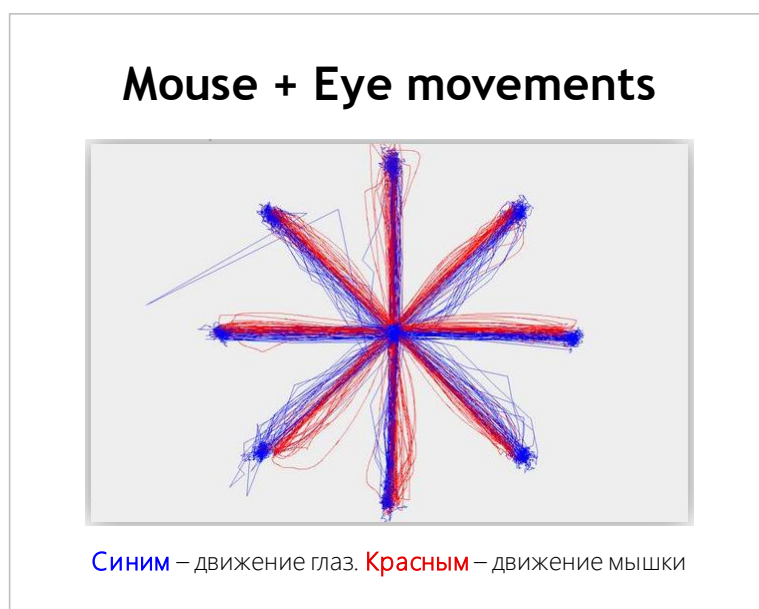
За время существования биометрии по клавиатурному почерку ее научились обходить, эмитируя необходимые паттерны почерка, основанные на таймингах нажатия клавиш. В относительно свежем исследовании 2015 года американские ученые из Университета Карнеги-Меллона предложили усилить технологию Keystroke, добавив вторую модальность – ЭМГ-сигналы (электромиография), снимаемые с мышечной активности пользователя через специальные датчики. Для практического применения такой биометрии ЭМГ-сигналы можно собирать, например, со смарт-браслетов пользователей. Варианты применения такой биометрии могут быть самыми разнообразными: вход в VIP-аккаунт, удаленное онлайн-тестирование на экзаменах и т.д.



Электроды от BioRadio, прикрепленные к рукам участника, измеряют ЭМГ-сигналы, когда участник набирает текст во время испытаний.

Помимо клавиатуры мы активно пользуемся компьютерной мышкой, а на смартфонах тачскрином. На основе этих данных ученые разработали биометрию по движению мышки – **Mouse movements**. Работы по мышинной биометрии ведутся примерно с 2003 года и в этом направлении тоже актуальна проблема с имитацией и подделкой паттернов движения мышки. Поэтому ученые стали думать над тем как усилить этот вид биометрии.

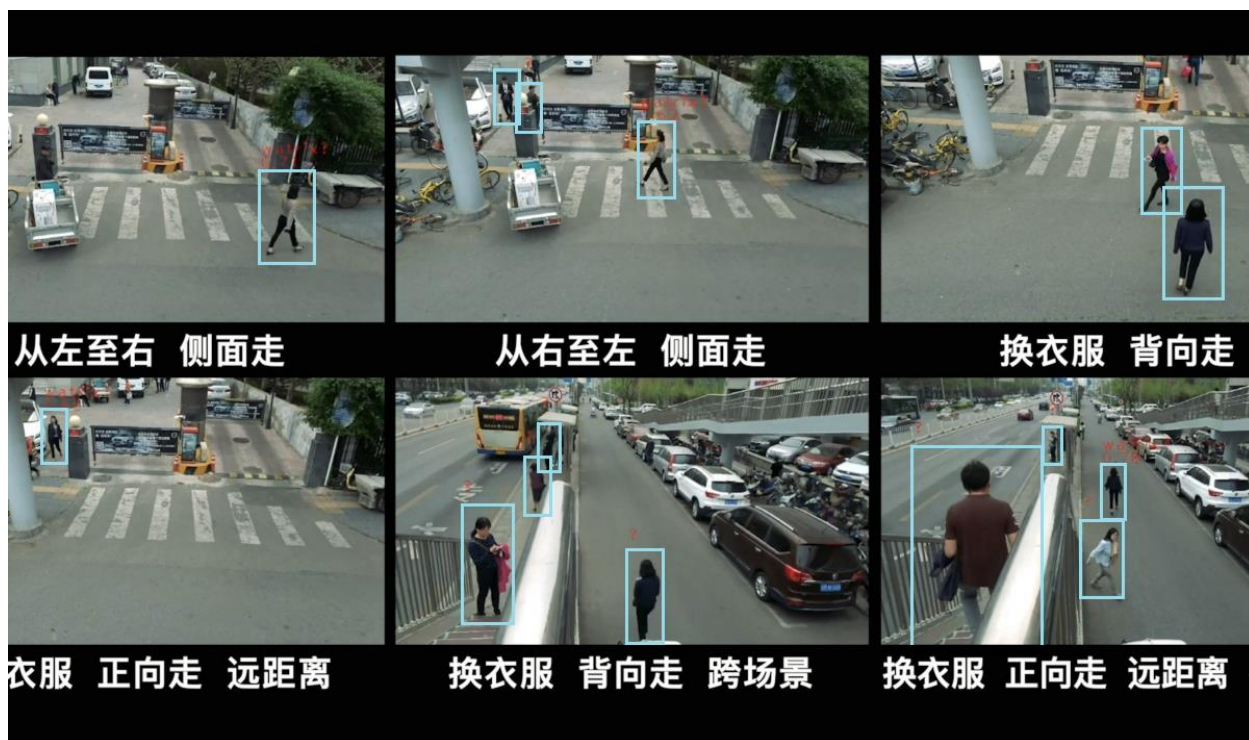
В свободное от науки время, американские ученые попытались одной рукой погладить себе живот и одновременно другой рукой похлопать себя по голове. Результат этого упражнения натолкнул их на мысль, что многие действия мы делаем синхронно. Например, оказалось, когда мы двигаем мышкой, мы направляем наш взгляд в ту же сторону, куда движется курсор мышки. Проведя ряд экспериментов, ученые выяснили, что траектории движения глаз и движения мышки имеют корреляцию 84–88%. Этот факт позволил использовать в биометрии по движению мышкой вторую контролируемую модальность – движение глаз. Использовать такую биометрию можно, например, в прокторинговых системах для удаленного прохождения тестов и сдачи экзаменов.



Другой набирающий популярность вид поведенческой биометрии – это биометрия по походке (**Gait recognition**). Работа над биометрией по походке тоже ведется достаточно давно. Еще в начале 2000-х годов эти идеи исследовались агентством DARPA Департамента обороны США.

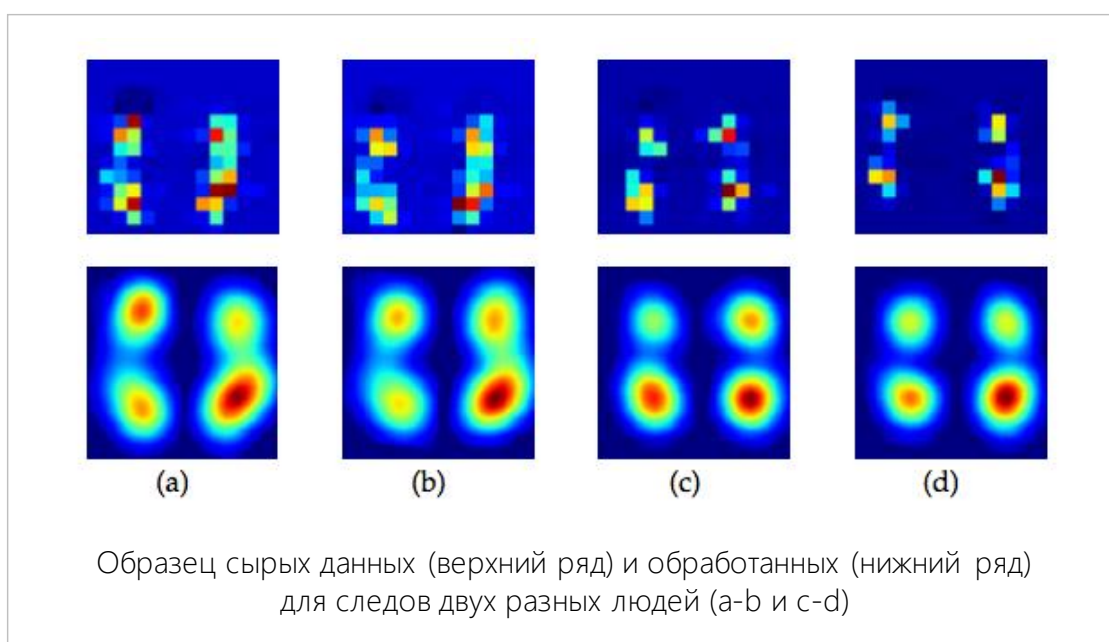
Сейчас этой технологией занимаются различные компании. Например, международная платежная система Mastercard недавно анонсировала использование биометрии по походке для оплаты проезда во время прохождения турникетов.

Китайский стартап Watrrix разработали биометрию по походке в 2018 году, а уже в 2019 году эту технологию протестировала китайская полиция в крупнейших мегаполисах – Пекине и Шанхае. В отличие от фотобиометрии, для определения паттернов походки не требуется чтобы человек смотрел в камеру, походку можно определить даже со спины. Сейчас биометрия по походке используется в городских системах видеонаблюдения Китая, дополняя традиционную фотобиометрию.



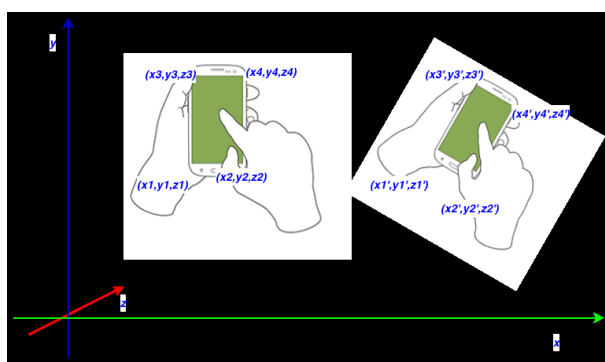
Но походку возможно тоже можно как-то имитировать и подделывать. Поэтому ученые решили сразу усилить этот вид биометрии второй модальностью.

Команда британских и испанских ученых предложила помимо временных паттернов походки учитывать отпечаток следа, который для каждого человека может быть уникальным. Ученые обучили нейронную сеть, которая позволила распознавать человека по характеристикам его следа, используя данные с пьезоэлектрических датчиков, рассчитывающих величину давления. Использовать такой вид биометрии можно, например, в аэропортах на паспортном контроле, где в пол можно встроить датчики для сбора необходимых показателей.



Сейчас многие из нас проводят свое свободное время со смартфонами в руках. И для смартфонов ученые и инженеры тоже придумывают различные виды биометрий. Приложения для мобильного банка уже давно оснащаются классическими видами поведенческой биометрии такими как клавиатурный почерк и биометрией по данным датчиков тачскрина (аналог биометрии по движению мышкой). Но в смартфоне есть много и других датчиков, с которых можно собирать поведенческие данные. Например, акселерометр, гироскоп, магнитометр, датчик температуры и т.д. Эти данные также используются для разработки поведенческой биометрии, которая получила название **Sensor Fusion**. Помимо высокой точности у Sensor Fusion есть важное преимущество – сбор данных с датчиков незаметен для пользователя, поэтому это становится удобным видом биометрии для владельца смартфона.

Sensor Fusion



- Accelerometer
- Gravity
- Gyroscope
- Magnetometer
- Pressure
- Temperature
- Humidity
- Orientation
- Touchscreen

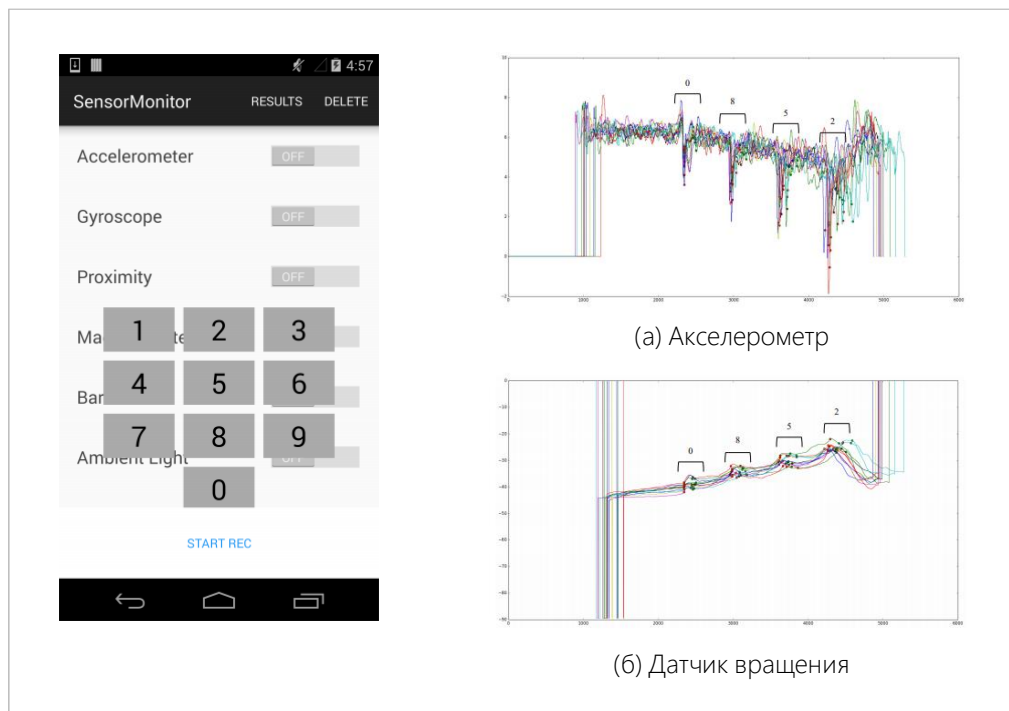
1. Поведенческие паттерны могут быть собраны даже без ведома пользователя
2. Сбор данных с датчиков смартфона не требует специального ПО

Клавиатурный почерк, тачскрин и Sensor Fusion – все это интересные альтернативные биометрии для смартфонов, если бы данные, используемые для этих технологий, были хорошо защищены. Например, данные с датчиков смартфона хранятся в незащищенном контуре, т.е. могут собираться любым авторизованным приложением.

В 2017 году инженеры по кибербезопасности разработали нейронную сеть, которая по данным датчиков смартфона распознает PIN-код владельца телефона. Основная идея данного подхода заключается в том, что когда мы вводим PIN-код для разблокировки телефона, мы держим смартфон определенным образом, т.е. у каждого человека свой уникальный паттерн ввода PIN-кода.

Используя эту особенность, ученые собрали данные с шести открытых датчиков: акселерометра, гироскопа, магнитометра и др. Далее на собранных данных они обучили нейросеть, которая угадывает PIN-код по данным датчиков смартфона с точностью 84%.

В кибербезопасности такой взлом называется атакой по сторонним (побочным) каналам – **Side-channel attack**.



Взлом PIN-кода по незащищенным данным наводит на мысль, что в биометрической гонке должны победить технологии, использующие хорошо защищенные данные, недоступные в открытых источниках. К таким видам биометрий относятся отпечатки пальцев, рисунки вен и радужная оболочка глаза.

Эксперты по кибербезопасности из вьетнамской компании Bkav (которые взломали FaceID на iPhone X) считают, что на сегодняшний день самым защищенным видом биометрии является отпечаток пальца. Так ли это на самом деле, узнаем в следующей части.

Источники:

1. <http://cecs.louisville.edu/ry/Behavioral.pdf>
2. http://checco.com/about/john.checco/publications/2003_Keystroke_Biometrics_Intro.pdf
3. http://openaccess.thecvf.com/content_cvpr_workshops_2015/W02/papers/Venugopalan_Electromyograph_and_Keystroke_2015_CVPR_paper.pdf
4. https://www.riverpublishers.com/journal_read_html_article.php?i=JCSM/6/1/1
5. <http://www.kasprowski.pl/lac/>
6. <https://www.scmp.com/tech/start-ups/article/2187600/chinese-police-surveillance-gets-boost-ai-start-watrix-technology-can>
7. <https://ieeexplore.ieee.org/document/8275035>
8. https://www.researchgate.net/publication/322295274_Behavioral_Biometrics_for_Smartphone_User_Authentication
9. <https://eprint.iacr.org/2017/1169.pdf>





4. Отпечаток, радужка и вены - взломать нельзя защититься.

В предыдущих частях мы разобрали уязвимости и способы защиты современных биометрических систем, таких как биометрия по фотографии, по голосу, по клавиатурному почерку и т.д.

Взломавшие Face ID на iPhone X специалисты по кибербезопасности из компании Bkav считают, что на сегодняшний день самым надежным видом биометрии является отпечаток пальца.

С ними не согласны хакеры из сообщества [Chaos Computer Club](#), которые взломали отпечаток пальца на iPhone 5s еще в 2013 году.

Для взлома хакерам потребовалось сфотографировать в высоком разрешении отпечаток пальца владельца айфона. Далее фотографию отпечатка распечатали на толстой бумаге на лазерном принтере, получив трафарет. После этого на трафарет-распечатку залили жидкий латекс, получив своеобразный «факсимиле» отпечатка. Далее один из хакеров наклеил латекс на свой палец и взломал **Touch ID** владельца айфона.

			
<p>1</p> <p>Необходимо сделать фото отпечатка в высоком разрешении – 2400 точек на дюйм. Фото отпечатка можно сделать, например, с оконного стекла</p>	<p>2</p> <p>Изображение распечатывается в разрешении 1200 dpi на лазерном принтере на толстой бумаге</p>	<p>3</p> <p>Отпечаток заливается жидким латексом, который после высыхания снимается и получается «факсимиле» отпечатка</p>	<p>4</p> <p>Надетое на чужой палец «факсимиле» отпечатка воспринимается Touch ID как подушечка пальца настоящего владельца смартфона</p>

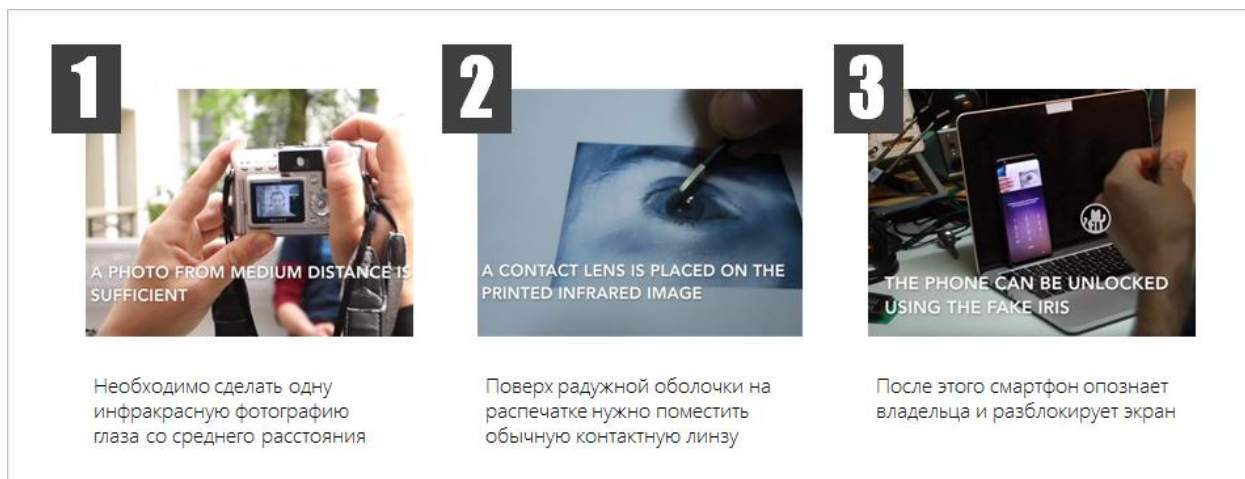
Сразу после этой шумевшей демонстрации другие эксперты по кибербезопасности принялись проверять методику взлома Touch ID с помощью отпечатка из латекса. И у многих это получилось. Однако некоторые эксперты отмечали, что процесс сопряжен с рядом трудностей. В частности, было отмечено, что на практике будет сложно получить изображение отпечатка пальца в высоком разрешении.

Но всего через пару лет изобретатели технологии взлома Touch ID развенчали миф о сложности получения фотографии отпечатка в высоком разрешении. Они смогли сфотографировать отпечаток пальца министра обороны Германии, находясь всего в трех метрах от нее, пока она читала доклад на публичной конференции.



Производители смартфонов учли эту уязвимость и в 2017 году компания Samsung выпустила свой флагманский смартфон Galaxy S8 с новейшей технологией биометрии по радужке глаза, которая должна была стать более защищенной по сравнению с биометрией по отпечатку пальца.

Однако с радужкой тоже оказалось не все так радужно. Та же самая группа хакеров из Chaos Computer Club показала, что взломать радужку еще проще. Для этого хакерам потребовалось сфотографировать с нескольких метров владельца смартфона на обычный фотоаппарат. Далее фотография глаза была распечатана на лазерном принтере той же компании Samsung, после чего на распечатку наклеили обычную контактную линзу и взломали биометрию смартфона, получив к нему доступ.



Примерно через год (в 2018 году) польские ученые создали технологию Liveness Detection для радужки, цель которой – определить, что фотография радужки сделана с живого человека, а не с мертвого.

Для этого разработчики обучили сверточную нейронную сеть, которая смогла отличать радужку живого человека от мертвого с точностью 99%. При этом использовали уже готовую предобученную нейронную сеть **VGG-16** (которая выложена во многих открытых репозиториях) и дообучили три последних слоя этой сети (из 16-ти) всего на 500 фотографиях. Таким образом разработчики продемонстрировали, что для решения таких

не очень сложных, но технологичных задач не требуются больших массивов данных и дорогих вычислительных ресурсов.

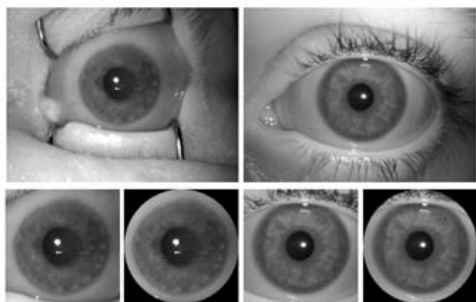


Рис. 1. Примеры изображений радужной оболочки, полученных от мертвого (слева) и живого человека (справа).

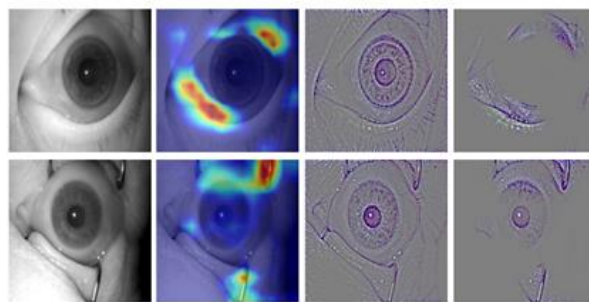


Рис. 2. Примеры карт активации классов, полученные с помощью метода Grad-CAM. Представлены образцы вскрытия (оба правильно классифицированы).

Если отпечаток пальца и радужку глаза легко сфотографировать на обычную фотокамеру, то получить рисунок вен, наверное, должно быть сложнее, поскольку для сканирования вен используются специальные инфракрасные камеры.

Изображение рисунка вен формируется благодаря тому, что гемоглобин в крови поглощает инфракрасное излучение, в результате чего степень отражения вен уменьшается и они отображаются на фотографии в виде черных линий. Примерно по такому же принципу работают пульсоксиметры, которые измеряют уровень кислорода (а точнее гемоглобина) в крови человека.

В 2019 году на конференции **Chaos Communication Congress**, организованной сообществом Chaos Computer Club, немецкие инженеры из Берлинского политеха продемонстрировали как взломать биометрию по рисунку вен. Для этого они сфотографировали вены на ладони с помощью инфракрасной камеры. Затем с помощью 3D-принтера сделали искусственную ладонь из воска, в которую была залита фотография с рисунком вен. С помощью полученной восковой ладони инженеры взломали биометрию по рисунку вен.



Рис. 1. Инфракрасный датчик для сканирования вен можно закрепить в сушилке для рук

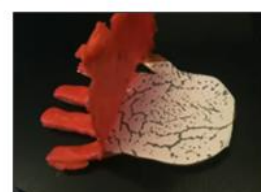
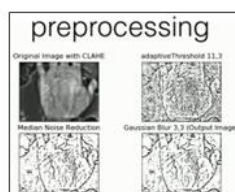


Рис. 2. Полученная фотография обрабатывается и заливается воском в 3D-форму

Докладчики отметили, что взлом биометрии по рисунку вен не сопряжен с технологическими трудностями, поскольку инфракрасные датчики можно купить в обычном магазине электроники и закрепить их, например, в сушилке для рук.

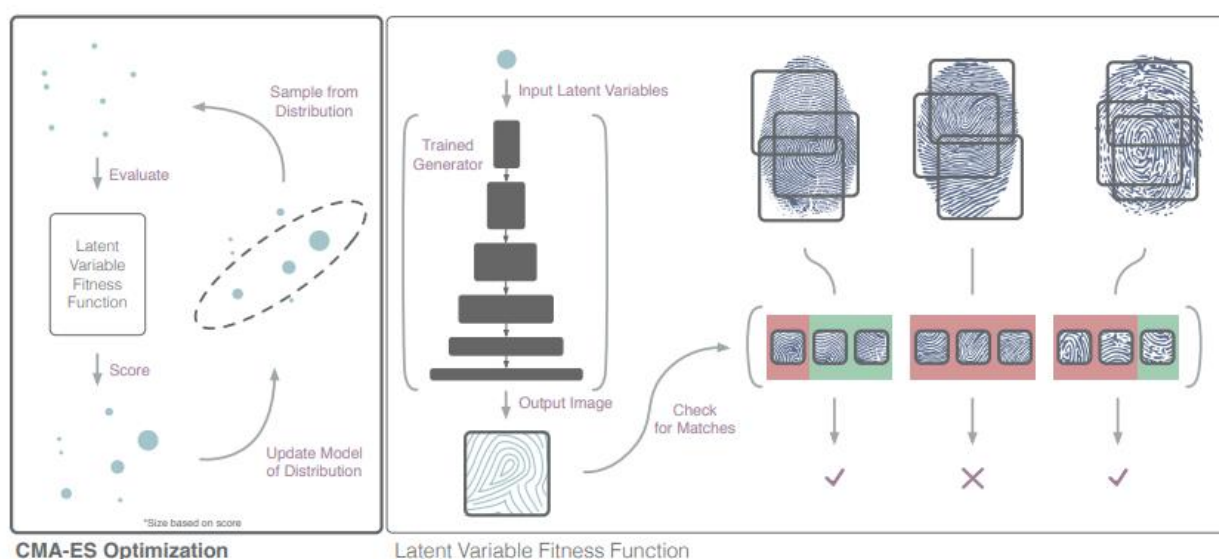
Взломы отпечатка, радужки и вен продемонстрировали слабую защищенность данных биометрических технологий. Однако для применения таких техник взлома необходимо находится в непосредственной близости к «жертве», чтобы получить фотографию отпечатка, радужки или вен. То есть масштабировать такие методы взлома вряд ли получится.

В 2018 году ученые из Нью-Йорского Университета придумали другой метод взлома биометрии по отпечатку, который в будущем может стать реальной угрозой и для радужки, и для рисунка вен.

Ученые разработали нейронную сеть **Deep Master Prints**, которая генерирует поддельный отпечаток пальца. Технология взлома достаточно интересная. Оказалось, что в биометрии по отпечатку пальца используется не весь рисунок отпечатка, а только грубые признаки. Это интуитивно понятно, зная, как работают сверточные нейронные сети, лежащие в основе биометрических систем – они выделяют грубые признаки без глубокой детализации, иначе пользователь не смог бы пройти биометрию повторно (принципы работы сверточных нейронных сетей мы разбирали в первой части статьи).

Ученые этим воспользовались и обучили генеративно-сопоставительную сеть, которая подбирает отпечаток «отмычку», подходящий сразу к нескольким реальным отпечаткам пальцев. Этот метод взлома работает по принципу "атаки словаря", используемый для взлома текстовых паролей, где перебираются наиболее часто употребляемые пароли или части паролей.

Единственным недостатком разработанной нейронной сети является ее невысокая точность – из пяти сгенерированных отпечатков проходит только один. Но такую технологию можно масштабировать, т.е. использовать ее для массовых атак. И конверсии 20% будет более чем достаточно, чтобы мошенники смогли на этом «зарабатывать».



Данная научная работа в очередной раз продемонстрировала насколько уязвимы биометрические технологии, в основе которых лежат нейронные сети. Причем в качестве криптолита для нейронных сетей выступают другие нейронные сети – **GAN'ы**. Чего нам ожидать в недалеком будущем узнаем в последней части этого обзора.

Источники:

1. <https://www.youtube.com/watch?v=plY6k4gvQsY>
2. <https://media.ccc.de/v/biometrie-s8-iris-en>
3. <https://arxiv.org/pdf/1807.04058.pdf>
4. https://media.ccc.de/v/35c3-9545-venenerkennung_hacken#t=2377
5. <https://arxiv.org/pdf/1705.07386.pdf>

5. Нейронные войны. Эпизод V. Социальная инженерия наносит ответный удар.

В предыдущей части мы разбирали методы спуфинга (взлома) биометрий по отпечатку пальца, радужке глаза и рисунку вен. Несмотря на эти уязвимости, специалисты по кибербезопасности считают биометрию по отпечатку пальца одной из самых надежных.

Практически все такие демонстрации взлома пока проводятся учеными и инженерами, которые сначала придумывают сложную защиту, потом сами же придумывают как ее обойти и так далее. Мошенники часто действуют намного проще.

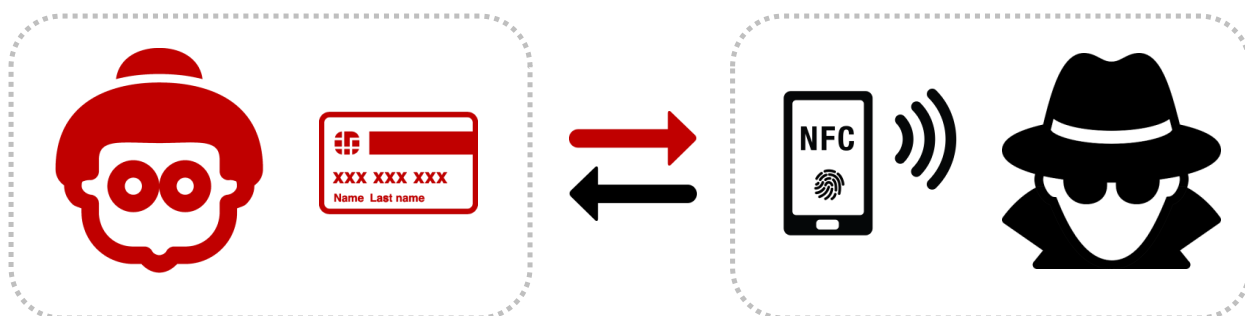
Многие из нас уже активно пользуются мобильными кошельками **Apple Pay**, **Android Pay** или **Samsung Pay**. Принцип активации кошелька простой и удобный:

- 1) К кошельку привязывается банковская карта по ее реквизитам.
- 2) Привязка подтверждается одноразовым sms-паролем и отпечатком пальца владельца смартфона (или другим видом биометрии, которая стоит на смартфоне).
- 3) После этого смартфоном можно оплачивать покупки в магазинах по бесконтактной технологии NFC, на любую сумму, без пинкода, подтверждая вход в кошелек отпечатком пальца или другой биометрией.

Когда Apple запускали эту технологию, они утверждали, что вход по отпечатку пальца в кошелек является одним из самых надежных видов защиты и это позволит снизить уровень карточного мошенничества.

Внедрив эту технологию, Apple возможно снизили риски карточного мошенничества, связанные с кражей PIN-кодов. Но, с другой стороны, они сами того не подозревая породили еще больший риск – риск кражи денег с карт с помощью методов социальной инженерии.

После запуска Apple Pay «социальные инженеры» стали активно использовать эту технологию в мошеннических целях. Они звонили клиентам банков и стандартными методами социальной инженерии выуживали у своих «жертв» реквизиты карт и авторизационные SMS-коды. Далее мошенники привязывали карту «жертвы» к **своему** Apple-кошельку, подтверждали SMS-кодом и **своим** отпечатком пальца. После этого мошенники могли расплачиваться в магазинах чужой картой с помощью своего смартфона без каких-либо ограничений на сумму покупки.



Социальная инженерия существовала и до появления Apple Pay, когда мошенники пользовались анонимными Web-кошельками для вывода денег с банковских карт. Но большим минусом анонимных Web-кошельков является то, что на их пополнение стоят лимиты на каждую транзакцию, из-за чего мошенникам приходилось делать несколько звонков «жертве», спрашивать несколько SMS-кодов, в результате «жертва» начинала что-то подозревать и возможно блокировать карту. Плюсом же Apple-кошельков для мошенников стало то, что требовался всего один SMS-код для привязки карты к кошельку, после чего деньги можно выводить без лимитов.

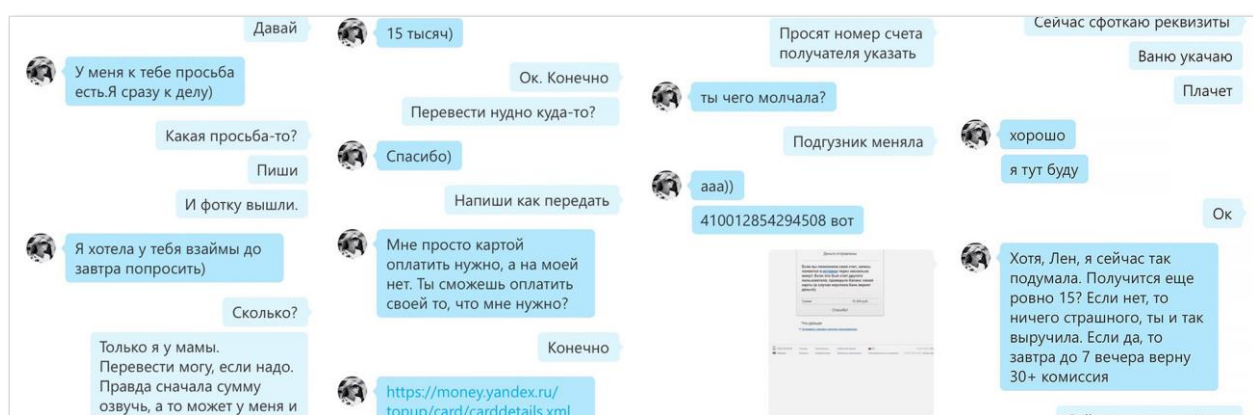
Так чрезмерная уверенность Apple в биометрических технологиях привела к тому, что эта технология стала удобным инструментом для мошенников.

Но есть много и других разновидностей социальной инженерии. Например, старая, но до сих пор популярная «нигерийская схема» – когда на почту приходит письмо от некоего принца Нигерии (или другой африканской страны), якобы наследника многомиллионного состояния, который просит помочь ему вывести деньги на счета «жертвы», предварительно выставляя счет в несколько тысяч долларов за открытие этого счета и оформление необходимых документов.

Или всем известная схема со звонками якобы от «службы безопасности банка».

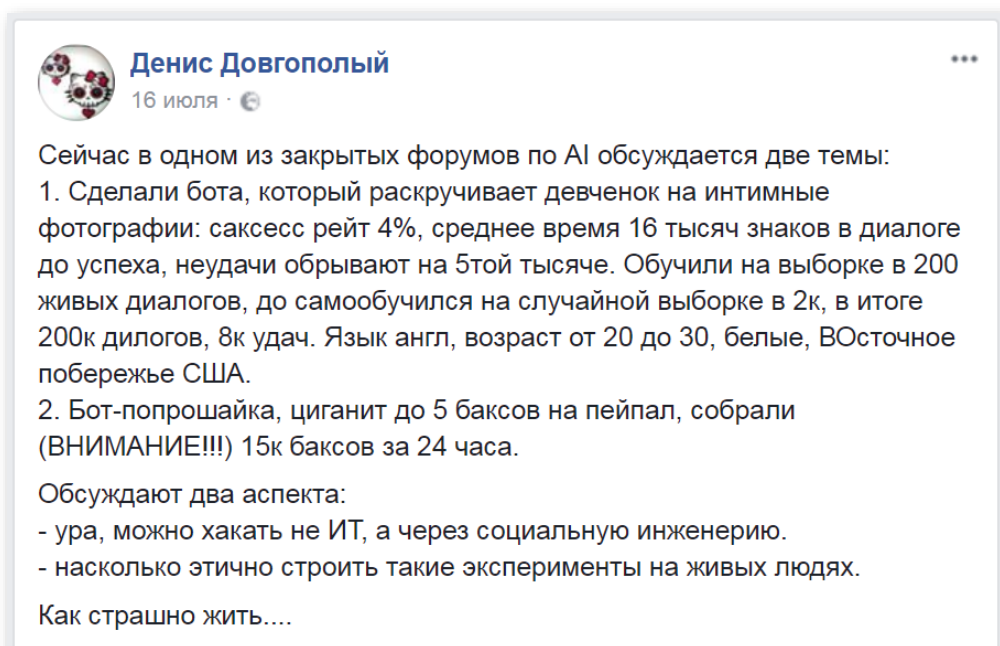
Или классическая схема с «просьбой одолжить денег» в социальных сетях и мессенджерах – когда мошенники пишут с ворованных аккаунтов. В [интервью](#) 2015 года один из скуре-мошенников подробно рассказывал, как устроен этот бизнес:

1. Для этой работы обычно нанимают студентов;
2. Предварительно их обучают, дают прочесть пару книг по психологии;
3. Потом этих дропов (наемников) сажают в офис, выдают компьютеры и логины ворованных аккаунтов, и они сидят и «разводят» людей на деньги.
4. Зарплата у таких наемников примерно 40- 50% с выручки.



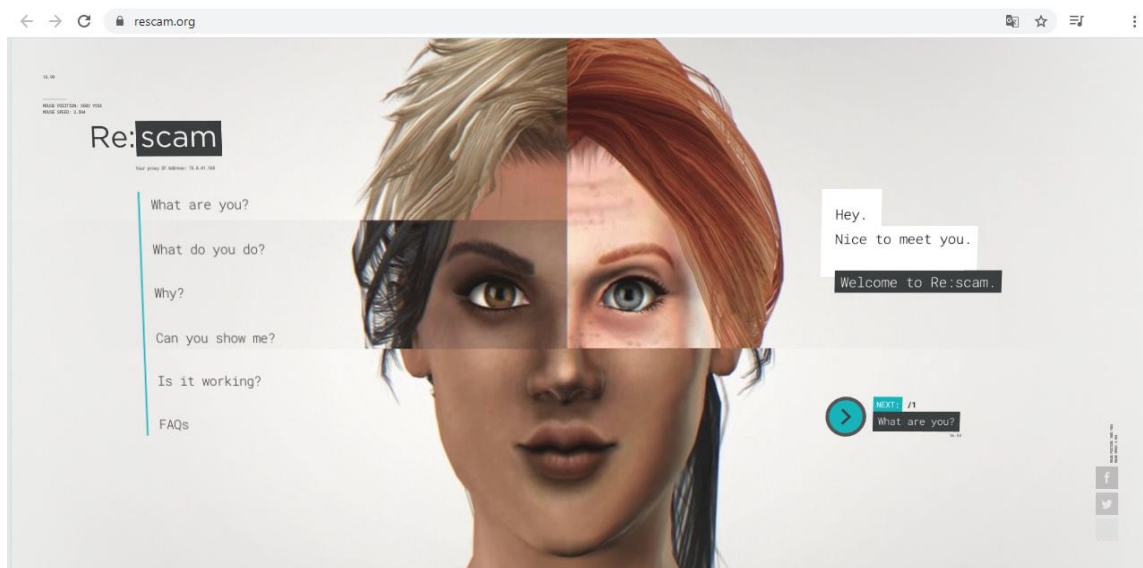
Это примеры того, как социальная инженерия устроена сейчас. Но современные возможности нейронных сетей позволяют создавать чат-ботов для различных целей, в том числе и для мошеннических.

В 2017 году на одном из американских форумов по искусственному интеллекту программисты обсуждали результаты тестирования двух чат-ботов, один из которых «разводил» девушек на интимные фотографии, а второй «цыганил» по 5 баксов на PayPal, собрав за сутки 15 тыс. долларов.



Такие чат-боты «попрошайки» могут позволить мошенникам автоматизировать свою работу. Конечно, до профессиональных skure-мошенников им еще очень далеко, но такие технологии легко масштабируются и затраты на разработку чат-бота разовые, т.е. не надо отдавать половину выручки дропам-наемникам.

Практически одновременно с чат-ботами «попрошайками» появились чат-боты «отвлекайки». Новозеландский стартап Netsafe разработали чат-бота **Re:scam**, который общается с мошенниками в почтовом клиенте, отвечая им на нигерийские письма. Тем самым такой бот занимает время мошенников, повышает их издержки и снижает эффективность.



Возможно, что скоро мы увидим, как такие боты «отвлекайки» будут общаться с ботами «попрошайками». И Григорий Бакунов из Яндекса (который придумал случайный макияж для обхода фотобиометрии) в своем телеграмм-канале пишет:








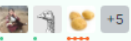





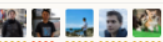

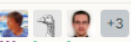




«Следующие 10 лет мы будем не только учиться создавать искусственный интеллект, но и обманывать его, делать анти-обманные системы и так далее. Война предстоит не хуже, чем вирусно-антивирусная, готовьтесь!»

Григорий Бакунов
Яндекс



И можно сказать, что такая война уже началась. Напомню, что пионерская работа Гудфеллоу с пандой и гиббоном была опубликована в 2015 году. Уже в 2016 году на самой большой мировой конференции по нейронным сетям NeurIPS стали появляться научные исследования на тему adversarial-атак на нейронные сети.

В этом году на площадке Kaggle завершились соревнования **Deepfake Detection Challenge** от Facebook с огромным призовым фондом \$1 млн. На всю организацию конкурса Facebook потратила беспрецедентные \$10 млн, наняв более 3,5 тыс. актеров для создания настоящих видеороликов и дипфейков. В соревновании участвовало более 2 тыс. команд, а в топ-10 победителей попало много представителей советской математической школы, которые забрали больше половины призового фонда.

\$1,000,000 Deepfake Detection Challenge									
	#	Δpub	Team Name	Notebook	Team Members	Score	Entries	Last	
	1	▲ 3	Selim Seferbekov	\$500 000		0.42798	2	5mo	
	2	▲ 35	\WM/	\$300 000		0.42842	2	5mo	
	3	▲ 3	NtechLab	\$100 000		0.43452	2	5mo	
	4	▲ 6	Eighteen years old	\$60 000		0.43476	2	5mo	
	5	▲ 12	The Medics	\$40 000		0.43711	2	5mo	
	6	▲ 42	Konstantin Simonchik			0.44289	2	5mo	
	7	▲ 27	All Faces Are Real			0.44531	1	5mo	
	8	▲ 6	ID R&D			0.44837	2	5mo	
	9	▲ 76	名侦探柯南			0.44911	2	5mo	
	10	▲ 23	vcg@xmu			0.45149	2	5mo	

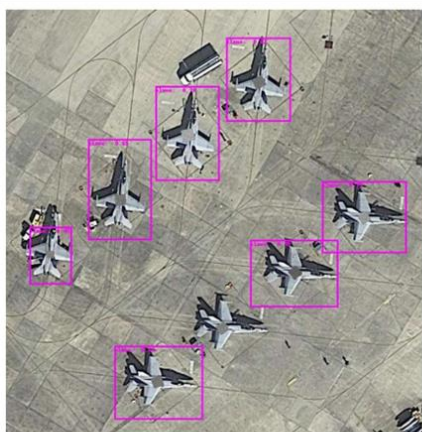
Белорус Селим Сефербеков занял 1 место и получил главный приз – \$500k.

Программист Азат Давлетшин, выступающий от компании NtechLab, занял 3-место и получили \$100k. Интересный факт, что NtechLab когда-то разработали популярное приложение FindFace, с помощью которого можно искать людей в социальной сети Вконтакте по фотографиям. Эта же компания совместно с мэрией Москвы внедрила распознавание лиц для городской системы видеонаблюдения.

В 2017 году лаборатория DSTL при Департаменте обороны Великобритании проводила открытый ML-конкурс по распознаванию объектов на спутников снимках. Участникам предлагалось распознавать на спутниковых снимках нигерийских джунглей различные объекты, такие как дороги, реки, крупную и мелкую технику и т.п. Несмотря на то, что конкурс был открытым, не обошлось и без политики, когда организаторы ограничили список стран для попадания в призовую зону. По этой причине, россиянин Владимир Игловиков, занявший 2-е место в абсолютном зачете, не получил призовые выплаты.

Сейчас уже многие страны (включая Россию) ведут свои собственные разработки по распознаванию военной техники и военных баз по спутниковым снимкам. Но, как мы уже знаем, война «снаряда и брони» уже идет полным ходом.

Пару месяцев назад, нидерландские ученые опубликовали результаты работы своей нейронной сети **YOLOv2**, которая создает специальные патчи (картинки), защищающие самолеты от систем распознавания военной техники по спутниковым снимкам или по фотографиям дронов. Эксперименты на спутниковых снимках показали, что большие патчи снижают среднюю точность систем обнаружения самолетов с 94% до 5,6%, а маленькие – до 37,8%. Такие патчи хорошо работают и при наложении их на соседнюю часть взлетно-посадочной полосы, а не на сам самолет. Т.е. патчи можно наносить краской прямо на взлетно-посадочной полосе и самолеты не будут обнаружены.



(а) случайный патч

а) Достоверность обнаруженных истребителей со случайными патчами находится в диапазоне от 0,45 до 0,78 при пороге обнаружения 0,4. Достоверность необнаруженного истребителя составляет 0,23.



(б) обученный патч

б) Истребители с наложенными обученными патчами не обнаруживаются при пороге 0,4: доверительный интервал от 0,01 до 0,04 с единственным пиковым значением 0,14.

В части биометрических технологий тоже продолжается гонка.

Месяц назад южнокорейские ученые разработали новый вид биометрии, которую назвали биоакустической подписью. Такая подпись формируется по звуковым волнам, проходящим через палец человека. В основе лежит тот факт, что акустический сигнал для разных людей передается по-разному из-за анатомических особенностей каждого человека – костных, хрящевых, сухожильных и мышечной ткани. В результате формируется уникальный для каждого человека акустический сигнал.

Разработчики уверяют, что такой сигнал лишён главной уязвимости оптических методов биометрии, таких как сканирование отпечатков пальца, радужной оболочки глаза или лица. Однако скептики уверяют, что снять акустический сигнал с пальца человека будет так же легко, как сделать фотографию отпечатка, радужки или рисунка вен.











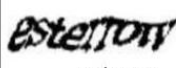




Если подвести итоги и порассуждать о будущем биометрии, то вполне возможно, что карикатурный биометрический банкомат скоро станет реальностью.



Использование нескольких модальностей в биометрических системах позволяет снизить вероятность их взлома путем повышения издержек для взломщика – когда надо взломать каждую модальность. Поэтому сейчас все чаще тестируются бимодальные виды биометрии – лицо + голос, движение мышки + движение глаз, клавиатурный почерк + электромиография, походка + отпечаток стоп и т. д.

Мы будем внимательно следить за развитием этих технологий, а кто-то из читателей возможно будет участвовать в их разработке.

И в завершении небольшой бонус. Капчу тоже уже взломали, [статья](#) вышла в журнале Science в декабре 2017 года.

Input & ground truth	RCN top parse	RCN second parse	Human labels	CAPTCHA name	Examples	Word accuracy	Character accuracy
 calwime	 calwime	 calwime	canmme caiwime	reCAPTCHA		66.6%	94.3%
 erldhbm	 erldhbm	 erldhbm	erldnhm erldhbm	BotDetect		64.4%	91.6%
 esterrow	 esterrow	 estenow	esterrow esterrow	Yahoo		57.4%	92.5%
				PayPal		57.1%	89.3%

Источники:

1. <https://habrahabr.ru/post/255225/>
2. <https://www.rescam.org/>
3. <https://www.kaggle.com/c/deepfake-detection-challenge/leaderboard>
4. <https://arxiv.org/pdf/2008.13671.pdf>
5. <https://ieeexplore.ieee.org/document/8859636>
6. <http://shoni2.princeton.edu/ftp/lyo/journals/MiscLEHistory/DileepGeorge-MachineLearningGenerativeVisionModel-Science2017.pdf>