Сможет ли Большой Брат определить ваше лицо по уличному видеонаблюдению и определить, счастлив ли вы, грустите или зол? Может ли это удостоверение личности привести к вашему аресту на основании невыполненного ордера? Каковы шансы, что идентификация неверна и действительно связана с кем-то другим? Сможете ли вы полностью победить слежку, используя какой-нибудь трюк?

С другой стороны, можете ли вы попасть в хранилище, защищенное камерой и программным обеспечением для идентификации лиц, подняв отпечаток лица уполномоченного лица? Что, если вы наденете трехмерную маску лица уполномоченного лица?

Добро пожаловать в распознавание лиц - и подделку распознавания лиц.

**Что такое распознавание лиц?**

Распознавание лиц - это метод идентификации неизвестного человека или аутентификации личности конкретного человека по его лицу. Это отрасль [компьютерного зрения](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.infoworld.com/article/3572553/what-is-computer-vision-ai-for-images-and-video.html) , но распознавание лиц является специализированным и включает в себя социальный багаж для некоторых приложений, а также некоторые уязвимости для спуфинга.

**Как работает распознавание лиц?**

Ранние алгоритмы распознавания лиц (которые все еще используются сегодня в улучшенной и более автоматизированной форме) полагаются на биометрию (например, расстояние между глазами), чтобы преобразовать измеренные черты лица из двухмерного изображения в набор чисел (функция вектор или шаблон), который описывает лицо. Затем процесс распознавания сравнивает эти векторы с базой данных известных лиц, которые были сопоставлены с особенностями таким же образом. Одной из сложностей в этом процессе является настройка лиц на нормализованный вид для учета поворота и наклона головы перед извлечением показателей. Этот класс алгоритмов называется *геометрическим*.

Другой подход к распознаванию лиц - нормализовать и сжимать двухмерные изображения лиц и сравнивать их с базой данных нормализованных и сжатых изображений аналогичным образом. Этот класс алгоритмов называется *фотометрическим*.

Трехмерное распознавание лица использует трехмерные датчики для захвата изображения лица или реконструирует трехмерное изображение с трех двухмерных камер слежения, направленных под разными углами. Трехмерное распознавание лиц может быть значительно более точным, чем двухмерное распознавание.

Анализ текстуры кожи сопоставляет линии, узоры и пятна на лице человека с другим вектором признаков. Добавление анализа текстуры кожи к 2-D или 3-D распознаванию лиц может повысить точность распознавания на 20–25 процентов, особенно в случаях двойников и двойников. Вы также можете комбинировать все методы и добавлять мультиспектральные изображения (видимый свет и инфракрасный свет) для еще большей точности.

Распознавание лиц улучшается из года в год с момента появления этой области в 1964 году. В среднем каждые два года количество ошибок снижается вдвое.

**Вендорные тесты распознавания лиц**

NIST, Национальный институт стандартов и технологий США, с 2000 года проводит тесты алгоритмов распознавания [лиц, тест поставщика распознавания лиц (FRVT)](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf) . Используемые наборы данных изображений в основном являются фотографиями полицейских, но также включают в себя дикие неподвижные изображения, например, найденные в [Викимедиа](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://commons.wikimedia.org/wiki/File:Sandra_Bullock_(9192364254).jpg) , и изображения с низким разрешением с веб-камер.

Алгоритмы FRVT в основном представлены коммерческими поставщиками. Сравнение по сравнению с прошлым годом показывает значительный прирост производительности и точности; по словам производителей, это в первую очередь из-за использования [глубоких сверточных нейронных сетей](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.infoworld.com/article/3397142/what-is-deep-learning-algorithms-that-mimic-the-human-brain.html) .

Связанные программы тестирования распознавания лиц NIST изучали демографические эффекты, обнаружение морфинга лиц, идентификацию лиц, опубликованных в социальных сетях, и идентификацию лиц на видео. Предыдущая серия тестов проводилась в 1990-х годах под другим названием, Face Recognition Technology (FERET).

**Приложения для распознавания лиц**

Приложения для распознавания лиц в основном делятся на три основные категории: безопасность, здоровье и маркетинг / розничная торговля. Безопасность включает в себя правоохранительные органы, и этот класс использования распознавания лиц может быть таким же безобидным, как сопоставление людей с фотографиями в паспорте быстрее и точнее, чем люди, и столь же жутким, как сценарий « [Интересующее лицо](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://en.wikipedia.org/wiki/Person_of_Interest_(TV_series)) », когда людей отслеживают с помощью системы видеонаблюдения и сравнивают в сопоставленные базы данных фотографий. Безопасность, не относящаяся к правоохранительным органам, включает общие приложения, такие как разблокировка по лицу для мобильных телефонов и контроль доступа для лабораторий и хранилищ.

Медицинские приложения распознавания лиц включают в себя регистрацию пациентов, обнаружение эмоций в реальном времени, отслеживание пациентов в учреждении, оценку уровней боли у невербальных пациентов, обнаружение определенных заболеваний и состояний, идентификацию персонала и безопасность учреждения. Маркетинговые и розничные приложения распознавания лиц включают идентификацию участников программы лояльности, идентификацию и отслеживание известных воров в магазинах, а также распознавание людей и их эмоций для целевых предложений продуктов.

**Споры, предубеждения и запреты на распознавание лиц**

Сказать, что некоторые из этих приложений являются спорными, было бы преуменьшением. Как говорится в [статье New York Times](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html) за [2019 год](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.nytimes.com/2019/05/15/business/facial-recognition-software-controversy.html) , распознавание лиц вызвало споры, начиная с его использования для наблюдения за стадионом и заканчивая расистским программным обеспечением.

Наблюдение за стадионом? Распознавание лиц использовалось на Суперкубке 2001 года: программа идентифицировала 19 человек, которые, как считалось, подлежали выдаче ордеров, но ни один не был арестован (не из-за отсутствия попыток).

Расистское программное обеспечение? Возникло несколько проблем, начиная с программного обеспечения для отслеживания лиц 2009 года, которое могло отслеживать белых, но не черных, и продолжая исследование MIT 2015 года, которое показало, что программное обеспечение для распознавания лиц того времени намного лучше работало на белых мужских лицах, чем на женских и / или Черные лица.

Подобные проблемы привели к полному запрету программ распознавания лиц в определенных местах или для определенных целей. В 2019 году Сан-Франциско стал первым крупным американским городом, который запретил полиции и другим правоохранительным органам использовать программное обеспечение для распознавания лиц; Microsoft призвала принять федеральные правила по распознаванию лиц; и MIT показали, что в Amazon Rekognition было больше проблем с определением женского пола, чем мужского, по изображениям лиц, а также больше проблем с женским полом чернокожих, чем с белым женским полом.

В июне 2020 года Microsoft объявила, что не будет продавать и не продавала свое программное обеспечение для распознавания лиц полиции; Amazon запретил полиции использовать Rekognition в течение года; и IBM отказалась от технологии распознавания лиц. [Однако полностью запретить распознавание лиц будет непросто](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.vox.com/recode/2020/7/3/21307873/facial-recognition-ban-law-enforcement-apple-google-facebook) , учитывая его широкое распространение в iPhone (Face ID) и других устройствах, программном обеспечении и технологиях.

Не все программы для распознавания лиц страдают одинаковыми предубеждениями. Исследование [демографических эффектов NIST в 2019 году](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects) продолжило работу MIT и показало, что алгоритмическая демографическая предвзятость широко варьируется среди разработчиков программного обеспечения для распознавания лиц. Да, есть демографические эффекты на частоту ложных совпадений и ложных несовпадений алгоритмов идентификации лиц, но они могут варьироваться на несколько порядков от поставщика к поставщику, и со временем они уменьшаются.

**Взлом распознавания лиц и методы антиспуфинга**

Учитывая потенциальную угрозу конфиденциальности, связанную с распознаванием лиц, и привлекательность получения доступа к ценным ресурсам, защищенным аутентификацией по лицу, было предпринято много попыток взломать или подделать технологию. Вы можете представить распечатанное изображение лица вместо живого лица, или изображение на экране, или трехмерную напечатанную маску, чтобы пройти аутентификацию. Для видеонаблюдения вы можете воспроизводить видео. Чтобы избежать слежки, вы можете попробовать ткани и макияж CV Dazzle и / или ИК-излучатели, чтобы обмануть программу и заставить ее не распознавать ваше лицо.

Конечно, для всех этих атак предпринимаются попытки разработать методы защиты от спуфинга. Для обнаружения напечатанных изображений поставщики используют тест живучести, такой как ожидание, пока объект моргнет, или выполнение анализа движения, или использование инфракрасного излучения, чтобы отличить живое лицо от напечатанного изображения. Другой подход заключается в проведении анализа микротекстур, поскольку человеческая кожа оптически отличается от отпечатков и материалов масок. Последние методы защиты от спуфинга в основном основаны на глубоких сверточных нейронных сетях.

Это развивающаяся область. Между злоумышленниками и антиспуфинговым программным обеспечением идет война вооружений, а также проводятся академические исследования эффективности различных методов атаки и защиты.

**Поставщики распознавания лиц**

[По данным Electronic Frontier Foundation](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.eff.org/pages/face-recognition) , MorphoTrust, дочерняя компания [Idemia](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.morpho.com/en/media/ot-morpho-becomes-idemia-global-leader-trusted-identities-20170928) (ранее известная как OT-Morpho или Safran), является одним из крупнейших поставщиков средств распознавания лиц и других технологий биометрической идентификации в Соединенных Штатах. Он разработал системы для DMV штата, федеральных и государственных правоохранительных органов, пограничного контроля и аэропортов (включая TSA PreCheck) и государственного департамента. Среди других распространенных поставщиков - [3M](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://solutions.3m.com/wps/portal/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOJDDQx8LZwMHQ38fQPNDBwtHE0sAhwNDAPdTPWDU_PiQ4P1C7IdFQHlleBy/) , [Cognitec](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.cognitec.com/applications-law-enforcement.html) , [DataWorks Plus](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.dataworksplus.com/faceplus.html) , [Dynamic Imaging Systems](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.dynamicimaging.com/solutions/facial-recognition/) , [FaceFirst](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.facefirst.com/) и [NEC Global](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.nec.com/en/global/solutions/safety/Technology/index.html) .

В [тесте NIST Face Recognition Vendor Test](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf) перечислены алгоритмы от многих других поставщиков со всего мира. Существует также несколько алгоритмов распознавания лиц с открытым исходным кодом разного качества и несколько основных облачных сервисов, предлагающих распознавание лиц.

[Amazon Rekognition](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://aws.amazon.com/rekognition/) - это служба анализа изображений и видео, которая может идентифицировать объекты, людей, текст, сцены и действия, включая анализ лиц и настраиваемые метки. [Google Cloud API Зрения](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://cloud.google.com/vision) является pretrained изображения сервиса анализа , который может обнаруживать предметы и лицо, прочитать печатный и рукописный текст и метаданные сборки в свой каталог изображений. Google AutoML Vision позволяет обучать пользовательские модели изображений.

[API Azure Face](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://azure.microsoft.com/en-us/services/cognitive-services/face/) делает обнаружение лица, воспринимающее лицо и атрибуты в изображении, идентификации выполняет человек , который соответствует индивидуальному в своем частном хранилище до 1 миллиона людей, и выполняют воспринимаемое распознавание эмоций. Face API может работать в облаке или на границе в контейнерах.

**Наборы данных лиц для обучения распознаванию**

Есть [десятки торцовых наборов данных](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=https://www.face-rec.org/databases/) , доступных для скачивания , которые могут быть использованы для обучения распознавания. Не все наборы данных лиц равны: они, как правило, различаются размером изображения, количеством представленных людей, количеством изображений на человека, условиями изображений и освещением. У правоохранительных органов также есть доступ к закрытым наборам данных лиц, таким как текущие фотографии и изображения водительских прав.

Некоторые из более крупных баз данных лиц - это « [Лица с метками в дикой природе»](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://vis-www.cs.umass.edu/lfw/) , в которых содержится около 13 тысяч уникальных людей; [FERET](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.nist.gov/itl/iad/ig/colorferet.cfm) , используемый для ранних тестов NIST; [Mugshot](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.nist.gov/ts/msd/srd/nistsd18.cfm) база данных , используемая в продолжающемся NIST FRVT; [база](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.scface.org/) данных камер видеонаблюдения [SCFace](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.scface.org/) , также доступна [с ориентировками](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://atvs.ii.uam.es/atvs/scfacedb_landmarks.html) на [лицах](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.scface.org/) ; и [помеченные лица из Википедии](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://www.info.polymtl.ca/~mdhas/LWF/) с ~ 1,5 тыс. уникальных личностей. Некоторые из этих баз данных содержат несколько изображений для каждой личности. [Этот список](https://translate.google.com/translate?hl=ru&prev=_t&sl=en&tl=ru&u=http://web.mit.edu/emeyers/www/face_databases.html) от исследователя Итана Мейерса предлагает несколько убедительных советов по выбору набора данных о лицах для конкретной цели.

Таким образом, распознавание лиц улучшается, и производители учатся обнаруживать большую часть спуфинга, но некоторые применения этой технологии вызывают споры. По данным NIST, количество ошибок при распознавании лиц уменьшается вдвое каждые два года. Поставщики улучшили свои методы защиты от спуфинга, добавив сверточные нейронные сети.

Между тем, существуют инициативы по запрету использования распознавания лиц при слежке, особенно со стороны полиции. Однако полностью запретить распознавание лиц будет сложно, учитывая, насколько широко оно стало.