Автор: Александр Егоров  НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 
27.07.2020, 19:10 

# Как стать невидимкой

Ни для кого не секрет, что современные системы распознавания лиц представляют угрозу личной приватности. Уже сейчас такие системы ежедневно сканируют миллионы лиц в Китае, Великобритании и России без согласия граждан на это.

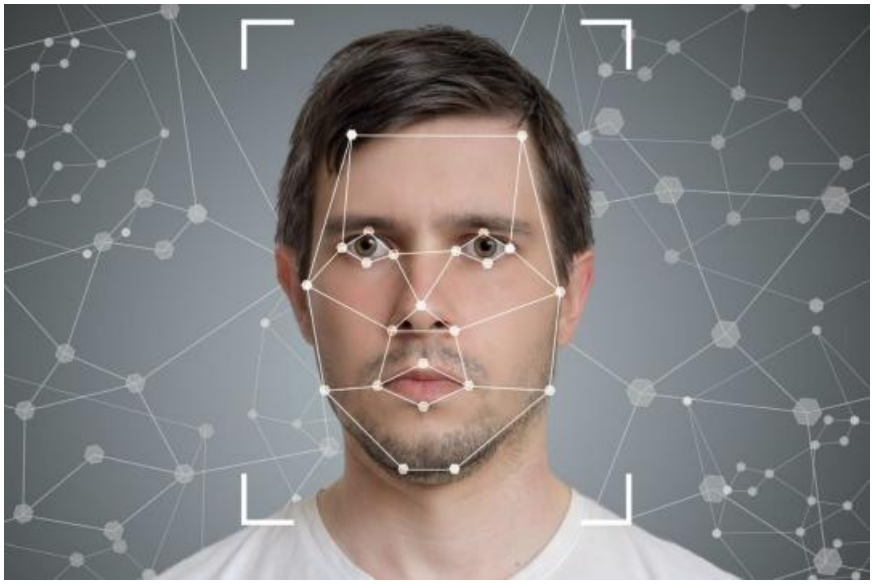
Исследователи из Чикагского университета придумали любопытный алгоритм клоакинга, который позволяет защититься от распознавания лиц.

Дело в том, что системы распознавания лиц берут фотографии для обучения своей системы из ваших открытых данных – в основном, из профилей в социальных сетях и других открытых источников.

Например, крупнейшая система распознавания лиц Clearview.ai для обучения использовала более трёх миллиардов фотографий из интернета и социальных сетей. Clearview.ai демонстрирует, насколько легко построить такую систему распознавания на снимках из Facebook и «Вконтакте».

Так вот, новый алгоритм Fawkes эффективно подрывает базу обучения «вражеской» нейросети. Перед публикацией каждой фотографии в ней делаются незаметные попиксельные изменения, после чего она становится не то что непригодной для использования при обучении, а буквально портит систему распознавания лиц.

Программа Fawkes работает локально на вашем компьютере и выполняет клоакинг фотографий. После обработки вы можете использовать фотографии как угодно – публиковать в социальных сетях, передавать друзьям или распечатывать на бумаге. В любом случае, для распознавания лиц они уже бесполезны, как показала проверка в ходе научного исследования чикагской группы.



Fawkes протестирован и показал эффективность 100% против самых известных моделей распознавания Microsoft Azure Face API и Amazon Rekognition.

Алгоритмы сжатия изображений тоже не портят защиту клоакинга. Исследователи проверяли материал на прогрессивном JPEG, который используется в Facebook и Twitter для пережатия картинок, на уровнях качества от 5 до 95. В общем, сжатие немного ослабляет защиту клоакинга, но при этом ещё более значительно снижается качество распознавания лиц.

Автор: Александр Егоров © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2817
27.07.2020, 19:10 0

*Также читайте эксклюзивную информацию в соцсетях:*
- *Телеграм*
- *ВКонтакте*

*Связаться с редакцией Бабра:*
*newsbabr@gmail.com*

Автор текста: **Александр Егоров**.

**НАПИСАТЬ ГЛАВРЕДУ:**

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

**ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:**

эл.почта: bratska.net.net@gmail.com

**КОНТАКТЫ**

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

**ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:**

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

**СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:**

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта