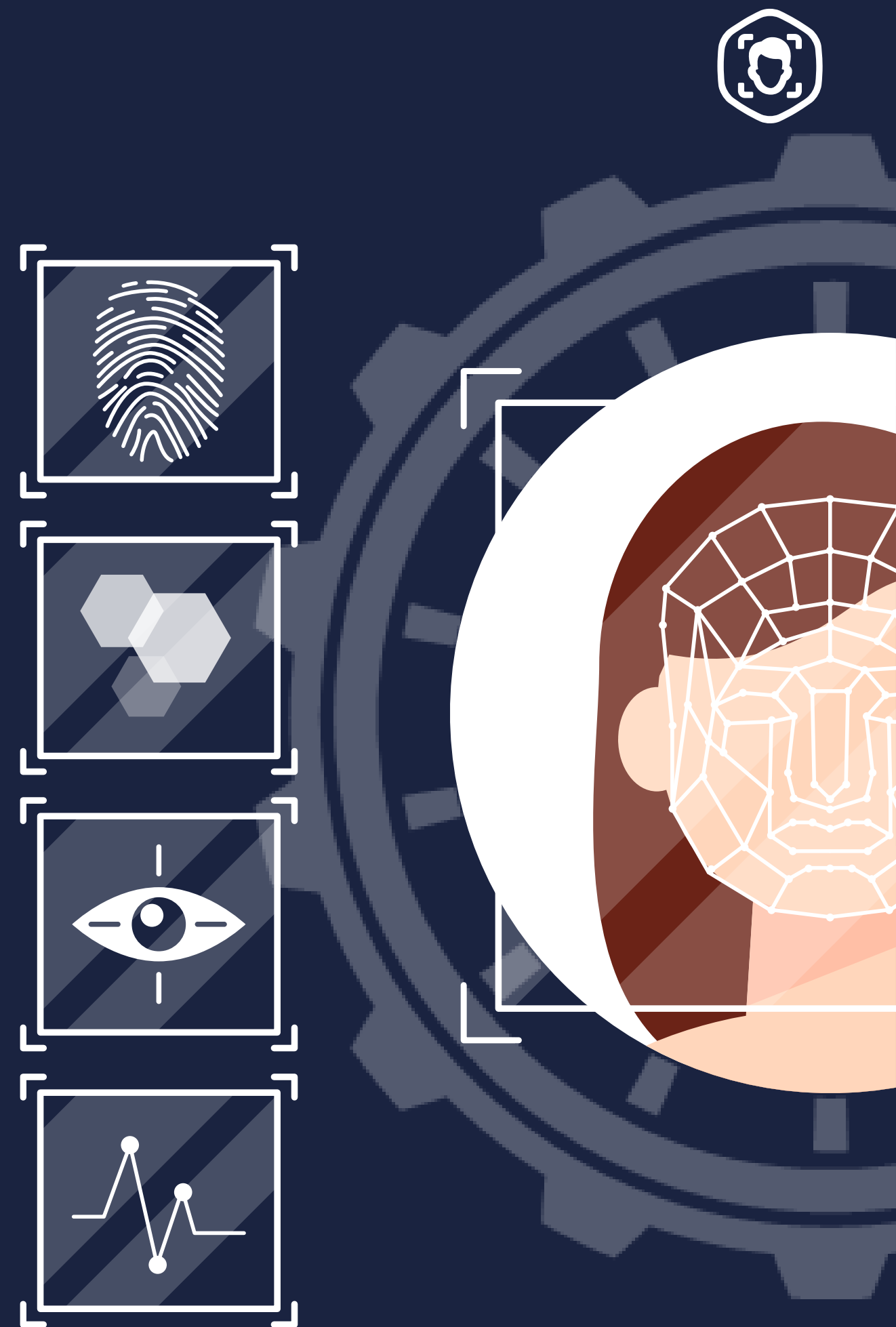


Поймай меня,
если сможешь!
Дипфейки в
биометрии: угроза
или искусство?



Почему дипфейки набирают популярность?



РОСТ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

По мере того, как биометрия находит все более широкое применение, мошенники становятся более изобретательными в методах атаки на биометрию. Количество случаев мошенничества с использованием биометрических данных увеличивается ежегодно в 2 раза.



ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ

Доступность алгоритмов, аппаратных ресурсов и баз данных упрощает реализацию атак. Реалистичность изображений, создаваемых генеративно-состязательными сетями (GAN) растет, а время создания дипфейков и требования к железу снижаются.

1.4k results (251 ms)

Sort by: Best match

Save

...



deepfakes/faceswap

Star

Sponsor

Deepfakes Software For All

machine-learning

deep-neural-networks

deep-learning

faceswap

neural-networks

Python · 47.5k · Updated 18 days ago



iperov/DeepFaceLab

Public archive

Star

DeepFaceLab is the leading software for creating **deepfakes**.

machine-learning

deep-neural-networks

deep-learning

faceswap

neural-networks

Python · 43.3k · Updated 18 days ago



lISourcell/deepfakes

Star

This is the code for "DeepFakes" by Siraj Raval on Youtube

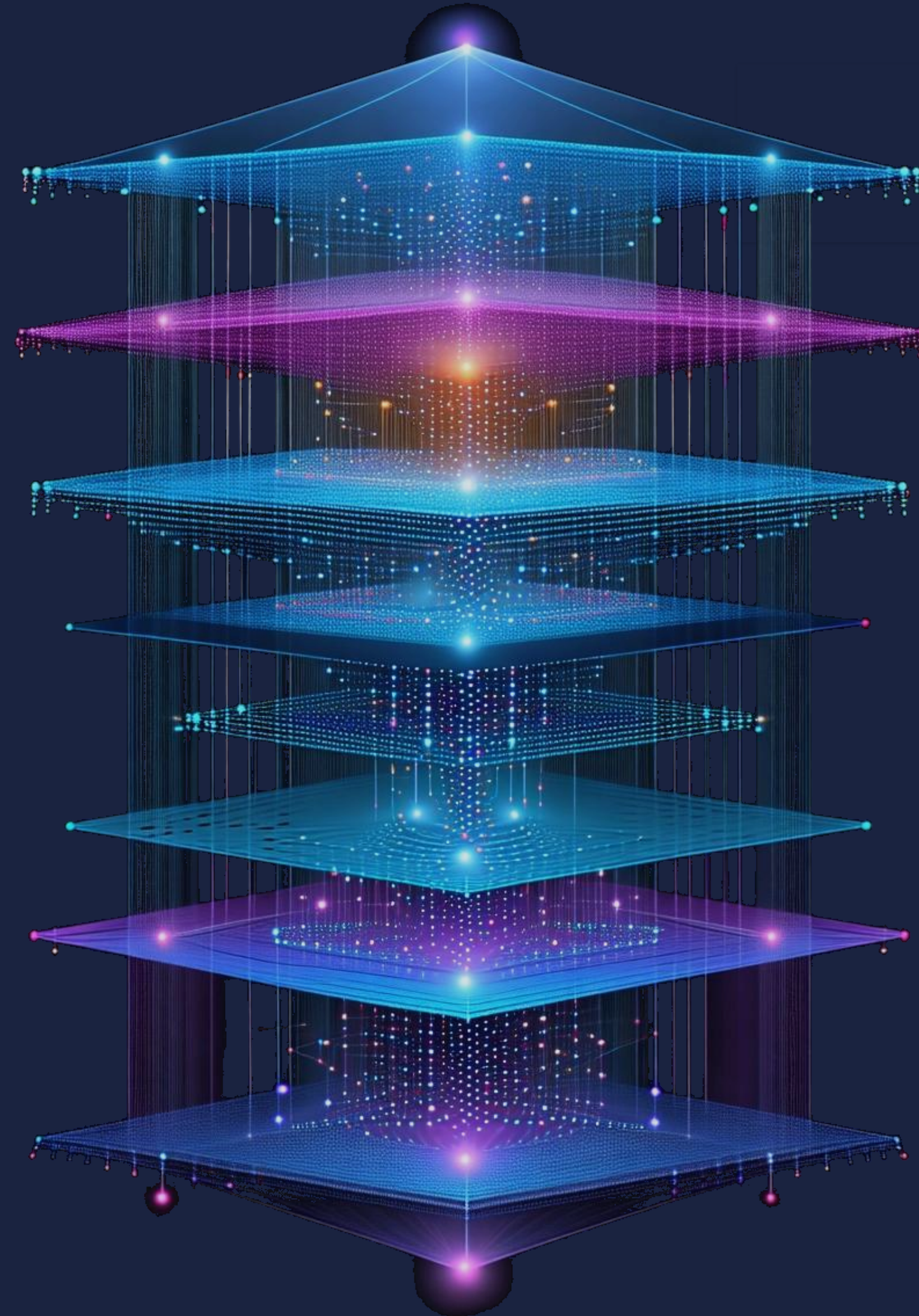
Python · 956 · Updated on 22 anp. 2021 r.

Нейронные сети в биометрии

Нейронные сети обучаются на данных.

Для эффективного обучения нейронных сетей требуются большие наборы данных, содержащие как легитимные, так и атакующие примеры.

Правильная настройка гиперпараметров необходима для оптимизации производительности и минимизации ложных срабатываний при обнаружении атак.



Атаки на биометрические системы

**пассивная
попытка
«самозванца»**

злоумышленник не прилагает никаких усилий, чтобы быть распознанным как другой человек, а просто использует свои собственные биометрические характеристики

**активная
попытка
«самозванца»**

Злоумышленник пытается совпасть с сохраненным шаблоном другого человека, предъявляя поддельный биометрический образец, либо намеренно изменяя свои собственные биометрические характеристики

Атаки на биометрические системы

пассивная
попытка
«самозванца»

злоумышленник не прилагает никаких усилий, чтобы быть распознанным как другой человек, а просто использует свои собственные биометрические характеристики

biometric recognition

активная
попытка
«самозванца»

Злоумышленник пытается совпасть с сохраненным шаблоном другого человека, предъявляя поддельный биометрический образец, либо намеренно изменяя свои собственные биометрические характеристики

liveness detection
deepfake detection

Liveness detection vs. Deepfake detection

Спуфинг предполагает использование поддельных биометрических признаков для получения несанкционированного доступа. Например, использование распечатанных фотографий или силиконовых масок для обмана биометрических систем.

Дипфейки— это синтетические данные, созданные с использованием технологий искусственного интеллекта (ИИ) и машинного обучения, которые реалистично заменяют внешность, голос, действия или иные характеристики физического лица или создают их с нуля.

Что такое дипфейк?

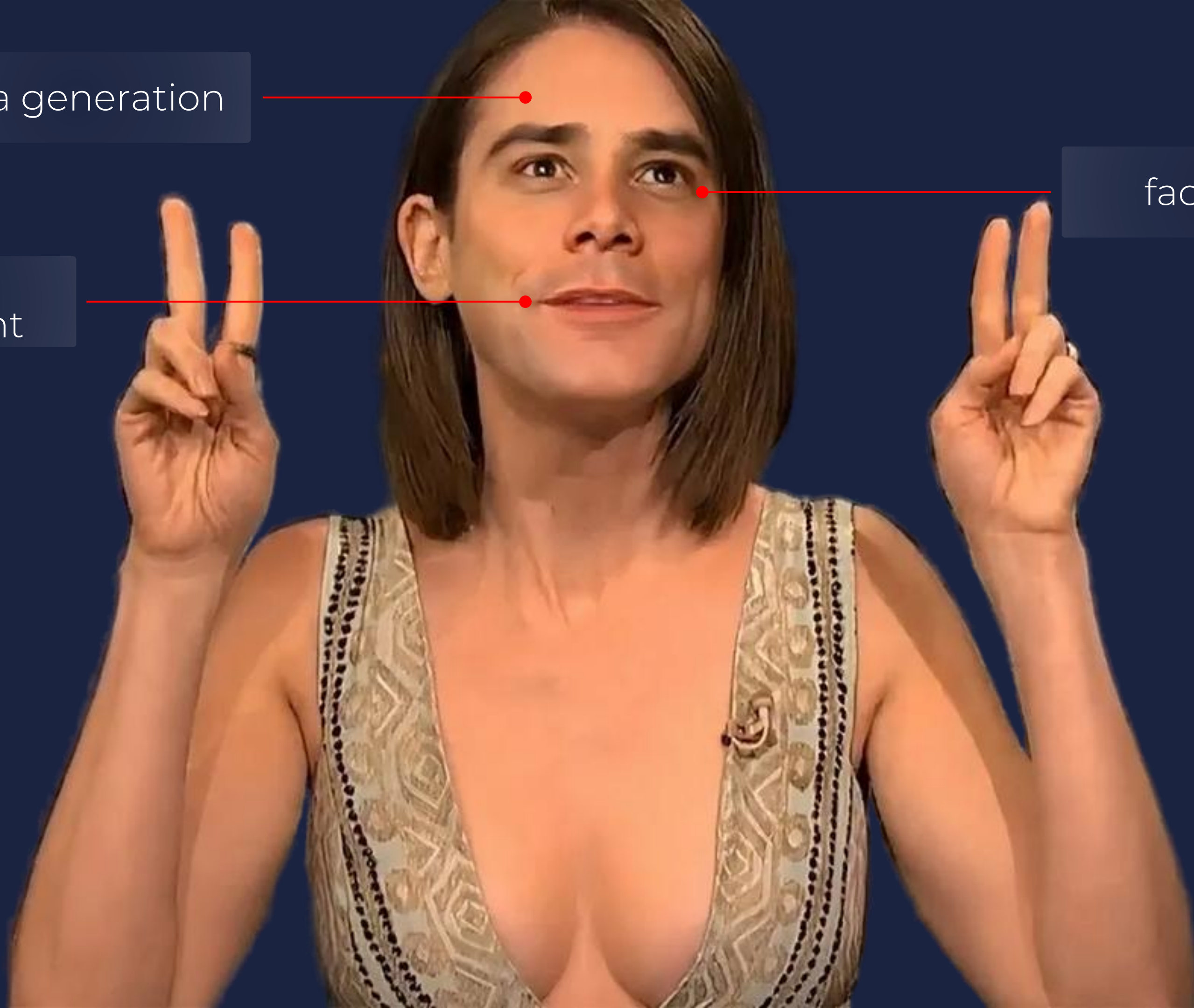
синтетические данные, созданные с использованием технологий искусственного интеллекта (ИИ) и машинного обучения, которые реалистично заменяют внешность, голос, действия или иные характеристики физического лица или создают их с нуля



data generation

facial
reenactment

face swap



Как создать дипфейк?

Генеративные нейронные сети стали неотъемлемой частью создания контента, изменив нашу повседневную жизнь, рекламу, киноиндустрию, политику и т.д.

Filter by

<> Code	227k
Repositories	9.4k
Issues	4k
Pull requests	621
Discussions	108
Users	291
More	

Languages

- Jupyter Notebook
- Python
- HTML
- JavaScript
- TypeScript
- CSS
- Java
- C++
- Dart
- TeX
- More languages...

Advanced

- Owner
- Size
- Number of followers
- Number of forks

9.4k results (260 ms)

 deepfakes/faceswap

Deepfakes Software For All

machine-learning

deep-neural-networks

deep-learning


faceswap

Python · 54k · Updated 4 days ago

 joshua-wu/deepfakes_faceswap

from deekfakes' faceswap: <https://www.reddit.com/user/deepfakes/>

Python · 3.1k · Updated on Feb 3, 2018

 IISourcell/deepfakes

This is the code for "DeepFakes" by Siraj Raval on Youtube

Python · 972 · Updated on Apr 22, 2021

 SCLBD/DeepfakeBench

A comprehensive benchmark of **deepfake** detection

Python · 760 · Updated 5 days ago

 aerophile/awesome-deepfakes

Everything **Deepfakes**


awesome

computer-vision

faceswap

deepfakes

1.6k · Updated on Jan 14, 2023

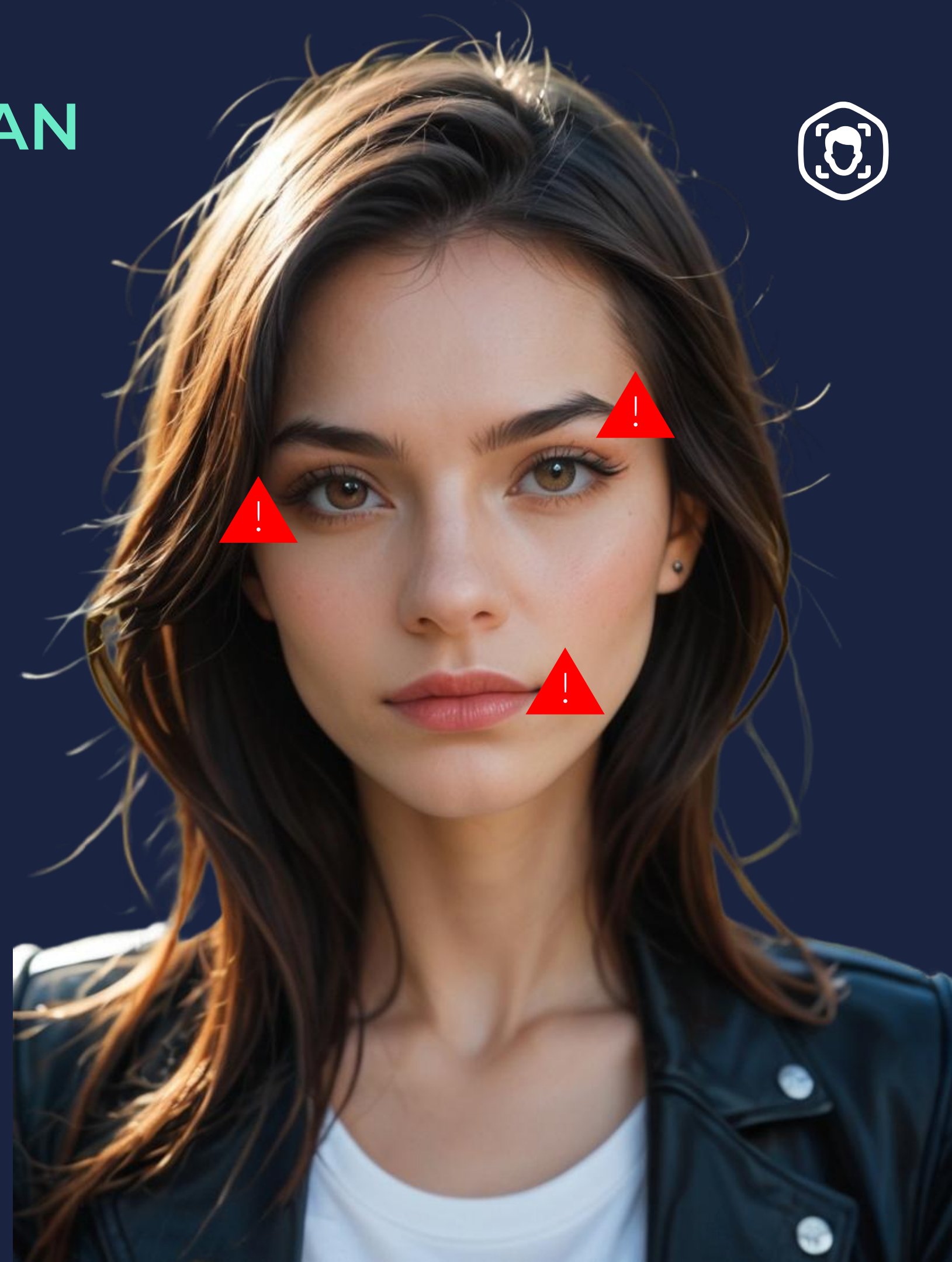
 sensity-ai/dot

The **Deepfake** Offensive Toolkit

Python · 4.3k · Updated on Jun 14, 2024

Как детектировать дипфейк: GAN против дипфейк детекторов

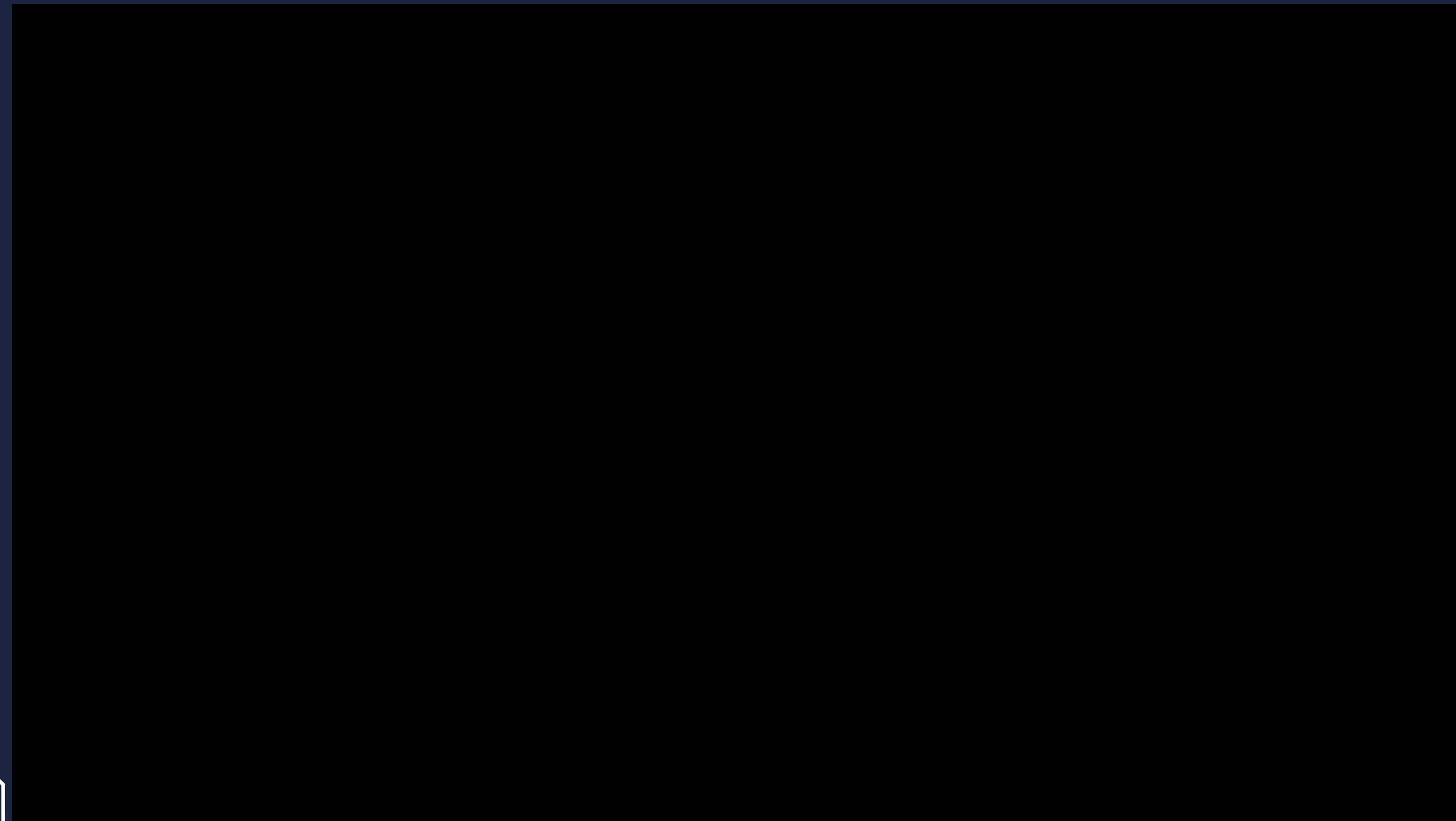
Нейронные сети обучаются на данных. Для эффективного обучения нейронных сетей для детекции дипфейков требуются большие наборы данных, включающие как реальные образцы, так и дипфейки. Для создания реалистичного дипфейка также требуются как можно больше данных



Как детектировать дипфейк?



Как детектировать дипфейк?



Почему детектировать дипфейк непросто?



Эволюция генеративных сетей

для генерации дипфейков

Малое количество реальных примеров

дипфейков, использованных для реальных атак

Увеличение доступности аппаратного обеспечения

для обучения генеративных нейронных сетей



Почему детектировать дипфейк непросто?

Одним из методов борьбы с дипфейками является маркировка искусственного контента. Но такие данные не подходят для обучения дипфейк детекторов, т.к. могут привести к отравлению обучающей базы данных



ОЦЕНКА АЛГОРИТМОВ



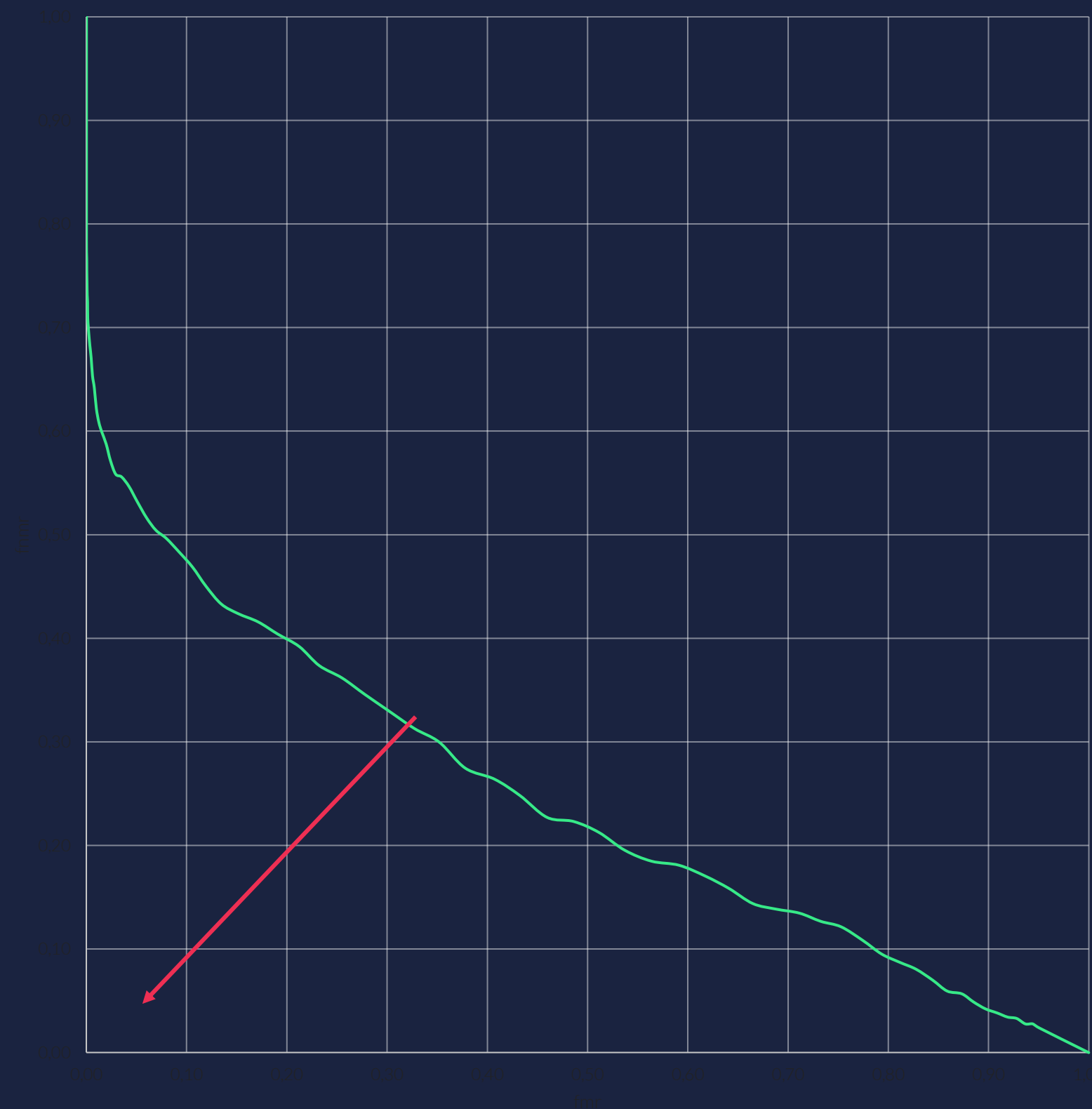
FAR

Доля попыток атак, которые будут ошибочно приняты

FRR

Доля попыток подлинного лица, которые будут ошибочно отвергнуты

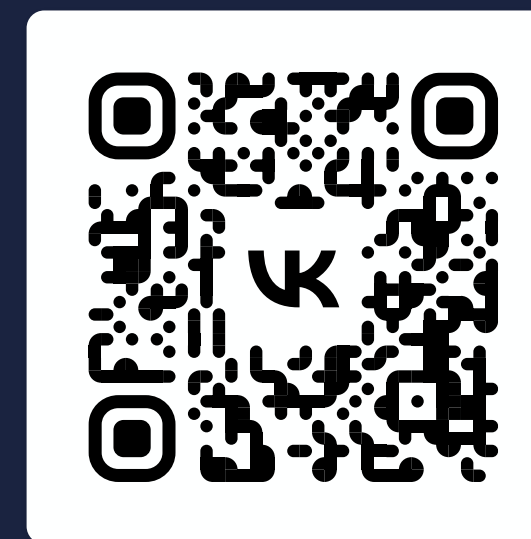
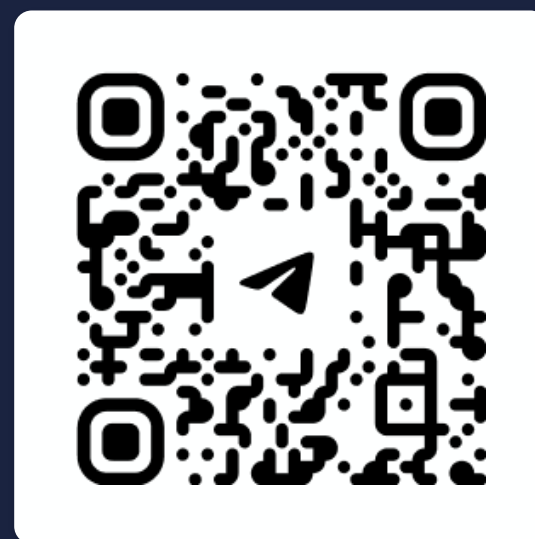
Изменяя пороговое значение, мы получаем пары значений ошибок



Мы на связи!



Официальный портал
ebs.ru



Социальные сети «Биометрия РФ»



Бессонова Наталья
natalya.bessonova@ebs.ru