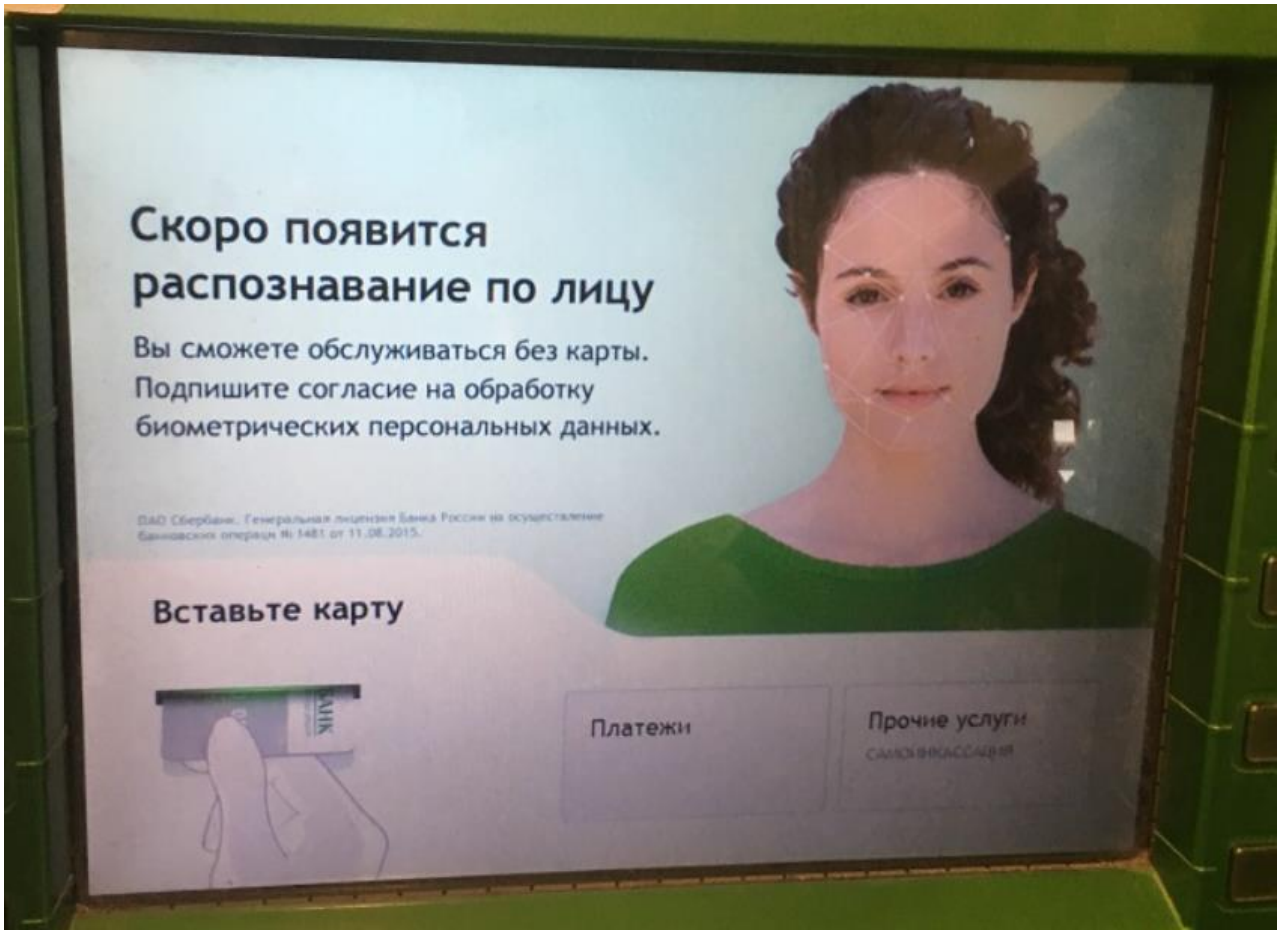
Во всех банках люди постоянно снимают деньги с банкоматов, используя при этом свою карту для ввода PIN-кода и выбором дальнейших операции. Сейчас все чаще и чаще существуют мошенники, которые способны украсть карту, получить незаметно PIN-код или даже получить допуск к банкомату для получения денег

Эксперты уточняют, что если злоумышленники будут использовать «плоскую картинку», где изображен человек в 2D, то легко смогут получить или воспроизвести мошенники, для получения данных о карте. При использовании 3D-изображения риск ниже, так как аферистам придется снимать человека с разных точек. Также неясно, как перевыпускать биометрический шаблон в случае его подделки. Если карту можно заменить, то с лицом клиента этого не сделаешь, отметили аналитики. В большинстве случаев, сейчас немало обсуждают о заказе новых банкоматах, в которых будут встроены биометрические АТМ, когда люди смогут снимать свои деньги используя при этом свои биометрические персональные данные



В биометрических АТМ можно будет совершать операции без пластиковой карты: банкомат распознает лицо или человека по его

внешности. Однако перед этим клиенту нужно будет предоставить кредитной организации свои биометрические данные, которые будут привязаны к счетам. Банкоматы нового поколения повысят безопасность операций, а также сделают процесс более удобным и быстрым, считают эксперты. Однако россияне пока недоверчиво относятся к биометрии, поэтому большой популярностью такие услуги в ближайшее время пользоваться не будут.

Обнаружение лица на фотографии относится к нахождению координат лица на изображении, тогда как локализация относится к разграничению границ лица, часто с помощью ограничивающей рамки вокруг лица.

Распознавание лиц — это проблема компьютерного зрения, которая включает поиск лиц на фотографиях.

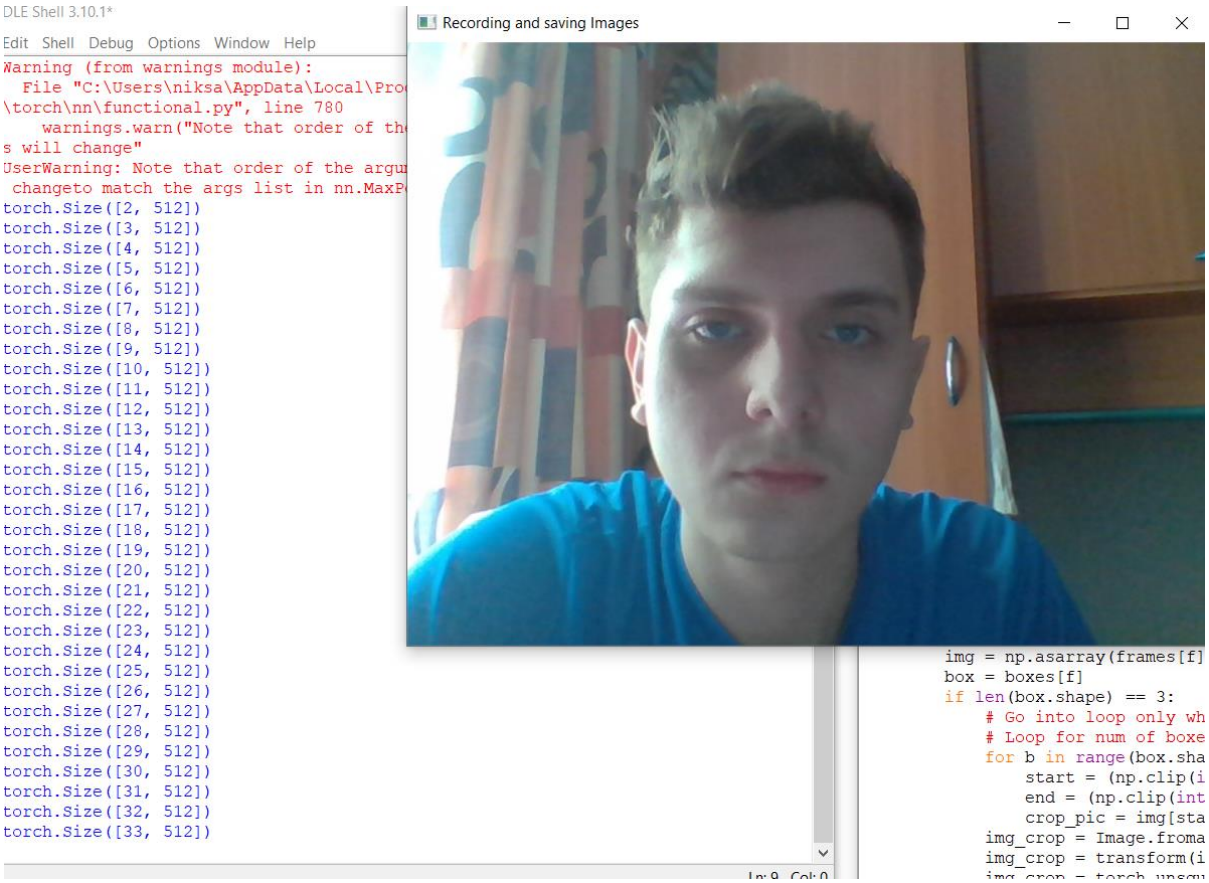
Это тривиальная проблема, которую может решить человек, и она достаточно хорошо решается с помощью классических методов, основанных на признаках, таких как каскадный классификатор. Совсем недавно методы глубокого обучения достигли самых современных результатов на стандартных наборах данных для обнаружения лиц. Одним из примеров является многозадачная каскадная сверточная нейронная сеть, или сокращенно MTCNN.

Работа алгоритма банковской системы:

К данному алгоритму посылаются номер кредитной карты пользователя для записи в определенную БД. После ввода нужно вписать имя владельца карты.

```
===== RESTART: C:\Users\niksa\Documents\HSE\Аутентификация\input_images.py =====
Enter the card number: 1234
Enter the person's name: nik
Try to keep your face at the centre of the screen and turn ur face slowly in ord
er to capture diff angles of your face
A window will pop up in abt 3 seconds
```

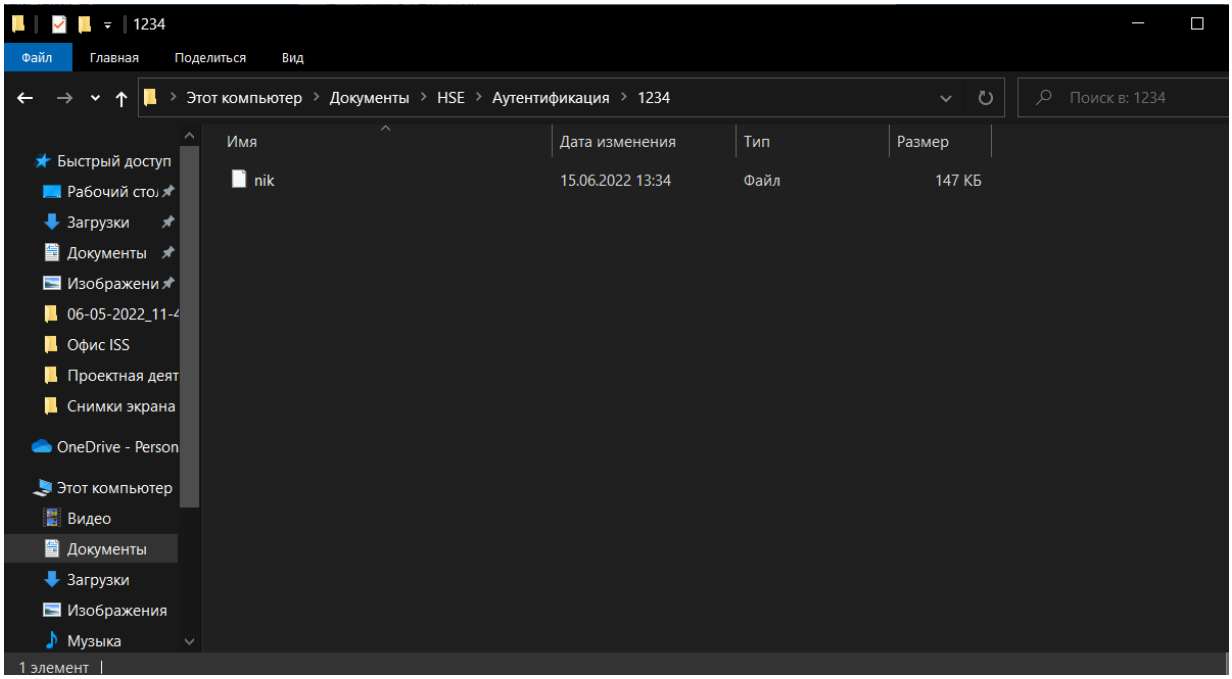
Затем алгоритм попросит Вас показать свое лицо на камеру в центр экрана. Лицо можно двигать медленно, чтобы модель нейронной сети смогла определить углы лица и построить ограничительную рамку для распознавания лица по аутентификации.



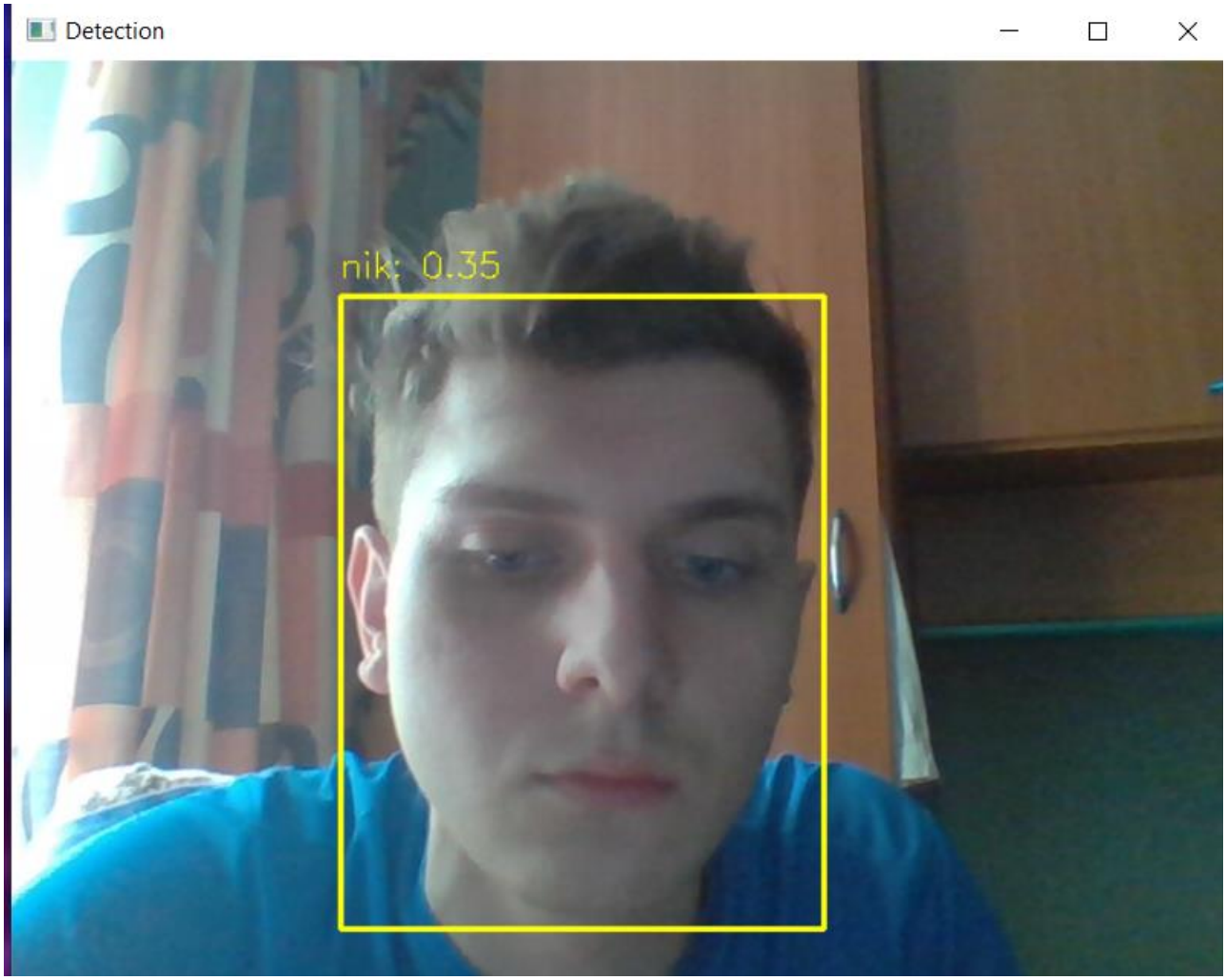
Чтобы воспроизвести запись в базу данных, нужно включить веб-камеру. Модель нейронной сети воспроизведет запись около 3 секунд, чтобы определить лицо человека. При запуске веб-камеры записываются некоторые тензоры матриц из пакета Pytorch. Аутентификация происходит по следующим параметрам:

- Глаза
- Нос
- Рот
- Шея
- Уши

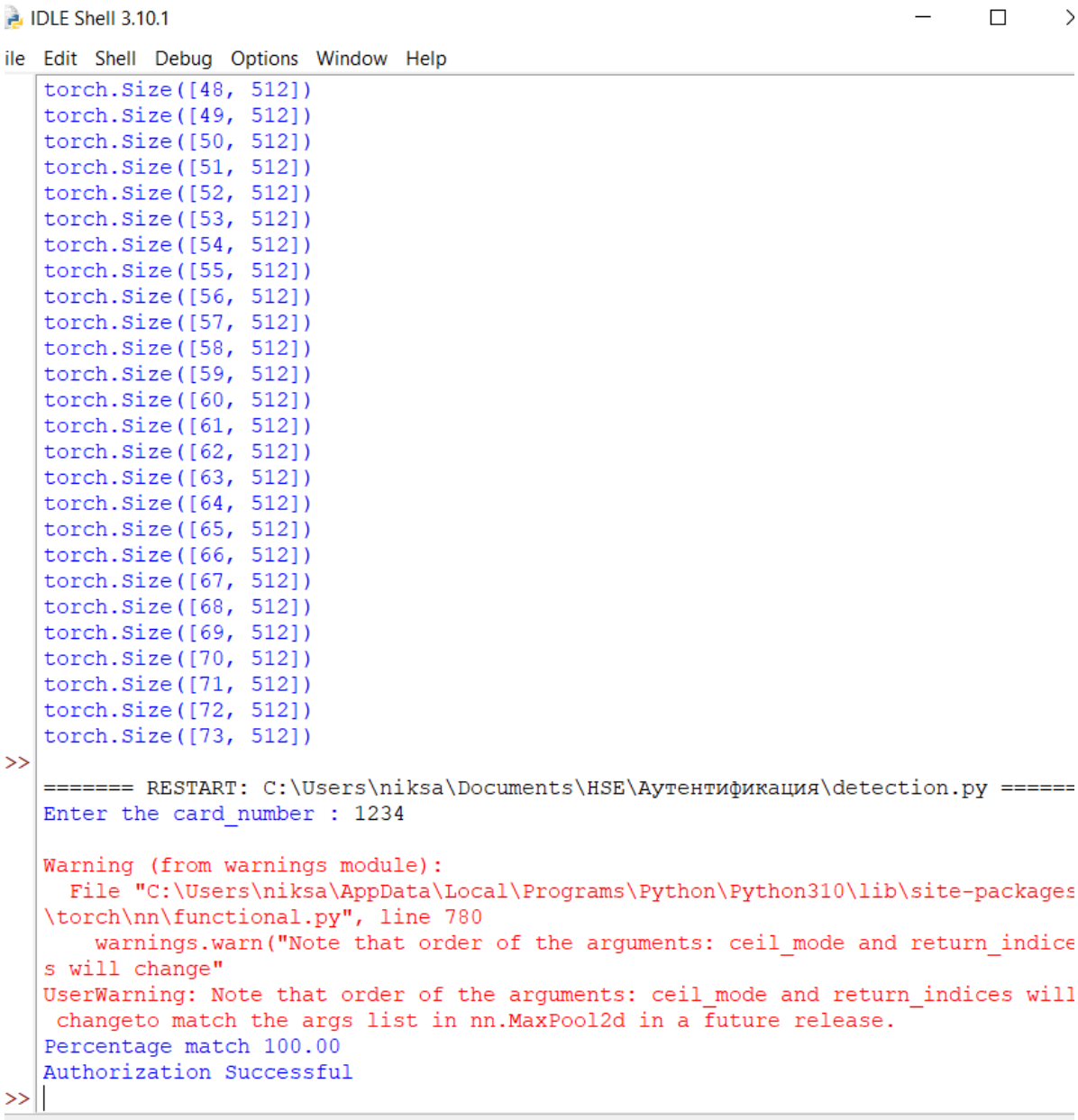
Обратите внимание, что запись происходит в папку, когда пользователь указывал номер карты. В нем хранится видеозапись пользователя для дальней двухфакторной аутентификации по карте. Видеозапись длится около 3 секунд. Саму видеозапись пришлось зашифровать “сторонним” форматом, чтобы злоумышленники не смогли получить доступ к данным и не “отравить” их



Далее, если запустить второй код детекции, то модель нейронной сети попросит пользователю ввести данные карты. После этого модель включит веб-камеру и наложит ограничительную рамку распознавания лица.



На первый план выходит имя владельца карты, а на второй якобы условная вероятность появления лица владельца карты.



В реализации использовалась модель mtcnn.

В сети используется каскадная структура с тремя сетями; сначала изображение масштабируется до диапазона различных размеров (называемого пирамидой изображения), затем первая модель (Proposal Network или P-Net) предлагает возможные области лица, вторая модель (Refine Network или R-Net) фильтрует ограничивающие рамки, а третья модель (Output Network или O-Net) предлагает ориентиры лица.

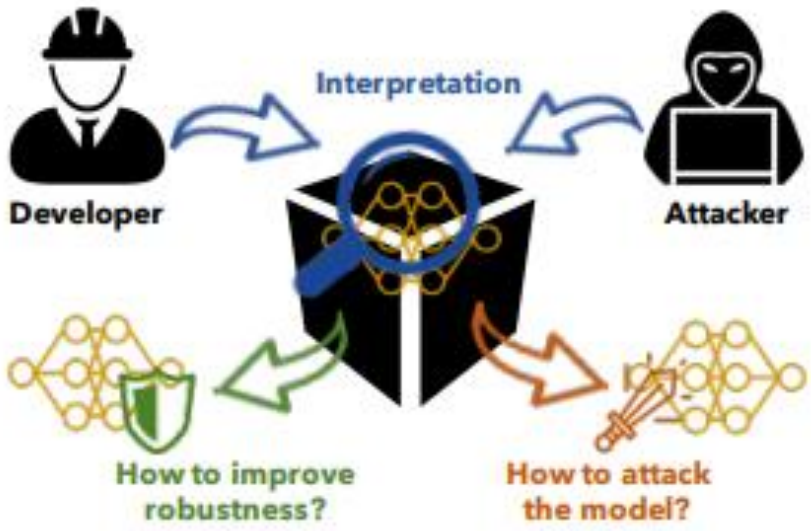
Модель называется многозадачной сетью, потому что каждая из трех моделей в каскаде (P-Net, R-Net и O-Net) обучена выполнению трех задач,

например, делать три типа прогнозов; это: классификация лиц, регрессия ограничивающей рамки и локализация ориентиров лица.

Три модели не связаны напрямую; вместо этого выходные данные предыдущего этапа подаются в качестве входных данных для следующего этапа. Это позволяет выполнять дополнительную обработку между этапами; например, немаксимальное подавление (NMS) используется для фильтрации ограничивающих рамок-кандидатов, предложенных P-Net первого этапа, до предоставления их модели R-Net второго этапа.

Архитектура MTCNN достаточно сложна для реализации. К счастью, существуют реализации архитектуры с открытым исходным кодом, которые можно обучать на новых наборах данных, а также предварительно обученные модели, которые можно использовать непосредственно для обнаружения лиц.

Блок-схема



С одной стороны, если противники знают, как работает целевая модель, они могут использовать ее для нахождения слабого места модели и соответственно инициирования атаки. С другой стороны, если разработчики модели знают, как модель работает, они могли определить уязвимость и работать над исправлением заранее. Интерпретация относится к понятной человеку информации, объясняющей, что имеет модель. В данном случае в этом алгоритме защитили видеоданные владельца карты, чтобы злоумышленник не смог никоем образом открыть и испортить данные