

# Люди в масках

Михаил Сысак

Лаборатория финансовых технологий, МФТИ

3 июля 2020 г.

# Постановка задачи

- ▶ Люди в солнечных очках, масках, капюшонах
- ▶ При использовании банкомата затрудняется идентификация
- ▶ На встрече с представителем может получиться плохое фото для базы
- ▶ Возможно умышленное использование окклюзий

# Постановка задачи

## 1. Ранжирование закрытий

- ▶ Выяснить, какие закрытия влияют сильнее
- ▶ Отранжировать окклюзии по этому показателю

## 2. Построение модели

- ▶ Модель, дающая численную оценку того, насколько закрыто лицо
- ▶ Предсказать, что идентификация затруднена

## Cropped Labeled Faces in the Wild (LFWcrop)



## Шаблоны различных закрытий, их композиции



- ▶ Модель Face Recognition из библиотеки dlib
- ▶ Отображает изображение  $150 \times 150$  в вектор размерности 128
- ▶ Если расстояние между векторами превышает некоторый порог  $T$ , то они принадлежат разным людям

# Методы

## Ранжирование закрытий

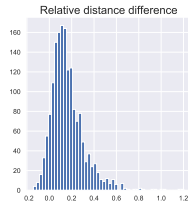
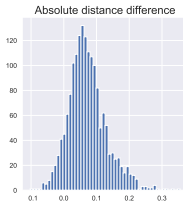
- ▶ Для человека рассматривается кластер его фотографий в латентном пространстве
- ▶ На фотографии накладывается закрытие, рассматривается второй кластер
- ▶ Межкластерное расстояние  $R$ , внутрикластерное расстояние чистых фотографий  $r$
- ▶ Распределение абсолютных  $R - r$  и относительных  $\frac{R - r}{r}$  разностей
- ▶ Доля случаев, когда человек перестает распознаваться из-за закрытия

# Результаты

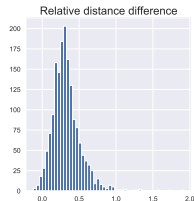
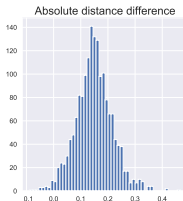
## Ранжирование закрытий

Для каждого закрытия получены два распределения и вероятность затруднения идентификации

Identity\_WhiteMask\_Identity  
Misidentification: 17.5%



Sunglasses\_Identity\_Hood  
Misidentification: 67.7%



# Результаты

## Ранжирование закрытий

### Окклюзии отранжированы по вероятности затруднения идентификации

Eyes	Mouth	Head	ID fault share, %
Identity	Identity	Identity	0.00
Eyepatch	Identity	Identity	11.87
Identity	Scarf	Identity	15.51
Identity	WhiteMask	Identity	17.47
Identity	Identity	Hood	23.88
Identity	BlackMask	Identity	26.10
Sunglasses	Identity	Identity	26.77
Eyepatch	Scarf	Identity	37.12
Eyepatch	WhiteMask	Identity	40.85
Eyepatch	Identity	Hood	45.19
Identity	Scarf	Hood	52.58
Eyepatch	BlackMask	Identity	56.39

Eyes	Mouth	Head	ID fault share, %
Identity	BlackMask	Hood	66.57
Sunglasses	Identity	Hood	67.67
Eyepatch	Scarf	Hood	70.30
Sunglasses	WhiteMask	Identity	72.56
Identity	WhiteMask	Hood	78.71
Sunglasses	Scarf	Identity	85.22
Eyepatch	BlackMask	Hood	88.48
Sunglasses	BlackMask	Identity	89.06
Sunglasses	Scarf	Hood	94.06
Eyepatch	WhiteMask	Hood	95.00
Sunglasses	WhiteMask	Hood	95.88
Sunglasses	BlackMask	Hood	96.95



# Методы

## Построение модели

- ▶ Даны пары фотографий одного человека  $A, B$
- ▶ Ко второй фотографии применяется окклюзия, получается закрытая фотография  $B'$
- ▶ В качестве метки выступает разность расстояний в латентном пространстве

$$y = \|B' - A\| - \|B - A\|$$

- ▶ Строится модель, предсказывающая по закрытой фотографии метку  $y$
- ▶ Архитектура модели — MobileNet

### Примеры из обучающей выборки



- ▶ Вычисляется среднее исходных расстояний

$$t = \text{mean}(\|B - A\|)$$

- ▶ По меткам строится бинарный флаг затрудненной идентификации

$$[y > T - t]$$

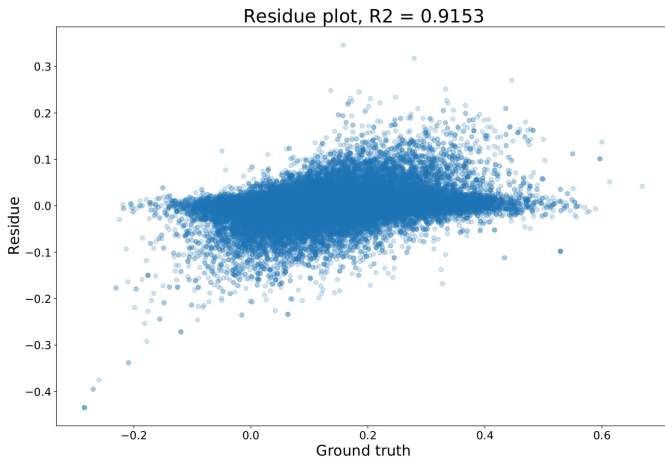
- ▶ По бинарному флагу и пресказаниям сети строится ROC-кривая, вычисляется наилучший threshold  $y_0$
- ▶ Предсказание модели  $p$  отображается в вероятность

$$P(\text{Идентификация затруднена}) = \sigma \left( \frac{p}{y_0} - 1 \right)$$

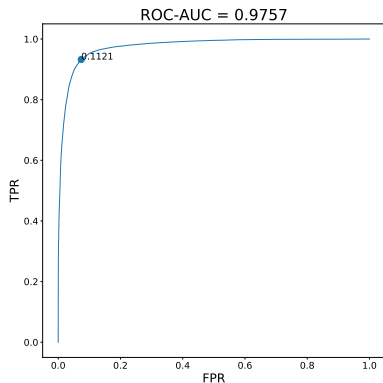
# Результаты

## Построение модели

График остатков ( $y - \hat{y}$  от  $y$ ) и  $R^2$  score



### ROC-кривая и ROC-AUC score



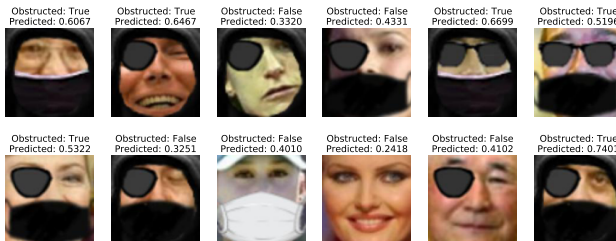
FPR, %	TPR, %	Threshold
0.00	0.00	1.627
0.09	32.40	0.220
0.30	42.67	0.198
1.00	62.60	0.163
2.99	81.44	0.133
10.00	95.21	0.106
30.00	98.62	0.079

# Результаты

## Построение модели

- ▶ Наилучший threshold: 0.112
- ▶ FPR при наилучшем threshold: 7.38%
- ▶ TPR при наилучшем threshold: 93.24%

### Примеры предсказаний модели



# Дальнейшие исследования

- ▶ Рассмотрение поворотов лица в качестве окклюзий
- ▶ Валидация на независимом датасете
- ▶ Использование более сложных архитектур, более долгое обучение модели
- ▶ Генерация закрытий по основным точкам лица (лендмаркам)
- ▶ Проверка работы методов на реальных данных