

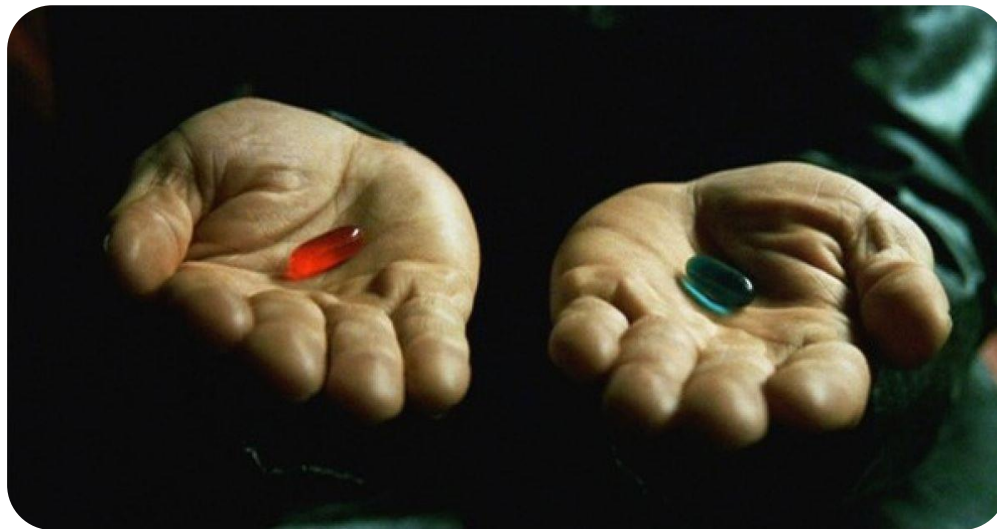
Как правильно сравнивать алгоритмы распознавания лиц

Что стоит за рекламой



Многообразие решений

- На рынке свои технологии и решения предлагает множество разработчиков: в тесте NIST представлено почти 40 различных алгоритмов распознавания лиц
- Однако, создание по-настоящему точного, надежного и быстрого алгоритма является весьма непростой задачей
- Как понять, какое из предлагаемых решений действительно лучше всего подходит под задачу?



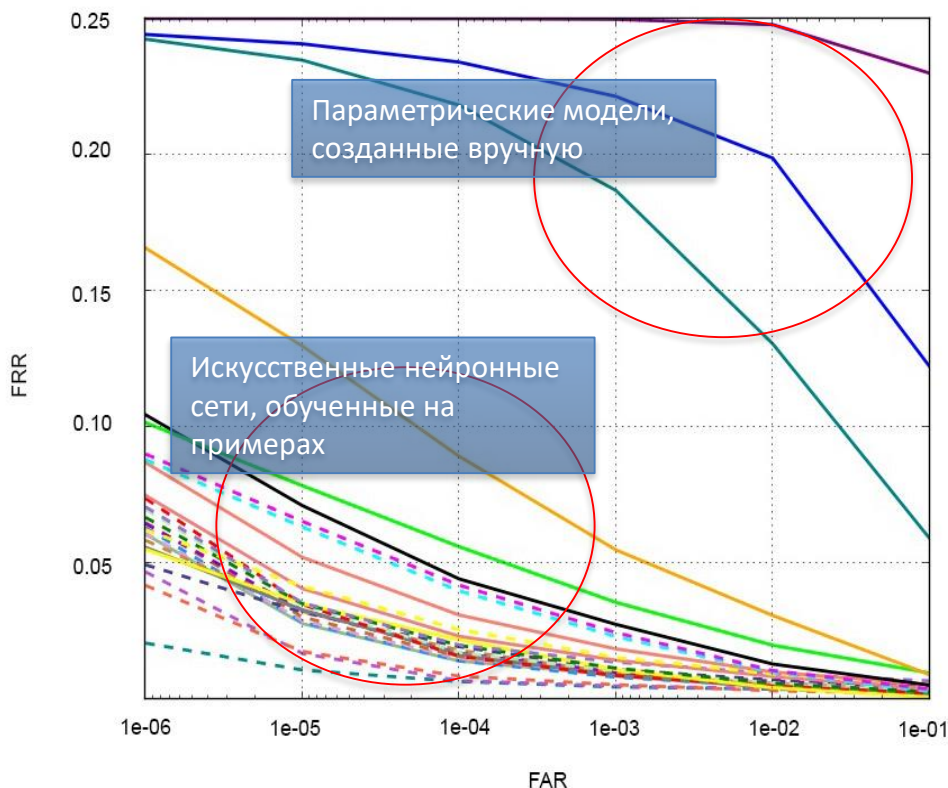
Сравнение различных проектов тестирования

Название конкурса	Кто проводит	Тип изображений	Размер тестовой базы	Тестовые данные	Метрики
LFW	Университет Массачусетса	Знаменитости, публичные персоны	10,000	Тестовые данные публичны	Низкий коэффициент ложного принятия (1/1000). Нет возможности установить разницу между алгоритмами: 32 алгоритма показывают результат >99%
MegaFace	Университет Джорджа Вашингтона	Знаменитости, публичные персоны	1,000,000	Тестовые данные публичны	Большой объем базы позволяет выявлять различия между алгоритмами
FRVT	NIST	Официальные данные правительства США из миграционных и полицейских БД	1,000,000	Тестовые данные не публичны (слепой тест)	Самая большая база изображений, FAR= 1/10,000,000

Источник: YITU

Нейросетевые vs. параметрические алгоритмы

- Параметрические модели базируются на расчетах взаимного расположения заданных заранее точек – такие модели **программируют**
- Искусственные нейронные сети в процессе **обучения** сами «находят» зависимости и рассчитывают оптимальные значения
- Нейронные сети во много раз эффективнее параметрических алгоритмов

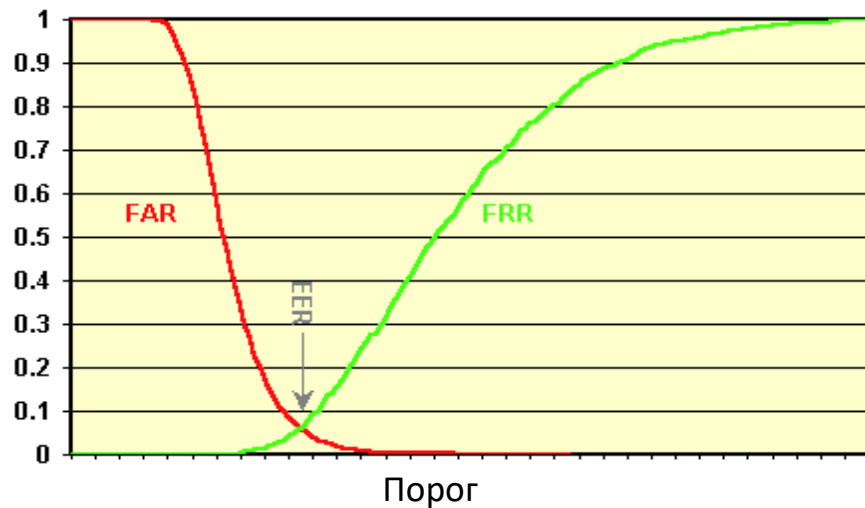


Два типа ошибок

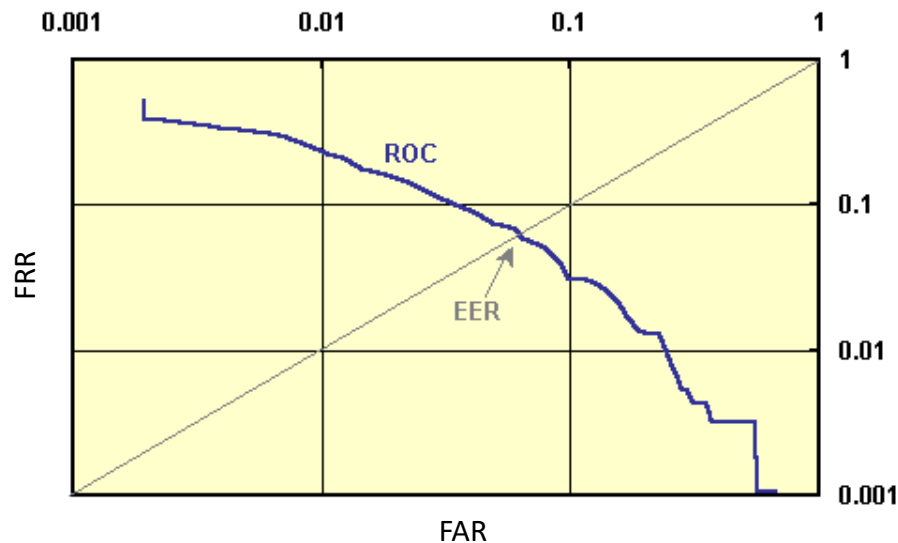
- Ошибка первого рода – это **ложноположительный результат**, то есть ошибочное принятие *разных* людей за одного и того же человека. В таблицах рейтингов этот тип ошибки может также называться False Acceptance Rate (FAR) или False Match Rate (FMR)
- Ошибка второго рода – **ложноотрицательный результат**, то есть система не распознает одного и того же человека на разных фотографиях, считая, что это разные люди. Этот показатель может обозначаться как False Rejection Rate (FRR) или False Not-Match Rate (FNMR)
- FAR и FRR тесно связаны – их всегда надо рассматривать вместе

Как строится кривая ROC-кривая («кривая ошибок»)

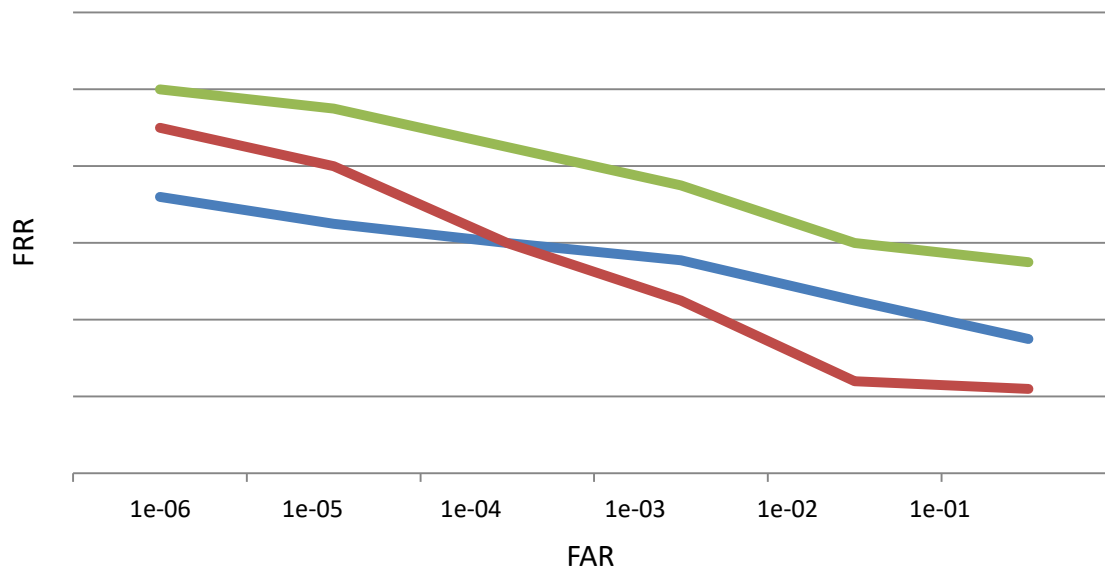
Диаграмма FAR - FRR



ROC-кривая



Какой алгоритм лучше?



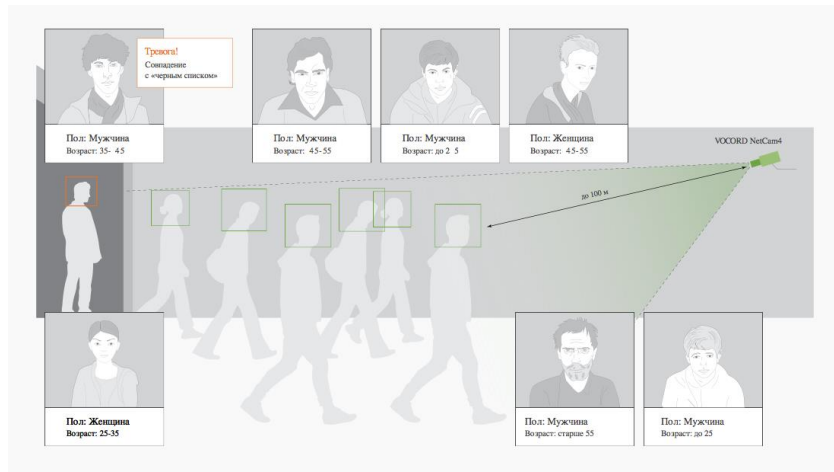
Если графики пересекаются, то нужно выбирать алгоритм с лучшими характеристиками именно в том диапазоне, который требуется для решения задачи

Как определить процент ложных срабатываний

- Определите область применения. Где будет использоваться система?
 - Удаленная идентификация в мобильном приложении, банкомате
 - Поиск разыскиваемых лиц в толпе
 - Системы контроля доступа и пр.
- Определите параметры системы:
 - Число лиц в эталонной базе
 - Допустимое количество ложных срабатываний в единицу времени
 - Допустимый уровень ложных пропусков
- Вычислите допустимый процент ложных срабатываний (FAR):
 - $$FAR = \frac{\text{допустимое количество ложных срабатываний в единицу времени}}{\text{количество лиц фиксируемых в единицу времени}} \times \text{размер эталонной базы}$$
- Выберите алгоритм с наименьшим процентом ложных пропусков (FRR) при найденном FAR

Пример 1. «Массовое» распознавание

- *Задача: выявление разыскиваемых лиц на станции метро*
- Эталонная база (база розыска): 10 000 лиц
- Количество сравнений («проход» перед камерой): 1000 человек/час
- Количество сравнений:
 $10000 \times 1000 = 10\,000\,000$ сравнений/час
- Ошибка ложного принятия $FAR=1\%$
- Число ложных тревог: $1\,000\,000 \times 1\% = 100\,000$ ложных тревог в час!
- Оператор не сможет обработать такое количество срабатываний => система не работоспособна
- Если исходить из того, что оператор может обрабатывать в час 10 тревог FAR должна быть **не более 0,0001% (1×10^{-6})**



Пример 2. Аутентификация пользователя / СКУД

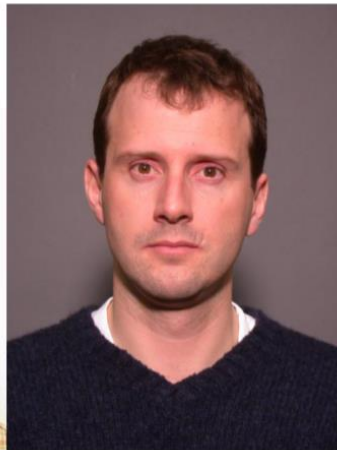
- *Задача: проверка, что представленное изображение соответствует эталонному изображению, хранящемуся в базе (сравнение 1 к 1) и предоставить соответствующие права доступа*
- В этом случае FAR определяет вероятность проникновения постороннего человека в охраняемое помещение / неавторизованный доступ в ИТ-систему
- FAR является критичным и мы можно установить его на минимум, несмотря на неизбежное увеличение FRR
- Высокий FRR означает, что человек, имеющий права, не получает доступ
- НО, это будет означать лишь необходимость дополнительной попытки авторизации



Результаты зависят исходных данных



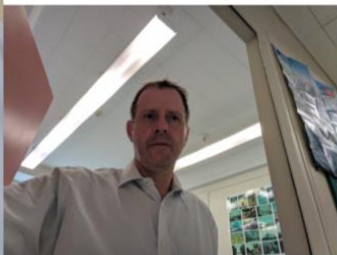
(a) Visa



(b) Mugshot



(c) Webcam



(d) Selfie

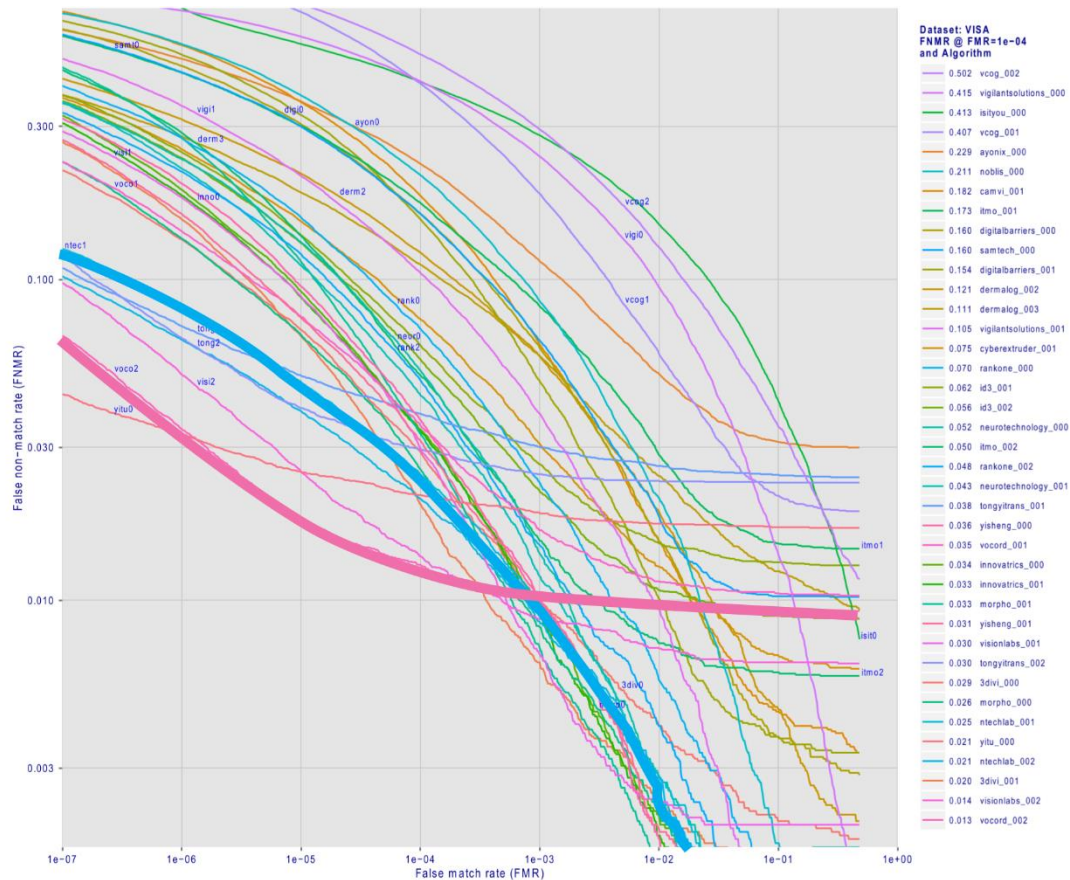


(e) Wild

База Visa – «хорошие» фото



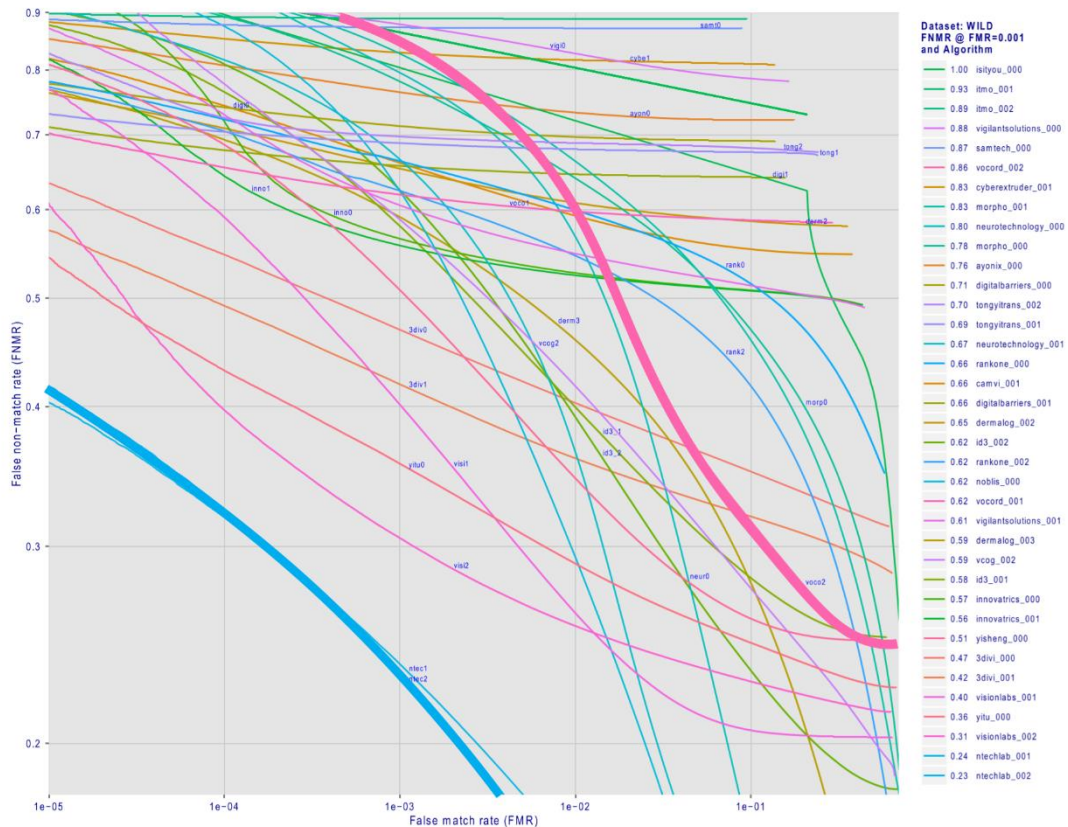
(a) Visa



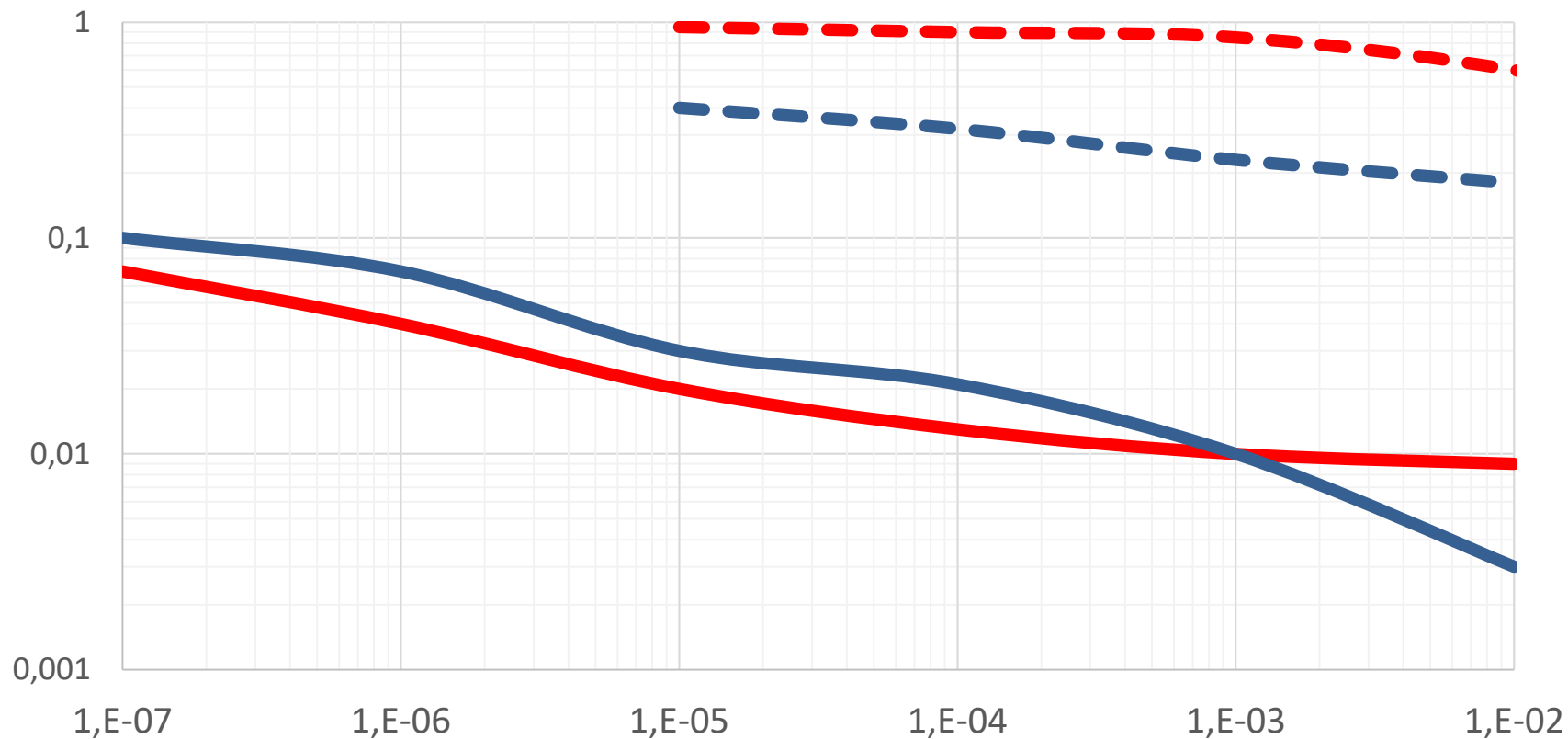
База Wild – «плохие» фото



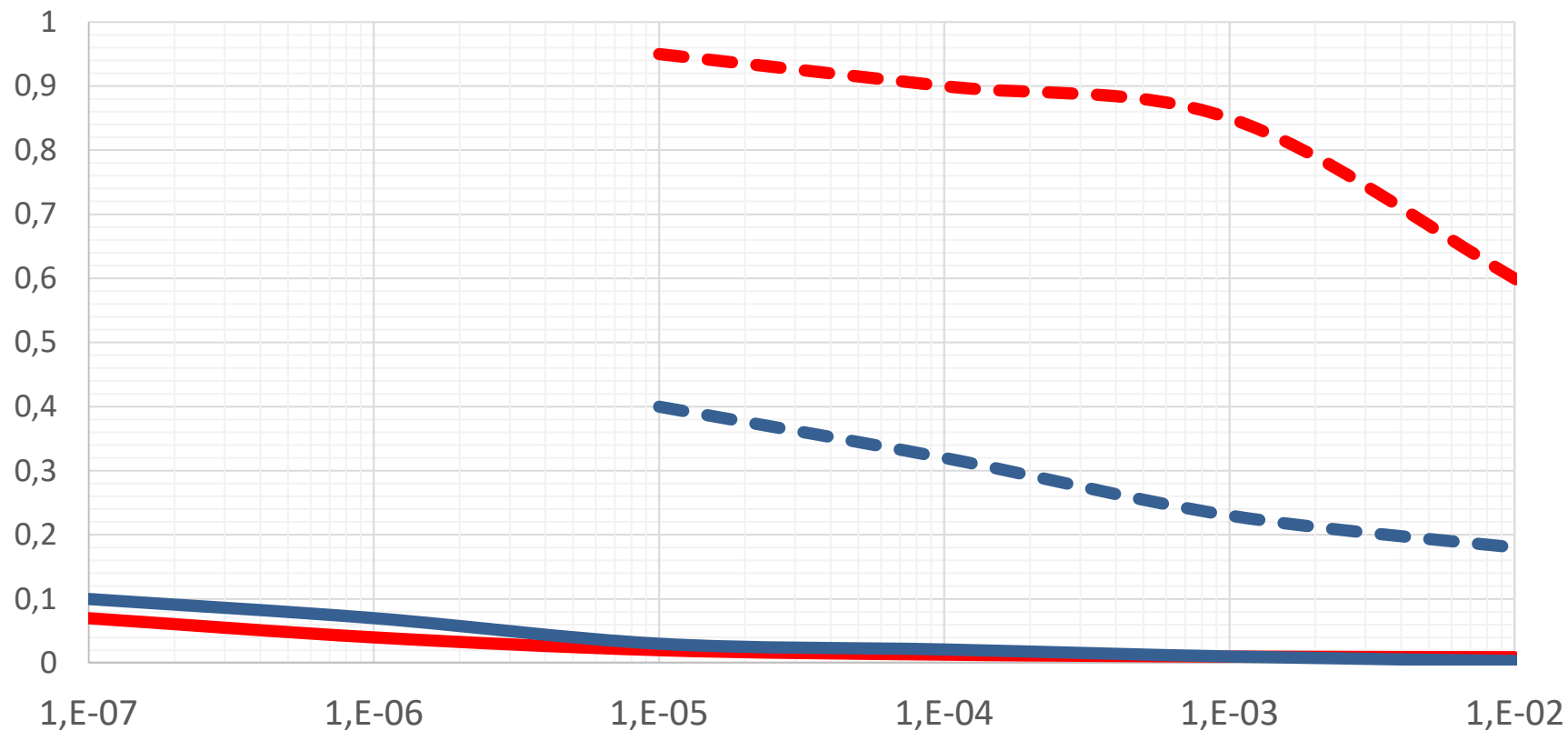
(e) Wild



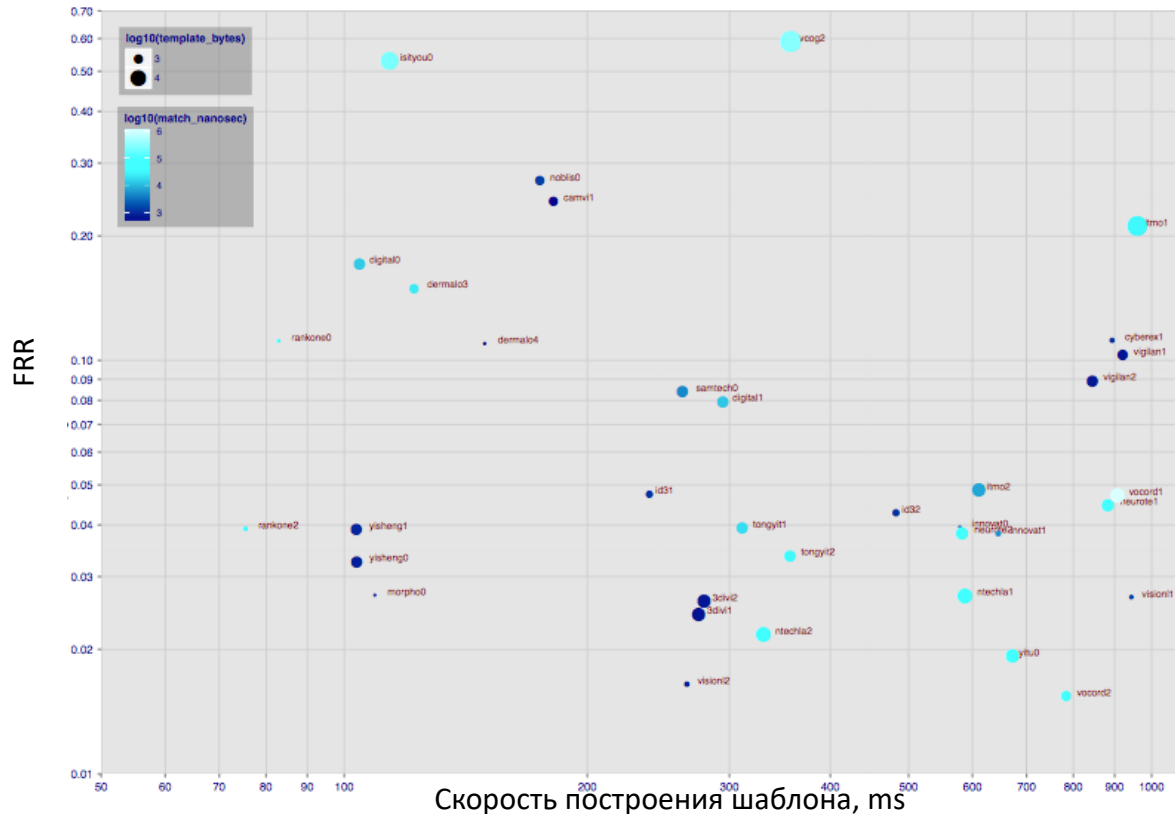
А теперь все вместе...



... и в линейном масштабе



Быстрее, меньше, точнее!



$FAR = 10^{-4}$; диаметр меток соответствует размеру шаблона (в байтах)

Скорость работы алгоритмов распознавания

Интересны два параметра:

1. Скорость сравнения (поиска по базе) – измеряется в наносекундах и на небольших базах мало дифференцирует алгоритмы
2. Скорость вычисления биометрического шаблона – сильно зависит от платформы

Template		GPU	Comparison Time (ns) ³	
Size (B)	Time (ms) ²		Genuine	Impostor
²⁸ 4096 ± 0	¹⁷ 274 ± 47	Yes	⁴ 636 ± 19	⁵ 634 ± 16
²⁹ 4096 ± 0	¹⁸ 279 ± 48	Yes	⁷ 692 ± 22	⁸ 707 ± 26
¹³ 1036 ± 0	¹ 18 ± 2	No	³ 621 ± 23	⁴ 620 ± 26
¹² 1024 ± 0	¹³ 181 ± 6	No	¹ 481 ± 16	³ 487 ± 23
⁷ 256 ± 0	³⁴ 893 ± 25	No	¹³ 1083 ± 16	¹⁵ 1079 ± 19
¹⁴ 1043 ± 0	⁹ 121 ± 22	No	²⁵ 22957 ± 93	²⁸ 22808 ± 131
² 128 ± 0	¹¹ 149 ± 5	No	² 490 ± 26	² 471 ± 26
²⁰ 2056 ± 0	⁶ 104 ± 0	No	²³ 13232 ± 166	²⁵ 13226 ± 146
²² 2056 ± 0	¹⁹ 294 ± 1	No	²² 12311 ± 164	²⁴ 12347 ± 197
¹¹ 520 ± 0	¹⁴ 238 ± 19	No	¹² 1058 ± 32	¹⁴ 1049 ± 28
¹⁰ 520 ± 0	²⁴ 482 ± 34	No	¹⁴ 1100 ± 59	¹³ 1048 ± 32
⁴ 146 ± 0	²⁵ 578 ± 5	No	¹⁹ 4964 ± 63	²⁰ 4665 ± 262
⁹ 284 ± 0	²⁹ 645 ± 5	No	²⁰ 5506 ± 131	²¹ 4975 ± 308
³⁶ 19200 ± 0	⁸ 113 ± 5	No	³⁶ 237517 ± 1318	³⁶ 237374 ± 1279
³⁷ 37997 ± 0	³⁸ 959 ± 18	No	²⁶ 28901 ± 1492	²⁹ 27517 ± 186
³¹ 4162 ± 0	²⁸ 611 ± 17	No	²¹ 7423 ± 96	²² 7451 ± 94

Пример расчета скорости работы алгоритма

Алгоритм	Вычисление шаблона [мс= 10^{-3} с]	Сравнение шаблонов [нс= 10^{-9} с]
Алгоритм 1	104	13 226
Алгоритм 2	482	1 048

Суммарная скорость работы алгоритма

Количество фото для сравнения	Размер эталонной базы	Алгоритм 1	Алгоритм 2	Отношение
1 фото	10 000 000	132,26 сек	10.96 сек	12:1
10 000 фото	1 000	1 040 сек	4 821 сек	1:4,6

Скорость зависит от платформы и режима обработки

Производительность вычисления шаблонов в режиме пакетной обработки

Количество изображений в пакете	Производительность на CPU, Intel Core i7, лиц/сек	Производительность на GPU NVIDIA Tesla P40, лиц/сек
1	1-3	11
16	Пакетная обработка не поддерживается	142
32		200
64		256
128		286



Компания Вокорд
123298, Россия, Москва,
ул. Маршала Бирюзова, д.1

Тел.: +7 (495) 787-26-26

Е-mail: sales@vocord.ru

Сайт: www.vocord.ru

