Image Manipulation Detection & Effects of Perspective Distortion on Face Identification

Delia McGarry
Stephen Melsom

United States Department of State
Bureau of Consular Affairs
Consular Systems and Technology

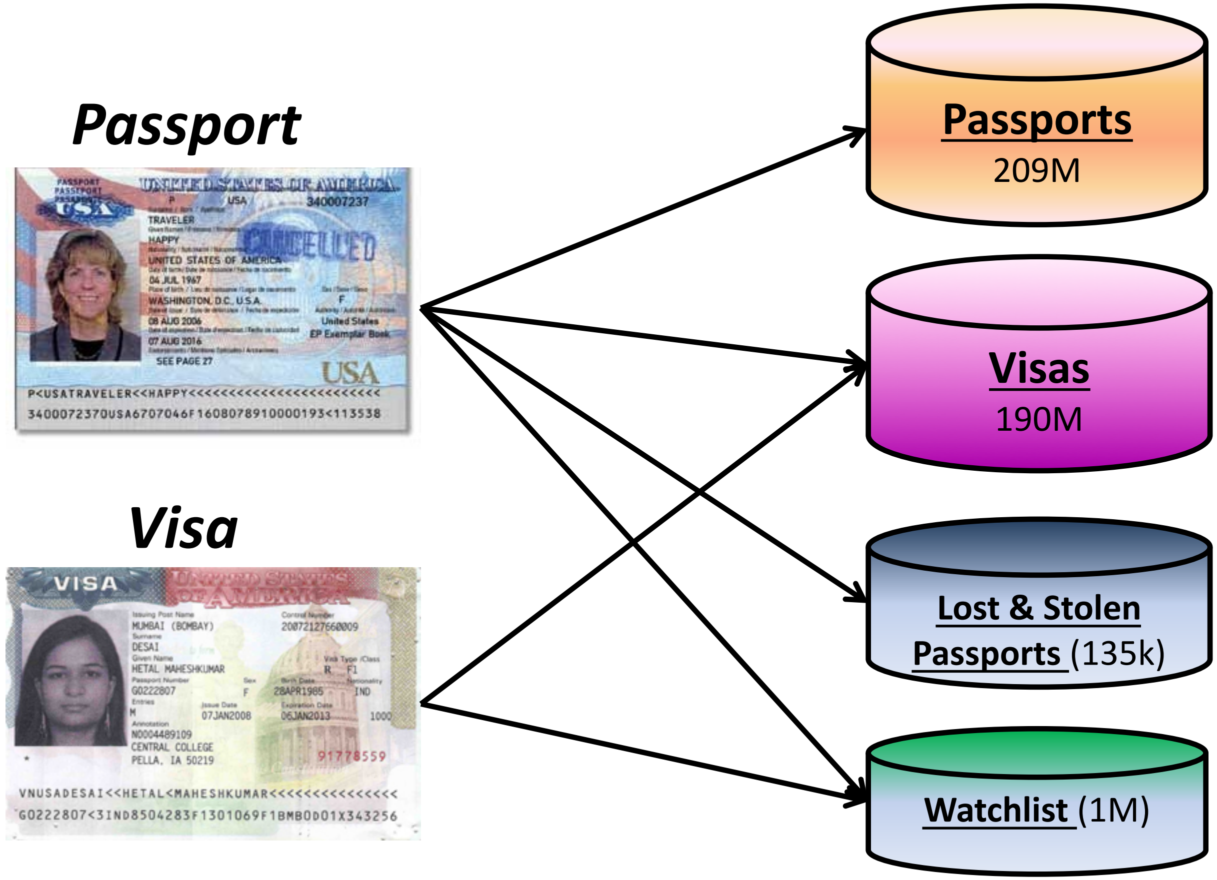
November 2018

DoS Face Initiatives

- Upgrading face recognition (FR) matcher
- Next generation passport with laser engraved polycarbonate data page
- Research
    - Image manipulation detection
    - Effect of perspective distortion on FR

DoS Face Recognition Operation

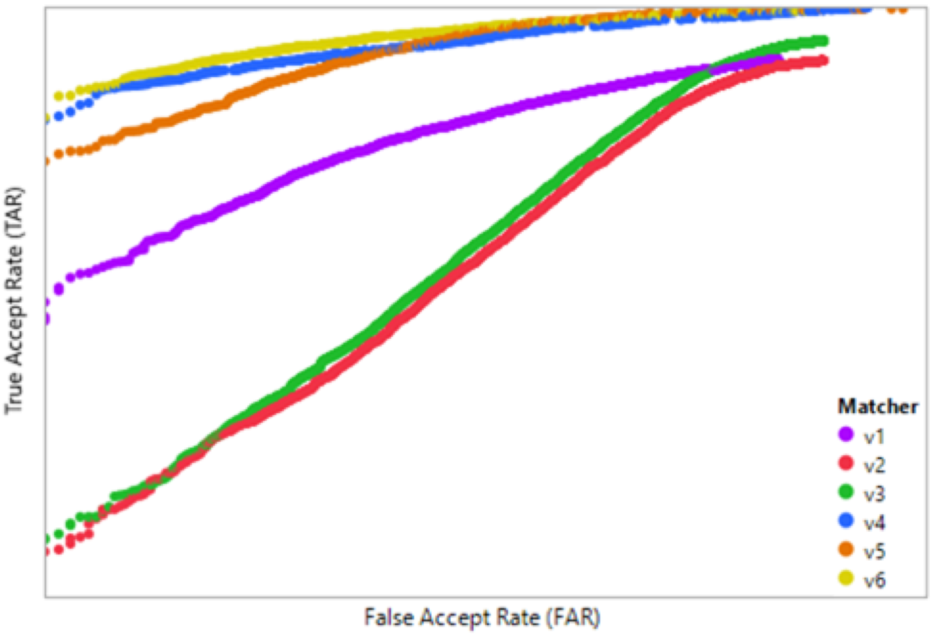
- ~45M applications annually for passports and immigrant, non-immigrant, and diversity visas
- Automated face recognition is conducted for all applicants



How to Obtain Optimal FR Version

- Upgrading FR matcher
- Multiple versions available from a given vendor
- As matchers evolve, so must test practices
- How DoS selects the optimal version
  - Define objectives
  - Choose metrics
  - Test on representative data
  - Perform sensitivity analysis
  - Communicate criteria and results with vendor
  - Select appropriate version for DoS' application

Identification ROC

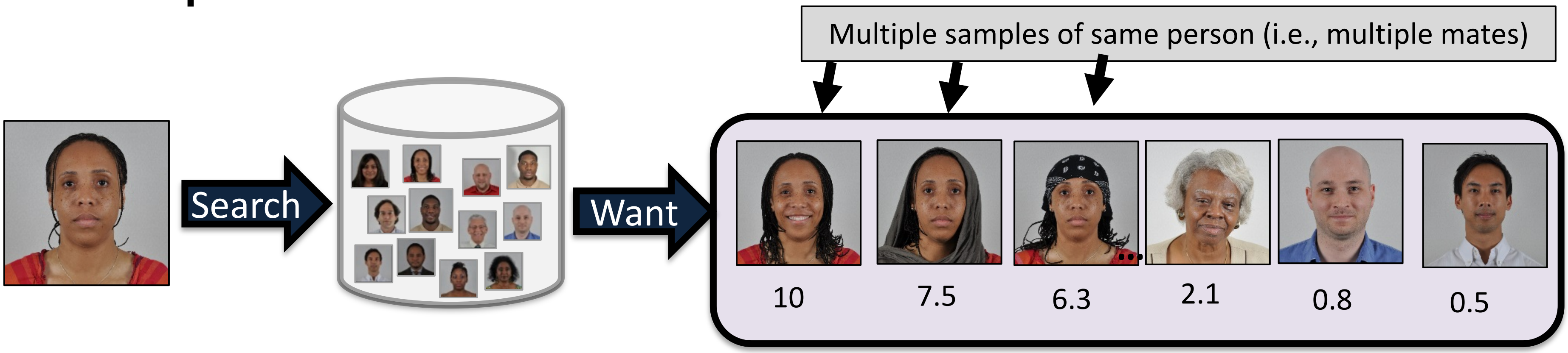


Performance variation on same dataset; six versions from same vendor.

~20 percentage point increase at an operationally relevant, low FAR

FR Test Objectives

- Gallery size independence
  - Estimate accuracy of system at scale
- Score AND rank matter
  - Candidate lists are managed by score and rank
- High TAR at *very* low FAR
  - Requires substantial number of impostor comparisons
- Must perform well on representative (constrained) data
- **Multiple mates matter!**



Choose Metrics

Common Metrics for Evaluation

	ROC	FPIR / FNIR / CMC[1,2]
Target Scenario (examples)	Find *all* mates (e.g., fraud detection)	Find *any* mate (e.g., watch-list)
Properties	Per-comparison credit Based on match scores	Per-search credit Based on rank and match scores
Weaknesses	Sensitivity to normalization Does not take rank into account	Sensitivity to normalization Dependent on N

- Best Practices for 1:N Testing
  - (Current): Requires execution of searches with and without mates[1,2]
  - (*Not Present*): Guideline regarding the proportion of mated searches
  - (*Not Present*): Guideline regarding proportion of mates in test database

- ROC was chosen due to gallery size independence and credit for multiple mates
  - Run in identification mode
  - Count all impostor comparisons

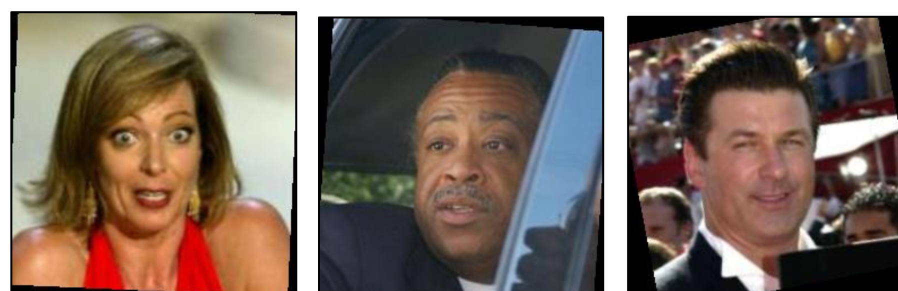
1 Grother, P., Ngan, M., "**Face Recognition Vendor Test (FRVT), Performance of Face Identification Algorithms**", *NIST Interagency Report 8009*, May 2014
2 Grother, P., Quinn, G., and Phillips, P., "**Report on the Evaluation of 2D Still-image Face Recognition Algorithms**", *NIST Interagency Report 7709*, 2010

Sensitivity Analysis – Data Type

- *Hypothesis 1*: some FR versions were trained and optimized on *unconstrained* imagery
- DoS travel documents are *constrained*
- Tested each version on constrained and unconstrained datasets

Constrained (Visas)

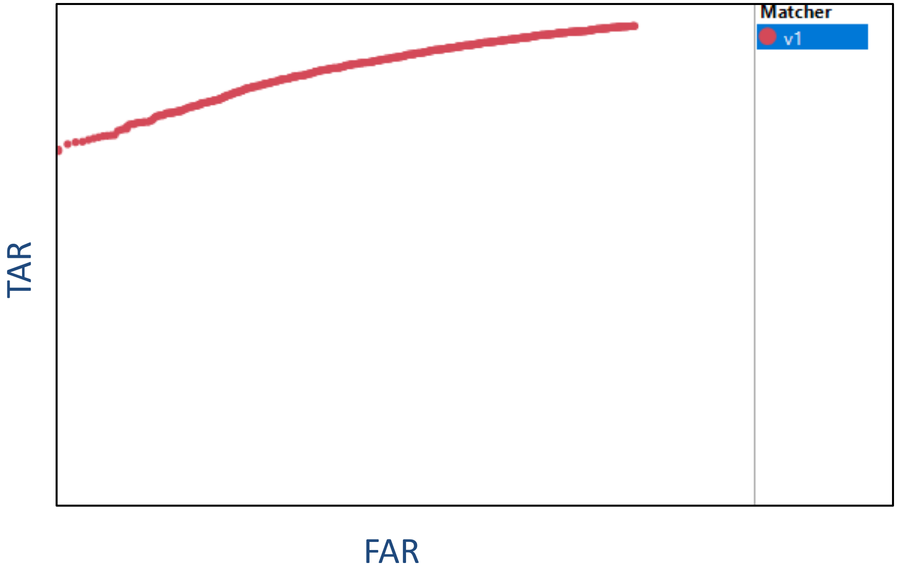
Unconstrained



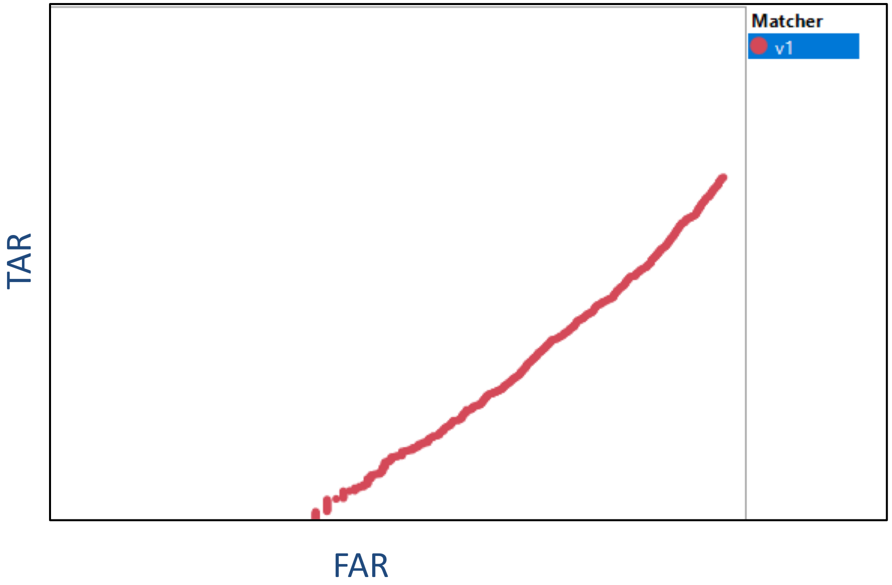
Current FR Version

- Identification ROCs for current FR version

Constrained (Visas)



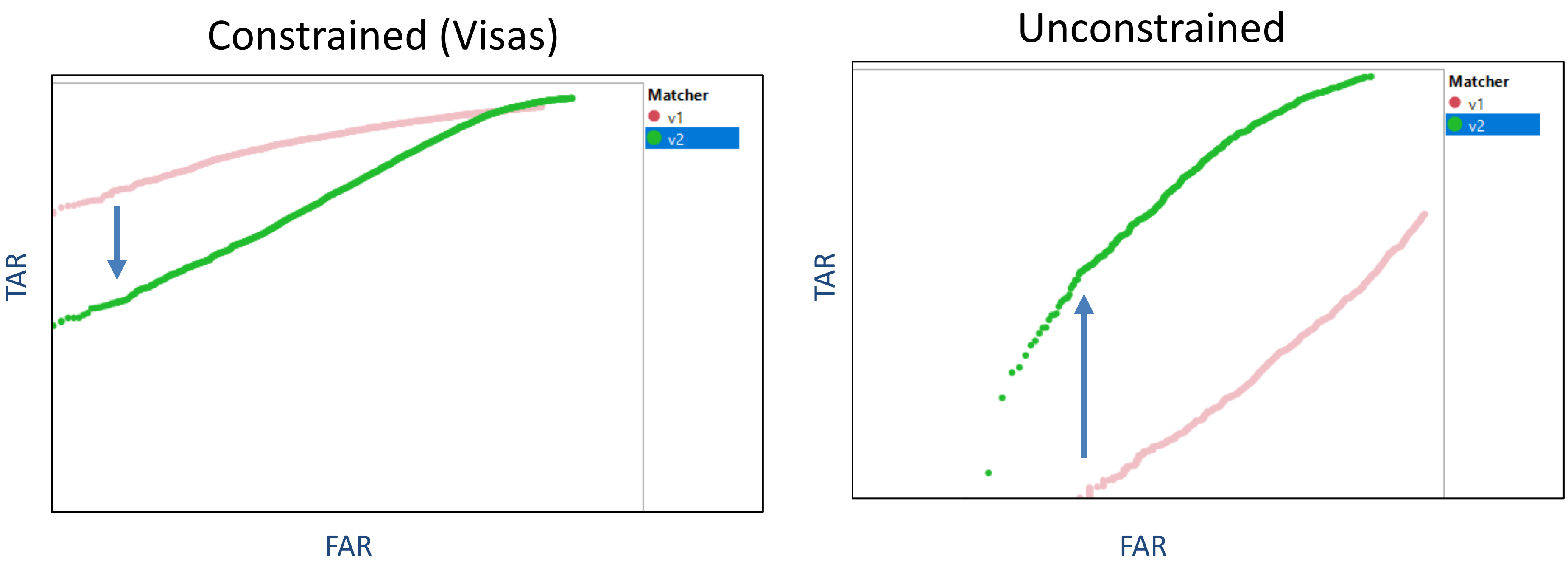
Unconstrained



- Current version is optimized for constrained imagery

Version Upgrade Candidate

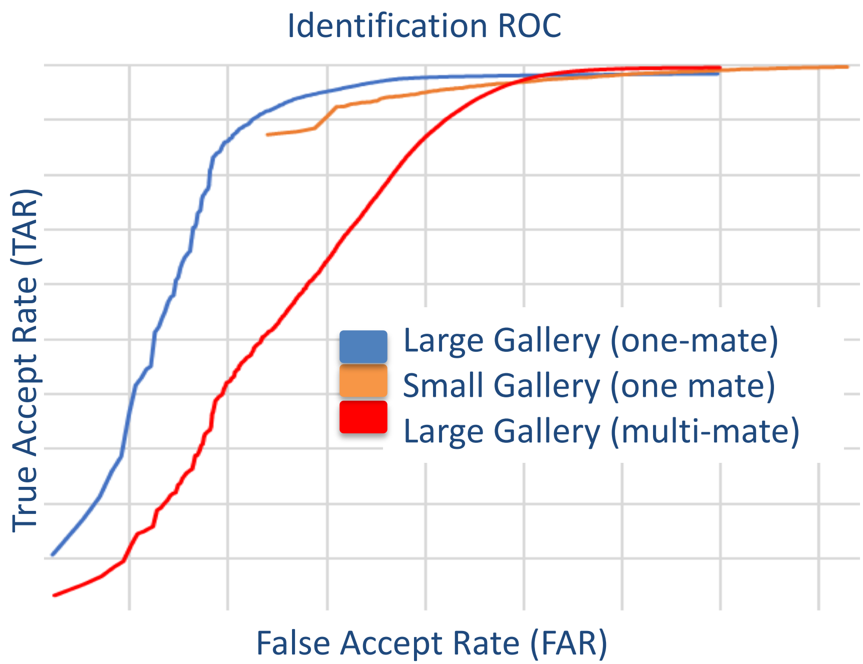
- Identification ROCs for FR version submitted for upgrade



- Performance of this version worsened for DoS constrained but improved for unconstrained images

Sensitivity Analysis – Normalization

- *Hypothesis 2*: normalization based on incorrect assumptions about data caused poor performance in some versions
- Tested single version with different test configurations
  - Varied gallery size
  - Varied number of mates



- ROC maintained gallery size independence when only one genuine mate was in the gallery
- Performance significantly decreased when multiple mates were in the gallery
- *Conclusion*: vendor incorrectly assumed only one mate and implemented inappropriate normalization

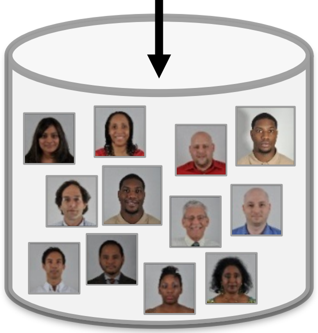
Identification with Normalization

Search

Candidate List

Rank	ID	Score
1		0.931
2		0.722
3		0.613
4		0.602
5		0.586
6		0.542
7		0.521
…		…
49		0.335
50		0.322

Normalize



Normalized Candidate List

Rank	ID	Nmzd. Score
1		0.991
2		0.715
3		0.598
4		0.581
5		0.565
6		0.491
7		0.355
…		…
49		0.192
50		0.187

Boost rank-1 score

Genuine suppressed -> lowers ROC

Reduce low rank scores

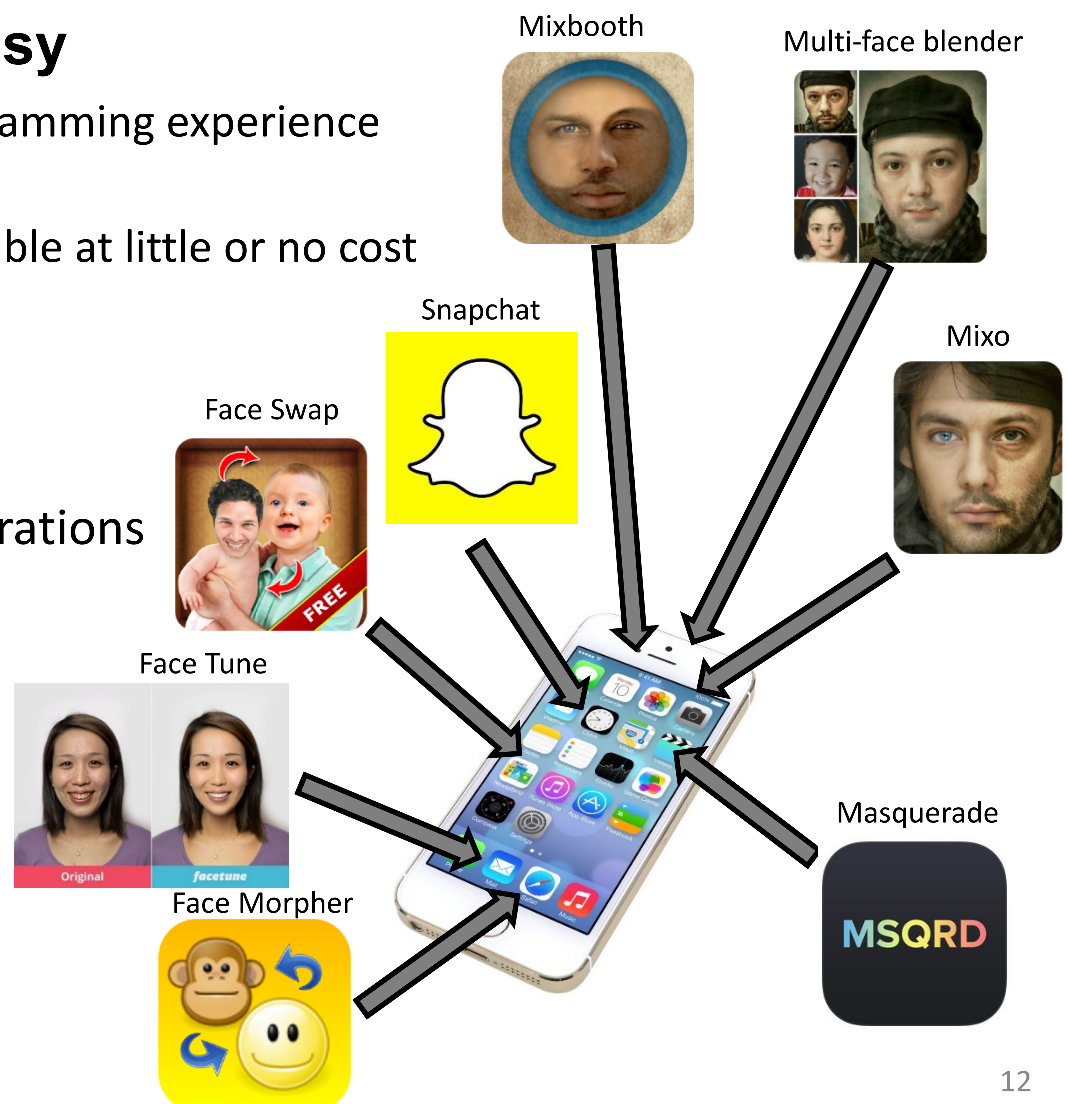
A 1:N matcher with gallery normalization may **boost high scores** and **suppress low scores** based on rank position.

Detecting Image Manipulation

- **Image manipulation is easy**
  - No image processing or programming experience required
  - Mobile applications are available at little or no cost on all platforms

…but difficult to detect!

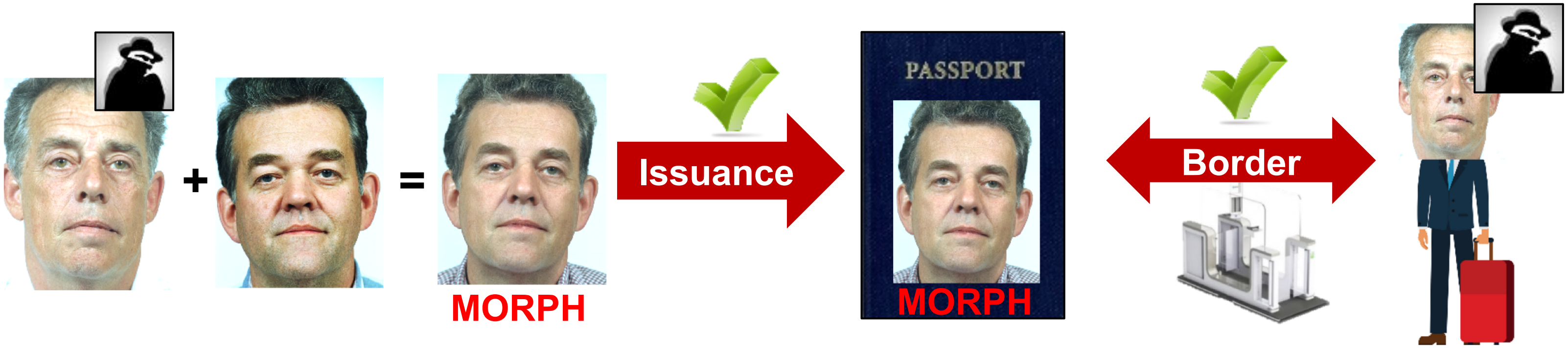
  - Detectors must be customized to specific alterations



Goal: Automatically detect image manipulation with low false detect rate

Face Morphing Presentation Attacks

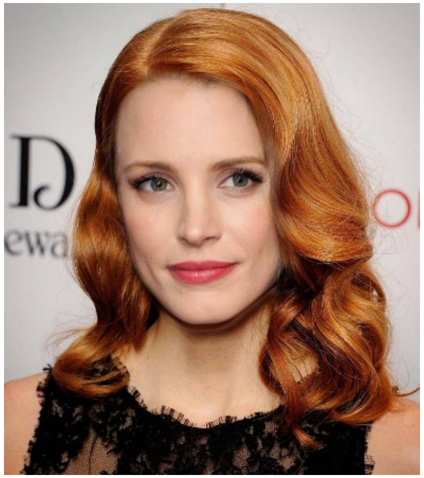
- Test and evaluation to understand the impact of morphing on automated Face Recognition
  - Data creation for a NIST evaluation of morphing detection algorithms
  - Analysis and development of automated detection methods



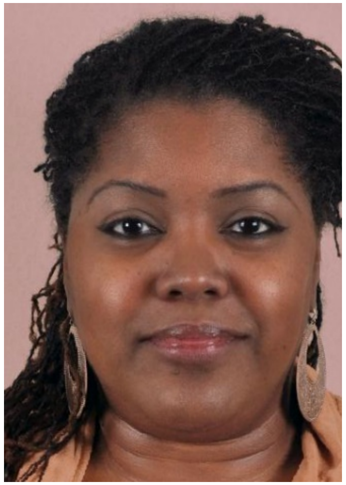
Face Blending Dataset

- Types of imagery:
  1. lower quality, methods and means available to non-experts as mobile apps, 1000+ images
  2. higher quality, experienced artists using commercial digital art applications, 300+ images
  3. automated methods based on academic research and best practices, 40K+ images

1. non-expert



2. artist

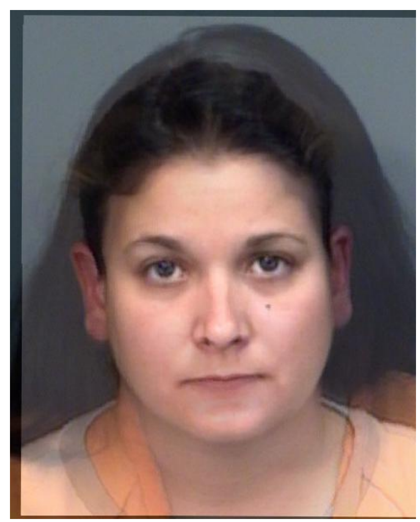


3. algorithmic

Automatic Morph Generation

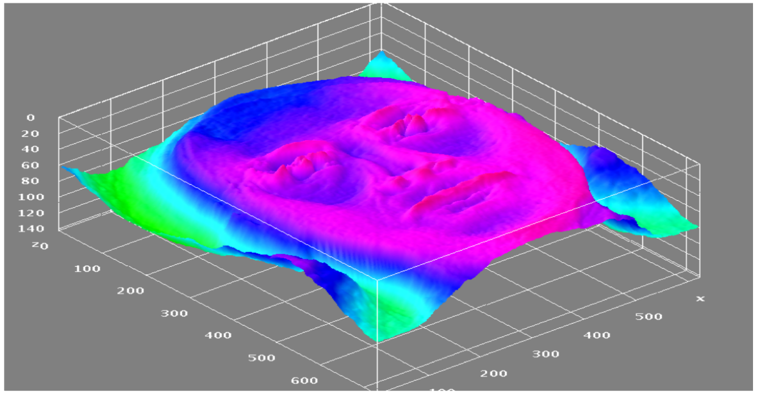
Subject A | 70% | 60% | 50% | 40% | 30% | Subject B

Typical artifacts were mitigated



Detecting Morphed Images

- Automated detection of morphed images
  - Multiple models learned from underlying data distribution
  - Models utilize kernel-based, pair-wise comparisons and a random forest decision tree classifier
- Test & Evaluation
  - Initial results on 1.4K developmental sets
  - Overall: 74% classification accuracy*
- Next step – increase number of models using large background face set



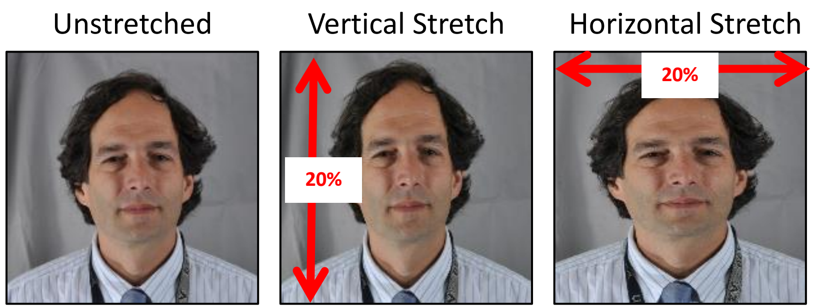
Model detection is per pixel;
higher likelihoods shown as hotter colors

	Actual Morphed	Actual Original
Predicted Morphed	TP=401	FP=164
Predicted Original	FN=201	TN=634

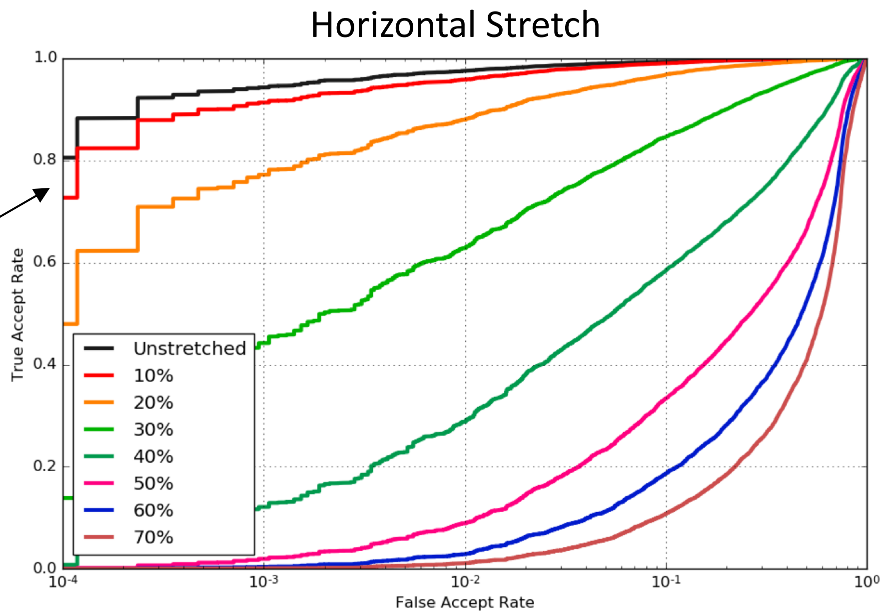
* Accuracy = TP + TN / Total Population = 401+634 / 1400

Effect of Stretching on FR

- Estimated ~12% of online visa applications are stretched
- May or may not be malicious
- Stretched images can severely impact the accuracy of Face Recognition

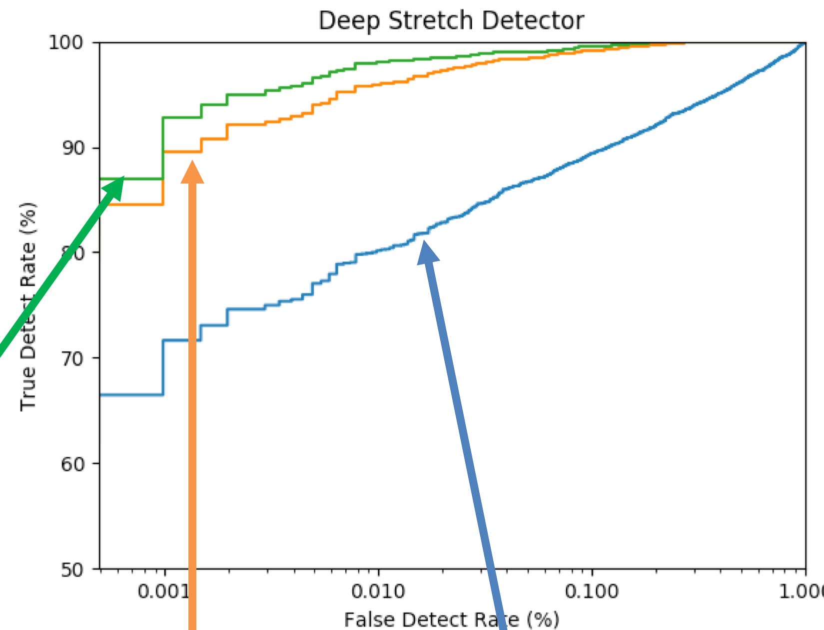


Matching performance *significantly* decreases following 10% stretch



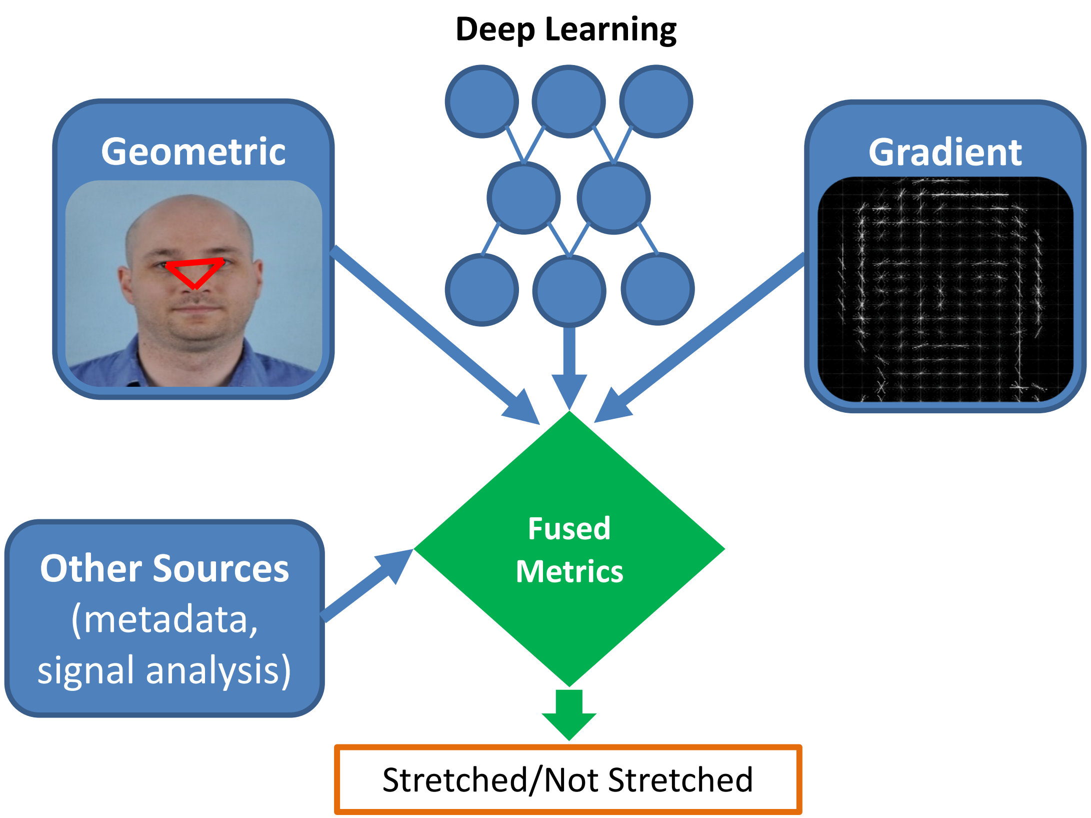
When is Stretching Detectable?

- Deep learning approach uses convolutional neural network
  - Trained on “artificially” stretched visas
- Detection difficulty increases as stretch magnitude decreases



Stretch Detection Approaches

- Variety of stretch detection approaches are in development
- Results can be fused to increase detection accuracy
- Scanning images greatly increases the difficult to detect

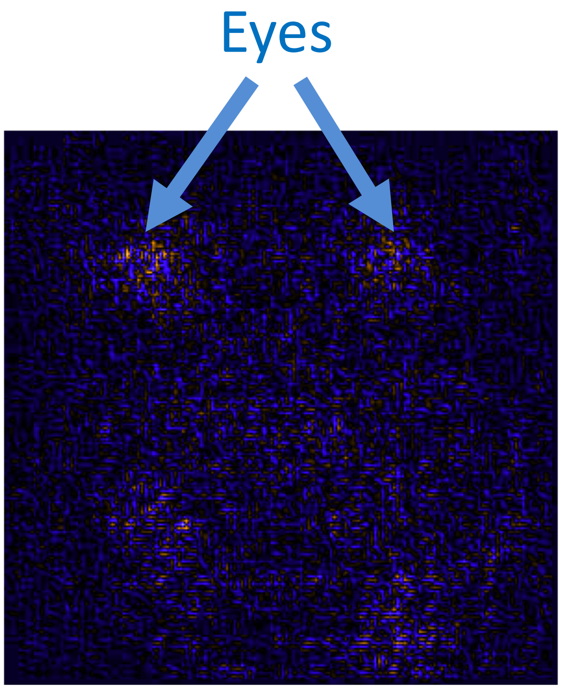


Stretch Detection: Where to Look?

- Layer-wise Relevancy Propagation[1] (LPR) indicates regions where deep learning convolutional neural network concentrated
- LRP maximums appear within the ocular region

Unstretched

20% stretched



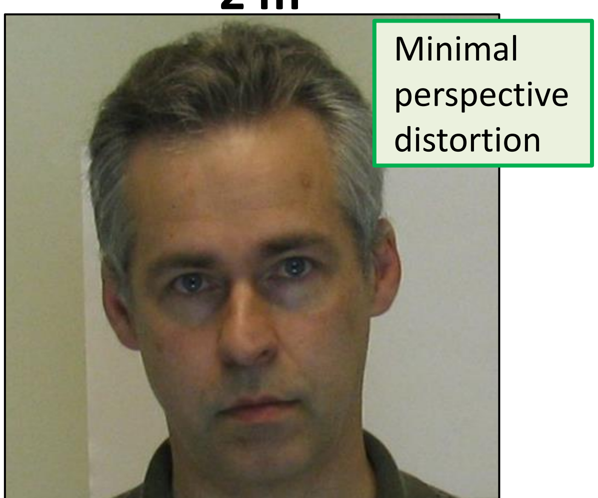
Stretched Images Mean LRP

[1]http://www.heatmapping.org/

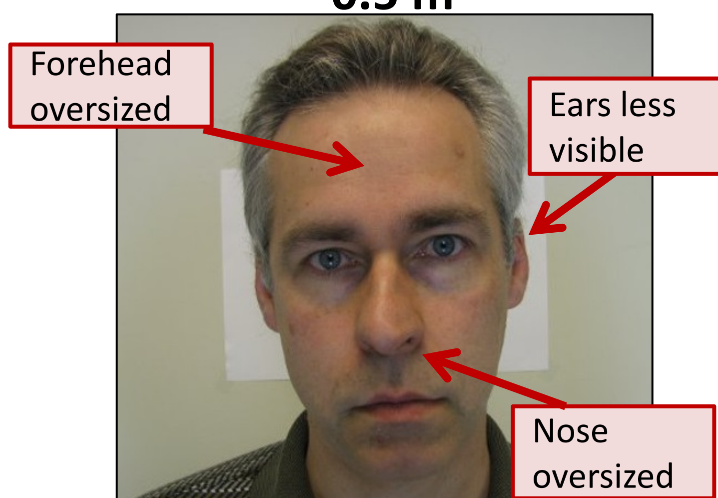
Perspective Distortion

- Perspective distortion is the apparent warping of an object due to relative scale of nearby and distant features, (i.e., fisheye)
- Study motivated by ICAO Portrait Document camera distance specification
  - ISO/IEC/JTC1/SC17/WG3 study found minimal impact of camera distance on FR down to 0.5m (1:1, same day experiment)
- DoS conducted 1:1 and 1:N experiments with artificially distorted subjects

2 m



0.5 m



Simulated Perspective Distortion

- Perspective-aware Manipulation of Portrait Photos[1]
- Steps to achieving a manipulative face model:
  1. Detect 2D fiduciary landmarks (3 additional manually-placed landmarks are also required)
  2. Instantiate parameters we seek to minimize:
     - Identity vector
     - Expression vector
     - Rotation
     - Translation
     - Intrinsic camera matrix
  3. Fit the 2D landmarks to the 3D model using gradient descent
  4. Update **valid** 3D landmarks
  5. Manipulate distance and pose using parameters

[1]http://faces.cs.princeton.edu/

Simulated Perspective Distortion (cont.)

- Algorithm enables users to simulate camera distance and head pose
- Assumes camera distance of 1m
- Distortion algorithm often fails when simulating camera distances below 0.4m
- Distortion algorithm evaluated with Caltech Multi-Distance Portraits dataset

Actual

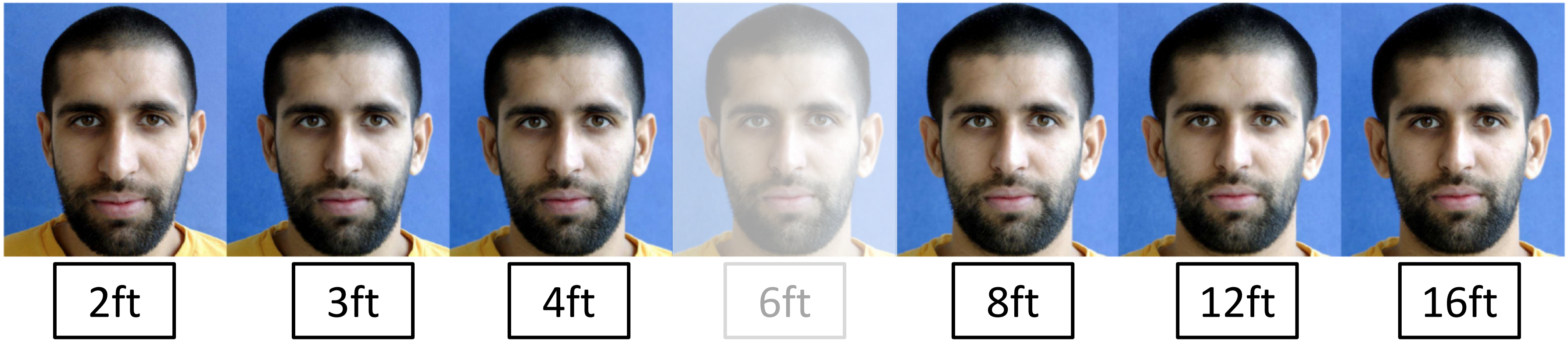
Simulated

0.5m 0.6m 1.2m 2.4m 3.6m

http://faces.cs.princeton.edu/

CMDP Dataset

- Caltech Multi-Distance Portraits
- Same-day portrait photographs taken from 7 camera distances
- 53 subjects
- 6ft images used as probe set while remaining images were enrolled into face recognition system



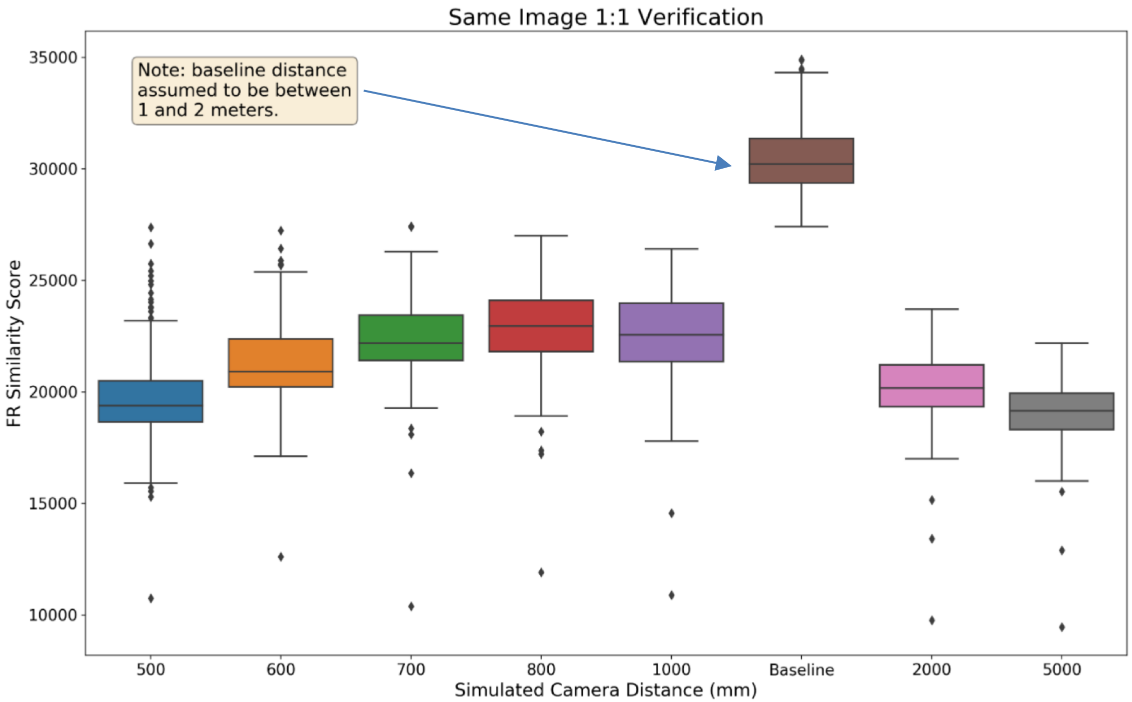
Testing Effects of Perspective Distortion

- Apply simulated perspective distortion to FERET dataset
  - Restricted to frontal, different-day mated subjects
  - 166 subjects
  - Simulated distances between 0.3m and 90m
  - Restricted experiments to 0.5m-5m
- Distorted images were grouped by simulated camera distance and enrolled into FR system with a background gallery of 1.5M visa images
- Original, mated images were used as probes

Original 0.3m Simulated

Verification Results: Simulated FERET

- Observe performance of perspective distortion algorithm
- 1:1 verification on same image between simulated distances

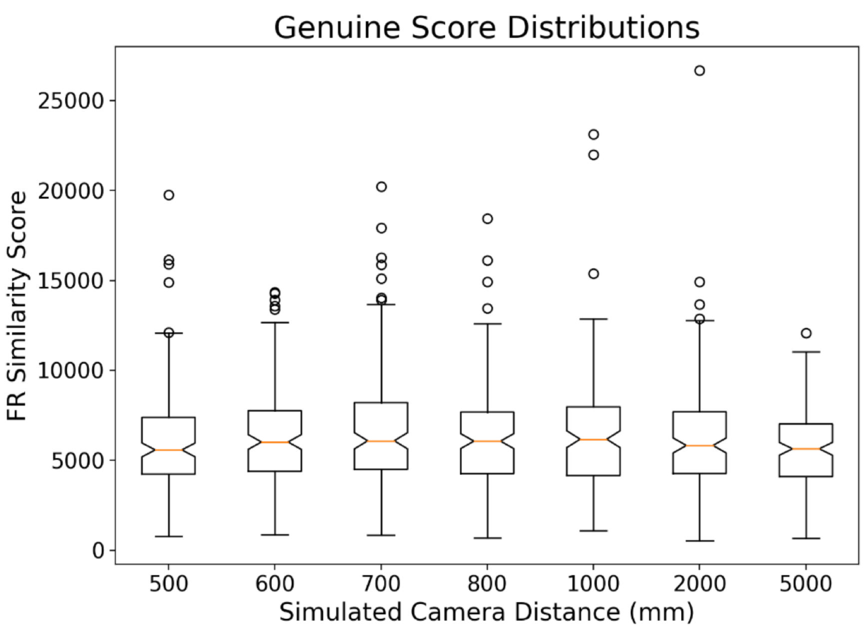


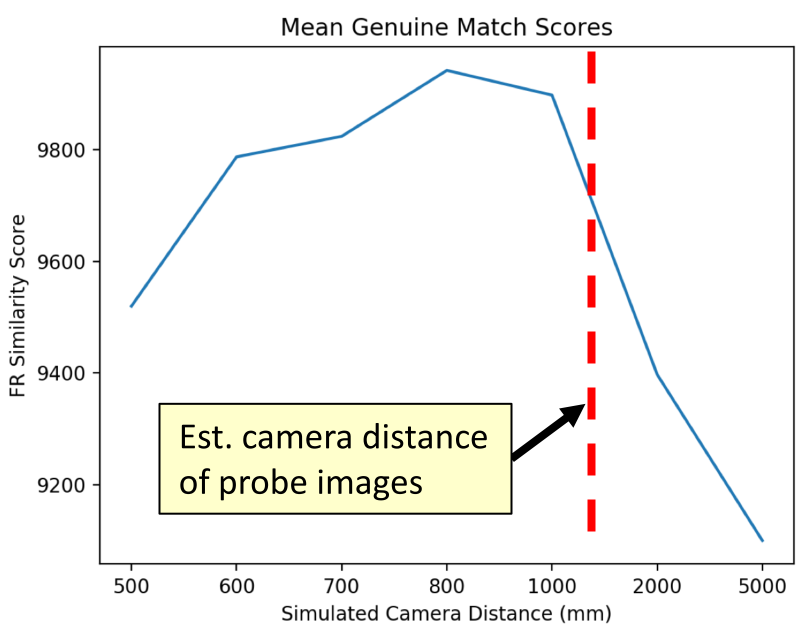
Original

0.3m Simulated

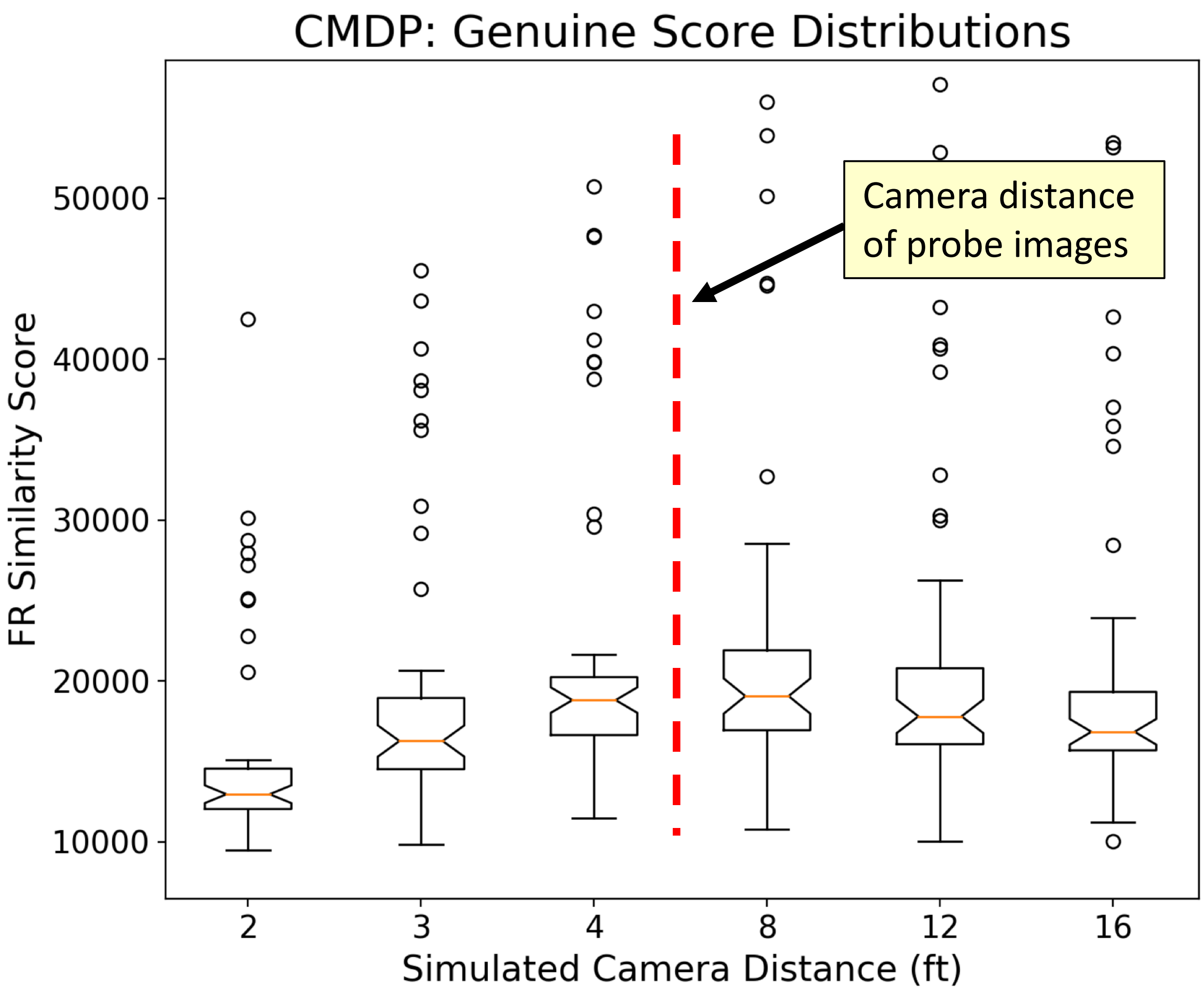
Identification Results: Simulated FERET

- Enroll individual groups of artificially distorted images into FR system with 1.5M background gallery
- Use original, ”undistorted” images as probes



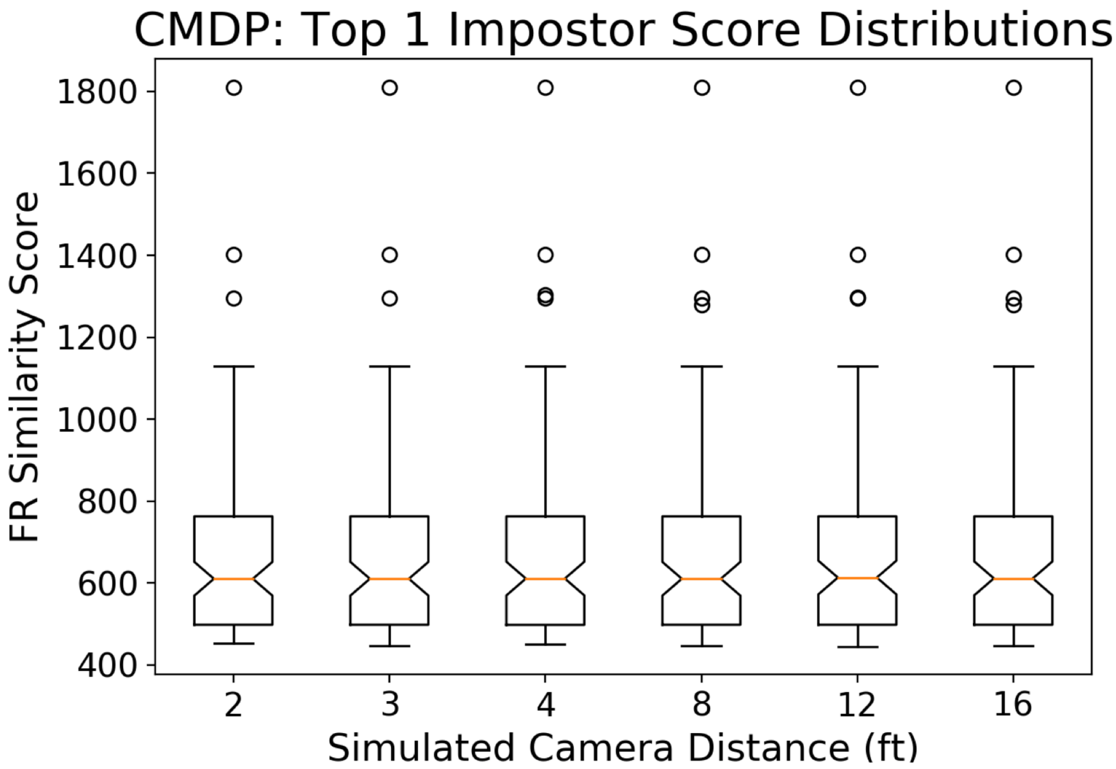


Identification Results: CMDP



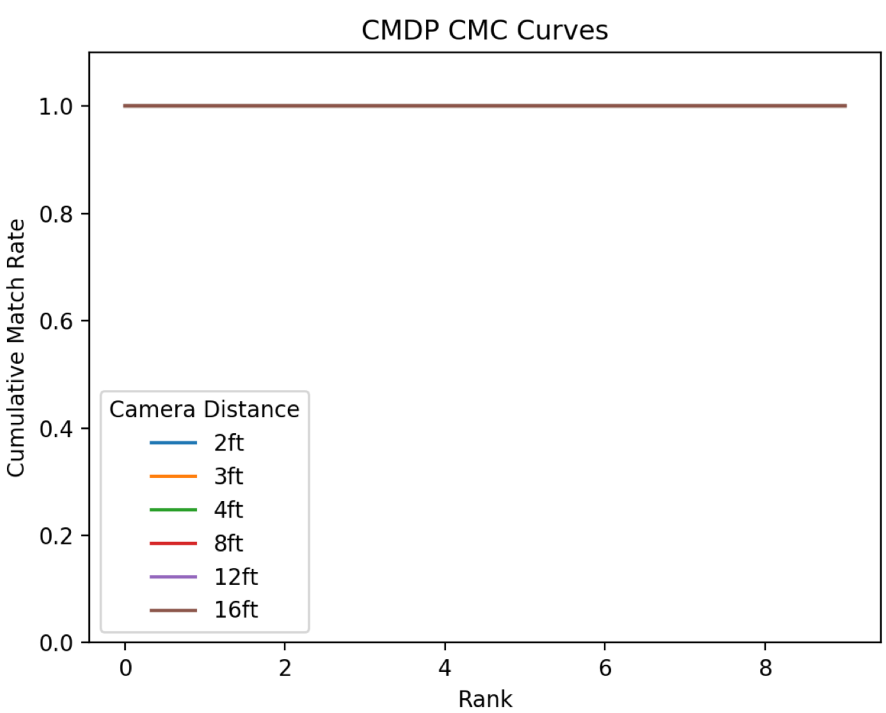
Identification Results: CMDP

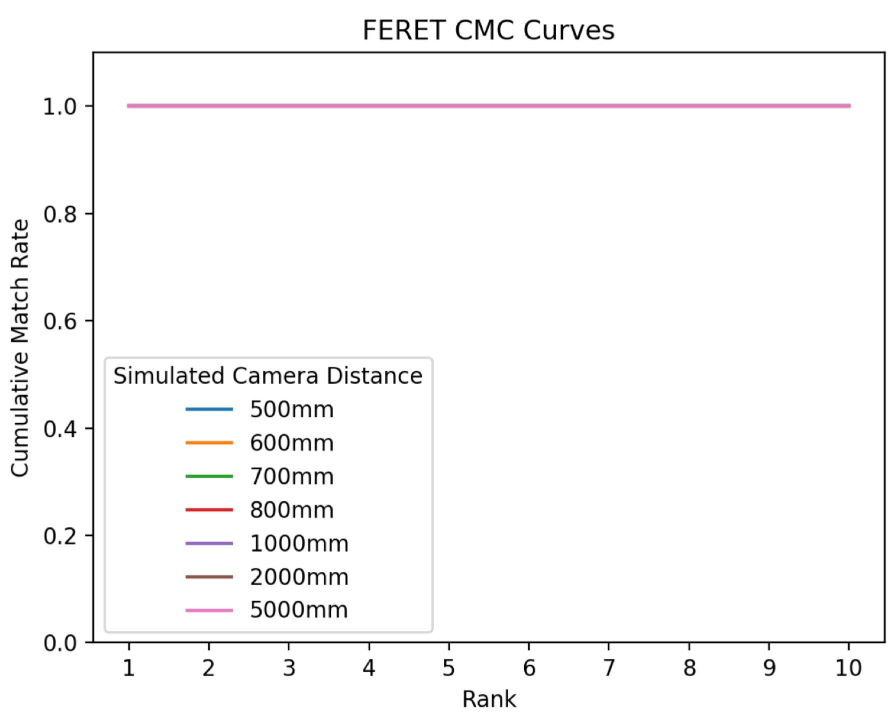
- Will similar levels of distortion between probes and impostors increase similarity scores?
- Impostor scores remained stable regardless of genuine mate's camera distance



CMC Results

- Using the camera distance simulation on this data did not affect identification performance





Perspective Distortion Experiment Conclusions

- Results warrant further investigation
- Why are the results ideal?
  - FR matcher pretrained on FERET data?
  - Unseen watermarking or artifacts?
  - Disparity between FERET dataset and visa images?
  - FR matcher may have a system in place to mitigate perspective distortion
- Next steps
  - Implement distortion algorithm
  - Process visa images with distortion algorithm
  - Rerun experiment

Conclusions

- Significantly improving FR accuracy by upgrading matcher
  - Achieving optimal version required defining objectives (e.g., finding multi-mates, operating point), representative testing, sensitivity analysis, communication of evaluation criteria to FR vendor
- Developing image manipulation detection algorithms to enhance travel document security
- Simulated effect of perspective distortion on FR identification to inform camera distance standards
  - FR was not adversely affected at camera distances as close as 0.5 m