Optimizing Key-Selection for Face-based One-Time Biometrics via Morphing

Dailé Osorio-Roig

PhD Dailé Osorio-Roig

PhD student:
Hochschule Darmstadt

Website:
https://dasec.h-da.de/staff/daile-osorio-roig/

Contact:
daile.osorio-roig@h-da.de

Topics: Workload reduction, multi-biometric systems, Privacy-enhancing technologies.

ATHENE
National Research Center
for Applied Cybersecurity

da/sec
BIOMETRICS & SECURITY
RESEARCH GROUP

Contents

Introduction

Today

"Sophisticated" ***side-channel attacks*** because we have smart card, cloud computing infrastructures, and … , but tablet computers and smartphones are powerful ***multi-purpose computing platforms***!

Gaming app connected to sensors

Banking app connected to offices

Email

We want more technologies, but more privacy protection

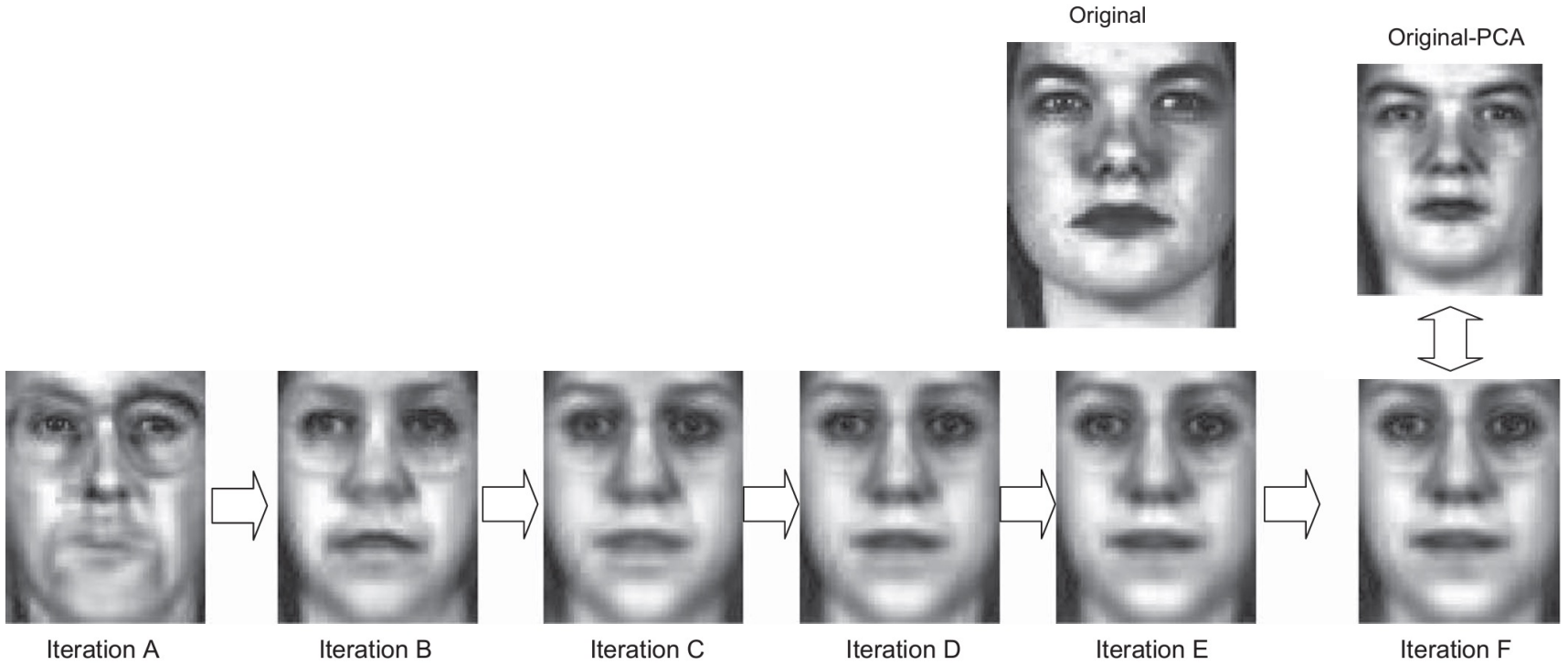
STOP!

It is very easy for me looking for a channel and listen to side-channel information!

Introduction

Attacks

"Sophisticated" ***side-channel attacks*** can be used to improve traditional attacks such as the so-called "*Hill-climbing*", making them yet more dangerous![1]



- ✓ Find a final face image which is very similar to the objective face: "Original-PCA".
- ✓ The attacker is trying to gain access to the application.
- ✓ Optimization problem.

Bayesian-based hill-climbing attack on the eigenface-based system. Figure taken from [2]

[1] Naylor JF. Peter Wright. Spycatcher: The Candid Autobiography of a Senior Intelligence Officer. New York: Viking Penguin, Inc. 1987. Pp. 392. 22.95. Albion. 1988;20(2):357-62.
[2] Galbally J, McCool C, Fierrez J, Marcel S, Ortega-Garcia J. On the vulnerability of face verification systems to hill-climbing attacks. Pattern Recognition. 2010 Mar 1;43(3):1027-38.

Introduction

Iterative optimization

1- Work on the workflow of “Machine learning techniques” – Deep Learning!.

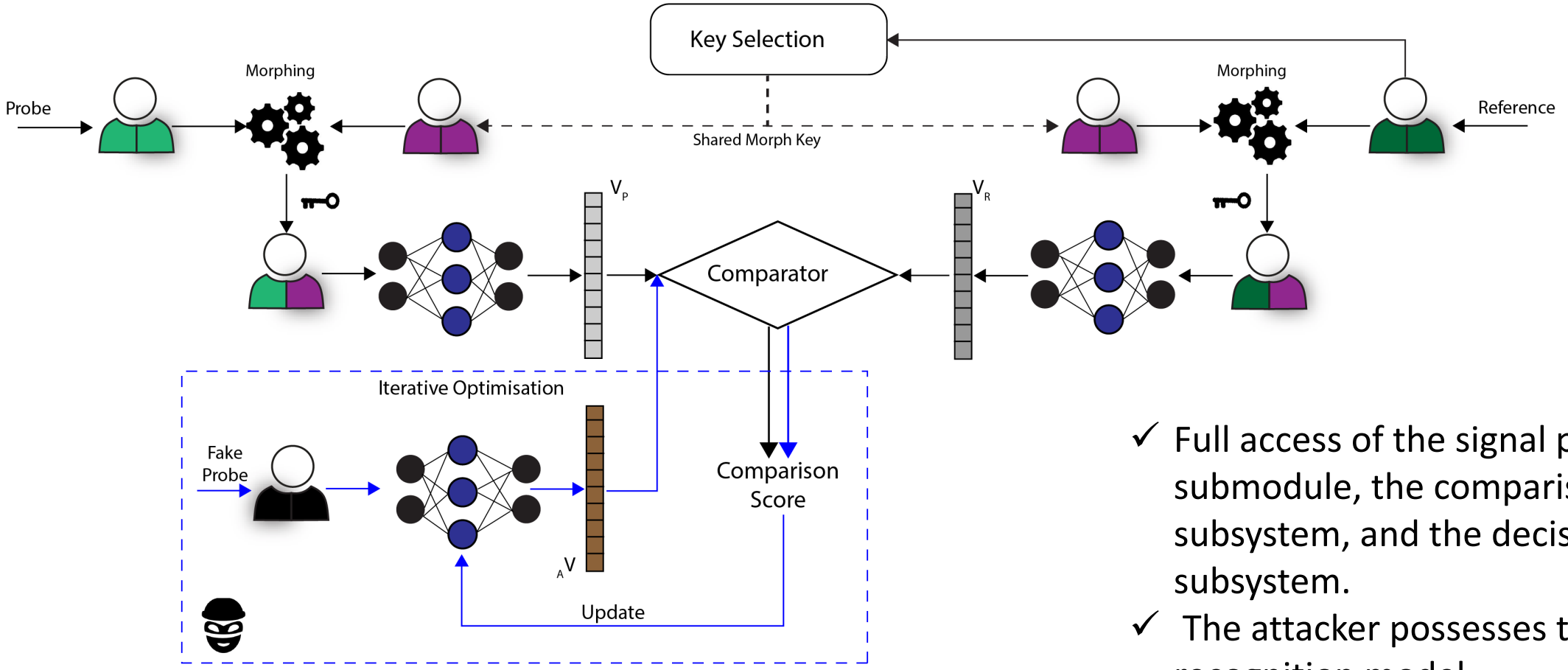
- Minimize the loss function
- Optimization can be through any optimizer e.g. Gradient Descent, Stochastic Gradient Descent (SGD), Adam, AdaDelta, etc.

2- Need an objective function.

3- Need a learning process which could require a “time-comsuming”.

4- ***The target (attacked input) is vulnerable to the “Iterative optimization (attacker)” but “Iterative optimization” is very sensitive to the changes occurring on the target!***

Proposal



- ✓ Full access of the signal processing submodule, the comparison subsystem, and the decision subsystem.
- ✓ The attacker possesses the face recognition model.
- ✓ The attack is injected when a biometric claim is made.

Experimental setup

- AdaFace[2] as face embedding extractor.
- Datasets:
  - VGGFace2 (identities of the set of testing selected as references and probes): 50 identities, multiple samples per identity.
  - LFW: database to build the morph, a single sample per identity was selected by quality factor.
- Biometric performance (threshold selection): 14 samples per identity are defined for references and probes.
- Execution of attack: for 50 identities, 30 samples per identity are defined as references and probes.
- Euclidean distance as comparator.

[2] Kim M, Jain AK, Liu X. Adaface: Quality adaptive margin for face recognition. InProceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition 2022 (pp. 18750-18759).

Experimental setup

- Key selection for building the morph by using LFW database.
  - Random key-based selection (Random_key) → original from the paper OTB-Morph[3]
  - Most dissimilar distance key-based selection (Distance_key).
  - Most dissimilar distance of the opposite demographic group (e.g. sex) (SFdistance_key).
  - Random sample of the opposite demographic group (SFrandom_key).
- Morphing process was based on the library Dlib for landmark detection and OpenCV for image processing.
  - Morph was built on the full face image (without alignment and cropping)
  - After morphing, the face image was aligned and cropped by the detector RetinaFace.

[3] Ghafourian M, Fierrez J, Vera-Rodriguez R, Morales A, Serna I. OTB-morph: One-time Biometrics via Morphing. Machine Intelligence Research. 2023 Jun 1:1-7.

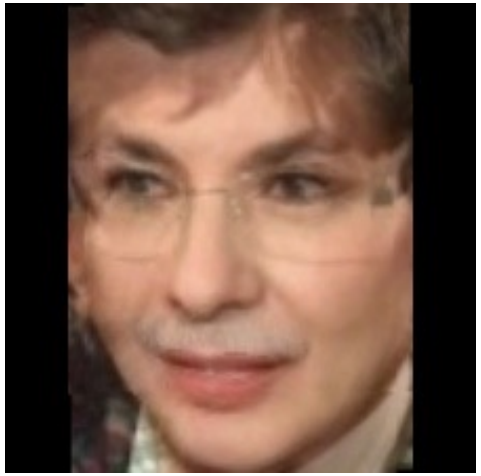
Experimental setup

- Key selection (Examples)

Original Sample (Reference)

Random

Distance

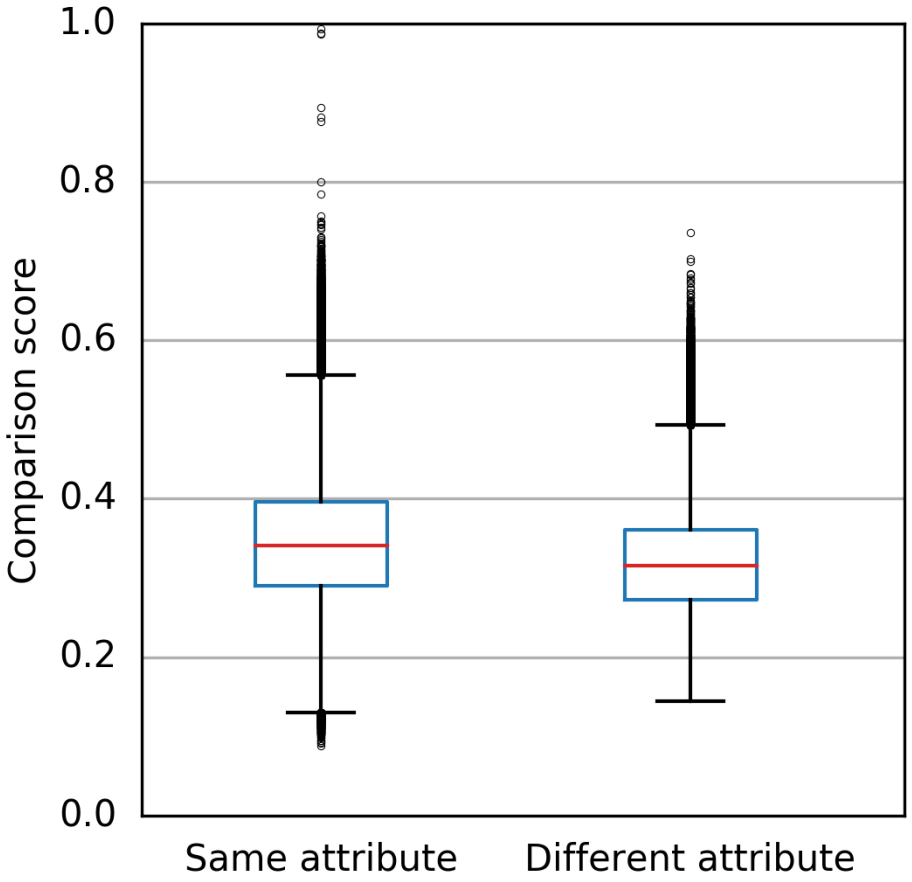


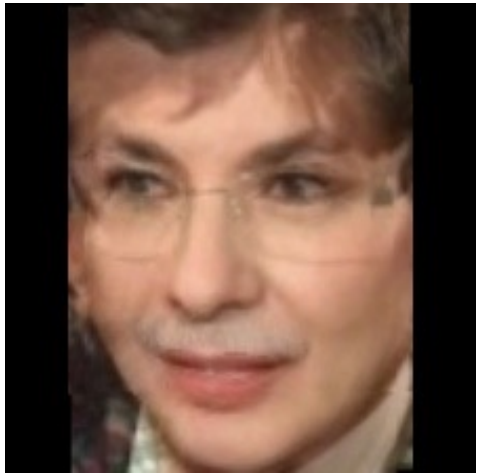
Opposite Sex

Distance and opposite Sex

Experimental setup

- Across opposite demographic information –Why?





Opposite Sex

Distance and opposite Sex

Effects of broad homogeneity [4] and chance of the false match is not new!

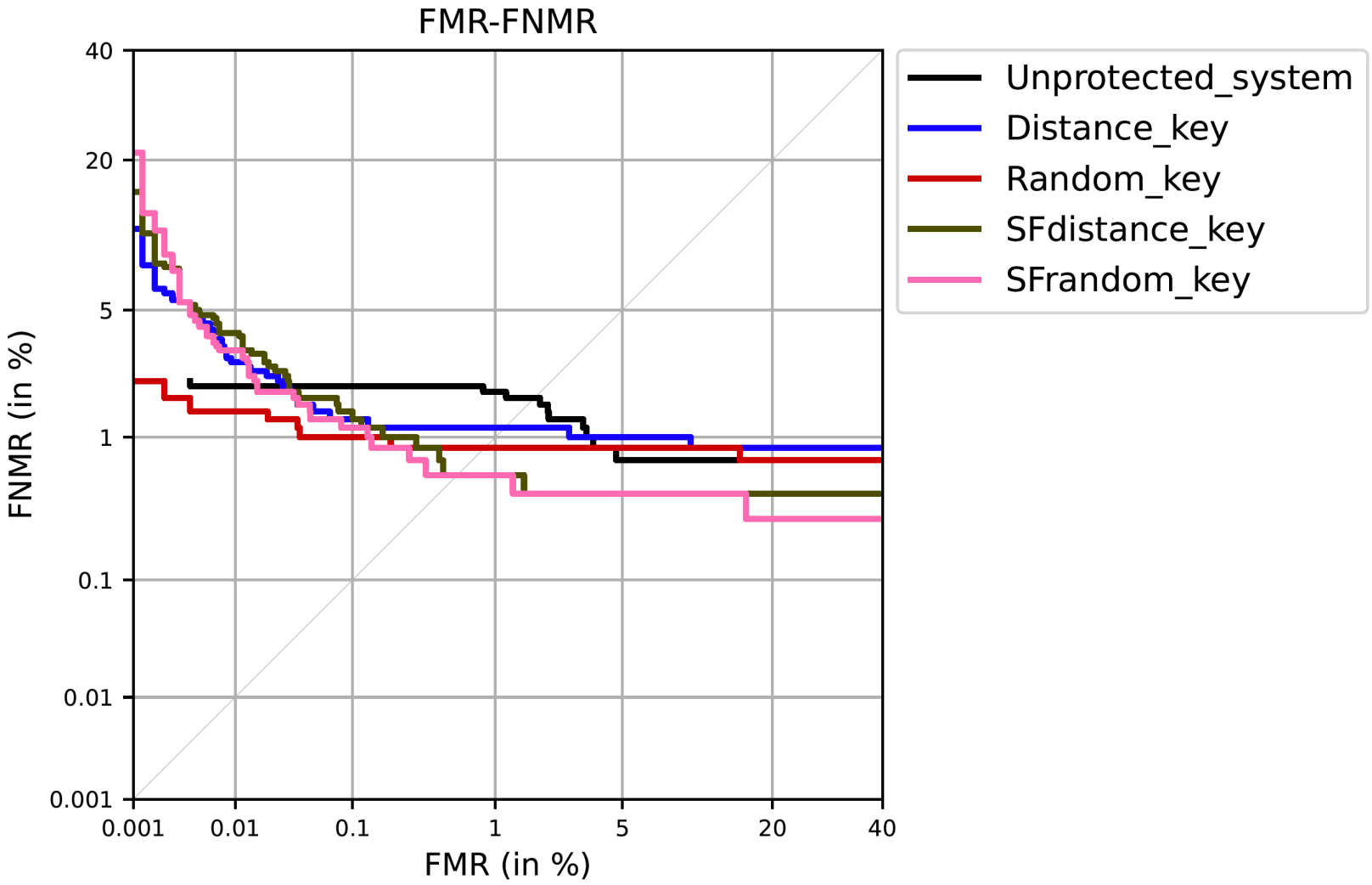
[4] Howard JJ, Sirotin YB, Vemury AR. The effect of broad and specific demographic homogeneity on the imposter distributions and false match rates in face recognition algorithm performance, 2019 ieee 10th international conference on biometrics theory, applications and systems (btas) 2019 Sep 23 (pp. 1-8). IEEE

Experimental setup

- Metrics.
  - DET curves (EER and different operational points at FMR) for verification scenario.
  - The attack chance via iterative optimisation across different key selections.

[3] Ghafourian M, Fierrez J, Vera-Rodriguez R, Morales A, Serna I. OTB-morph: One-time Biometrics via Morphing. Machine Intelligence Research. 2023 Jun 1:1-7.

Results

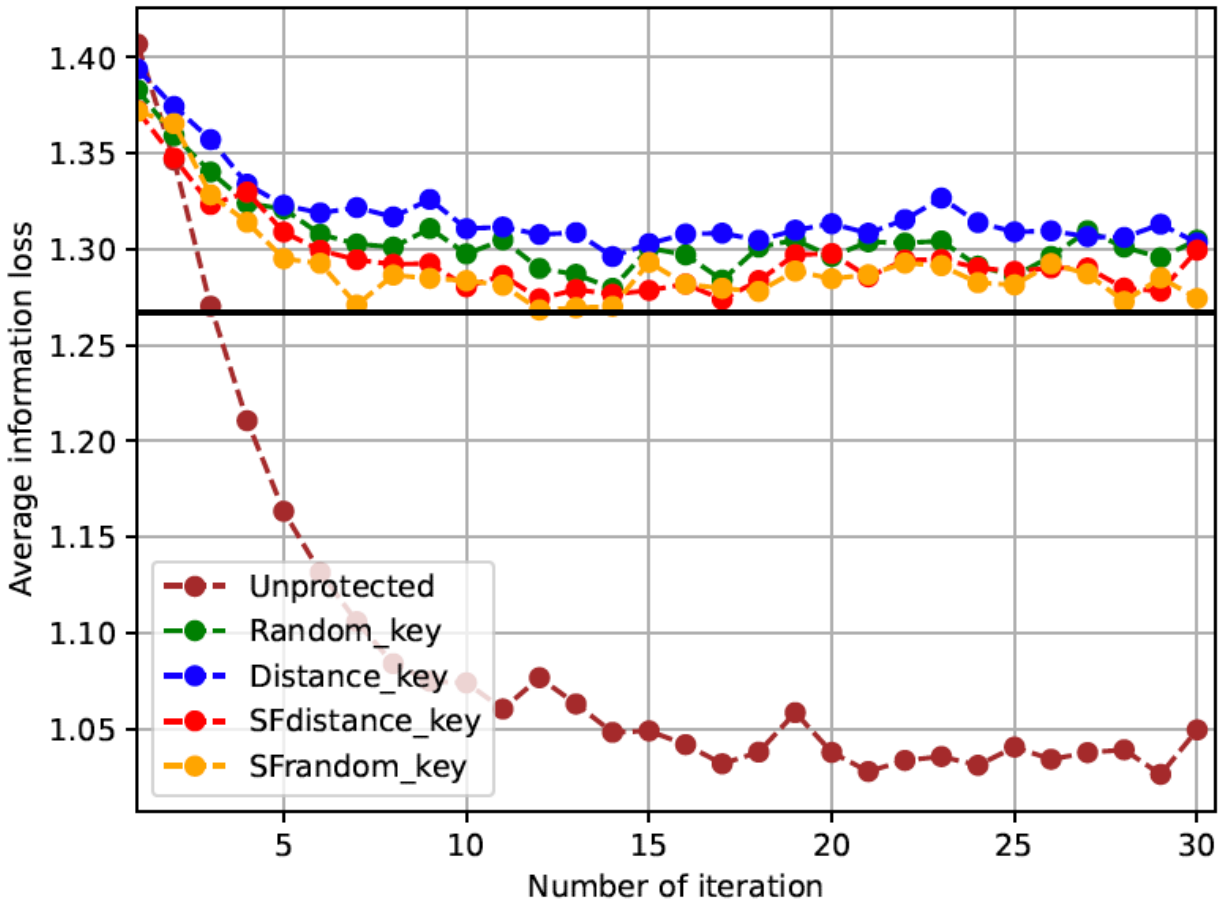


Biometric performance

- ✓ Key-selection process outperforms the unprotected system (FMR = 0.1%).
- ✓ For higher security thresholds (e.g. FMR=0.01%), Random_key is competitive w.r.t other cancelable strategies using other key selections.

Results

Evolution of the average information loss



- ✓ The attacker will be accepted by the unprotected system in most of the iterations or attempts .
- ✓ No drastic reduction in the dissimilarity score is observed in cancelable schemes.
- ✓ We have high security?

Horizontal black line visualizes the threshold fixed at FMR=0.1% for unprotected system

Results

TABLE I: Error rates(%). The best results are highlighted in bold.

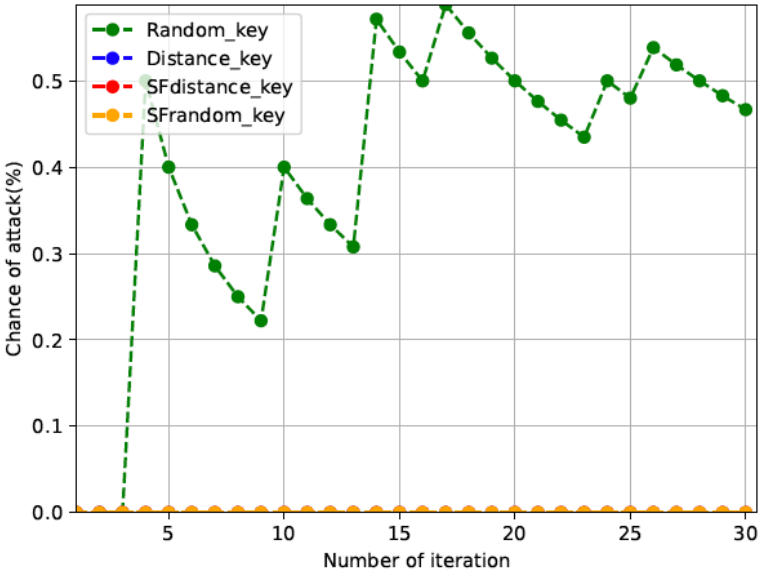
System	Selection of key	EER	FMR	FNMR	Threshold	ASR
Unprotected	-	1.71	0.0010	2.00	1.1981	1.67
	-		0.0100	2.00	1.2342	6.33
	-		0.1000	2.00	1.2667	18.20
	-		1.0000	1.86	1.3074	40.73
OTB-morph	Random_key	0.86	0.0010	2.14	1.1543	0.47
			0.0100	1.42	1.1894	2.07
			0.1000	1.00	1.2292	8.93
			1.0000	0.86	1.2781	29.60
	Distance_key	1.14	0.0010	11.29	1.0751	**0.00**
			0.0100	2.71	1.1811	**0.60**
			0.1000	1.29	1.2317	**5.87**
			1.0000	1.14	1.2818	**25.33**
	SFdistance_key	0.57	0.0010	15.57	1.0370	**0.00**
			0.0100	3.86	1.1451	**1.00**
			0.1000	1.29	1.2043	7.60
			1.0000	0.57	1.2566	**25.40**
	SFrandom_key	0.57	0.0010	15.57	0.9925	**0.00**
			0.0100	3.86	1.1443	**1.13**
			0.1000	1.14	1.2071	8.87
			1.0000	0.57	1.2567	28.07

Attack chances

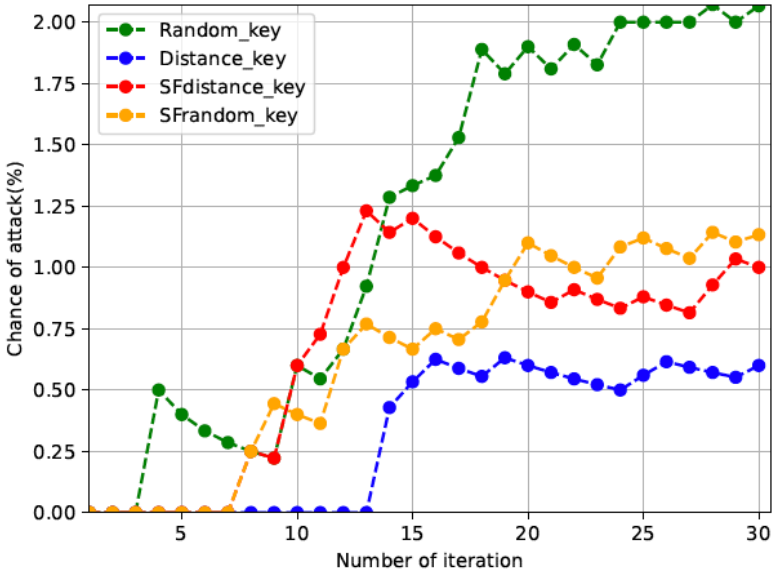
- ✓ Key-selection process helps to decrease the attack chance compared to the unprotected system.
- ✓ For the most practical threshold (FMR=0.1%), protected system represents approx. seven times lower than the one achieved by the unprotected system.
- ✓ For more stringent security thresholds, Random_key is vulnerable w.r.t other key selections:
  - FMR=0.001%: 0% of attack chance
  - FMR=0.01%: slight increase resulting approx. in 1%.

Results

Cumulative attack chances over the stringent security thresholds



(a) FMR=0.001%

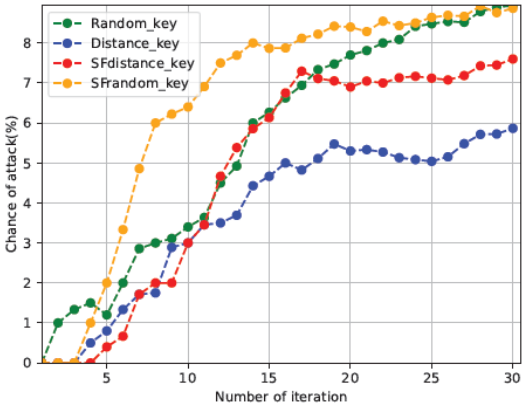


(b) FMR=0.01%

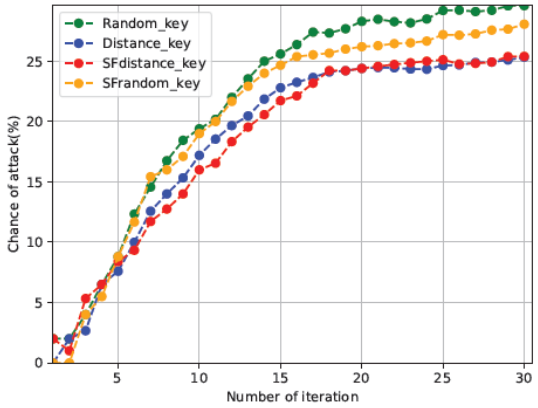
- ✓ The attack rate strongly depends on the security thresholds fixed in the system.
- ✓ Attack chance for FMR=0.001% is reduced to 0% for most of the key-selection strategies.
- ✓ The attack chance looks constant from a certain number of iterations (e.g. FMR=0.01% for red, yellow, and blue curves at 15).

Results

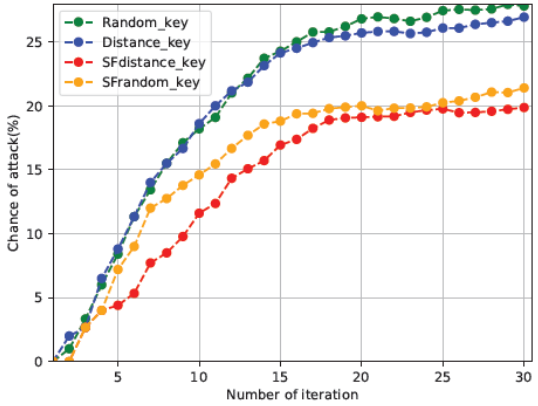
Cumulative attack chances over the most practical security thresholds.



(c) FMR=0.1%



(d) FMR=1.0%



(e) FMR=FNMR

- ✓ Distance_key appears most promising for the most practical threshold (FMR=0.1%).
- ✓ The opposite demographic information included on the morphing process reduces the attack chance for the more relaxed thresholds.

Conclusions

- Varying the criteria of key selection in order to produce a worse similarity score led to higher confusion for the learning process of the attacker.
- Future work could introduce the randomness of the key selection by using the different criteria utilised in this work.
- Further work could be focused on analysing information loss from existing biometric templates protection schemes and working on feature-level.
- Iterative optimization may be explored on state-of-the-art face recognition models and different comparators.

Thank you for your attention!
Questions ?