Scientific Talk

Stable Hash Generation for Efficient Privacy-Preserving Face Identification

Dailé Osorio-Roig

da/sec – Biometrics and Internet Research Group

Hochschule Darmstadt

Agenda

1. Introduction and Motivation.
2. Proposed Approaches.
3. Proposed System.
4. Experimental Setup.
5. Evaluation and Result Discussion.
6. Future Work.

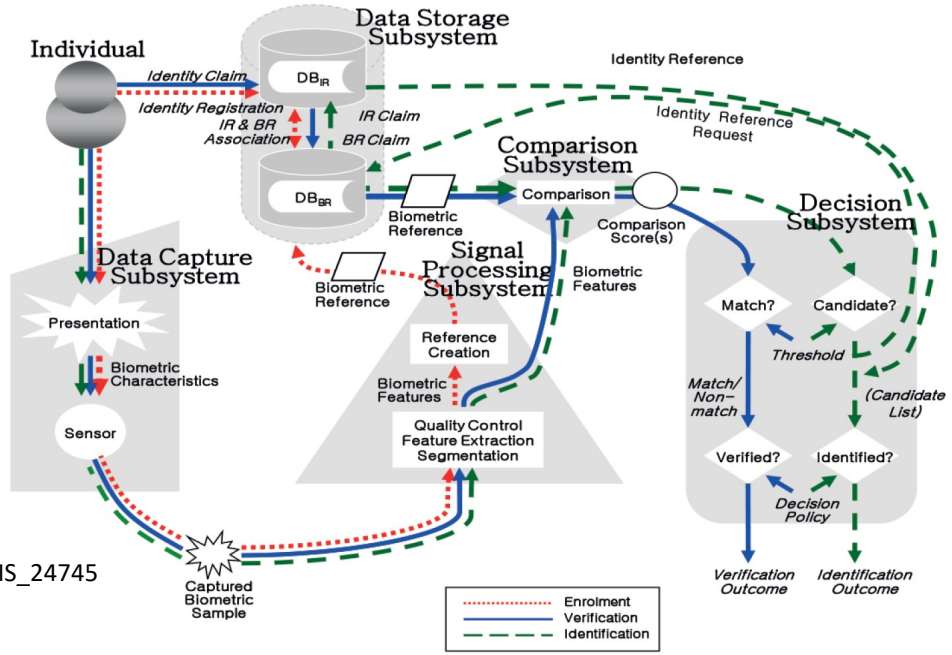
Introduction and Motivation

Biometric Operation Modes

Verification A biometric claim through one-to-one (1:1) biometric comparison.

Identification A biometric probe is compared against all stored biometric references.

- ***one-to-many*** (1:N) biometric comparisons.
- scenarios: closed-set identification and ***open-set*** identification.



Source: ISO_IEC_DIS_24745

Exhaustive Search (1:N)

Motivation

Operational and planned large-scale biometric identification systems host millions of enrolled subjects (e.g., Aadhaar system on ***1.3 billion of data***) [1].

Consequences

- Time-consuming task: ***comparison cost***.
- Probability of the ***false match*** increases [2]. $P_N = 1 - (1 - P_1)^N$
- Properties of biometric data (e.g., ***fuzzy data***) [1].

[1] *Drozdowski P, Rathgeb C, Busch C. Computational workload in biometric identification systems: an overview. IET Biometrics. 2019 Jul 23;8(6):351-68.*
[2] *Daugman J. Biometric decision landscapes. University of Cambridge, Computer Laboratory; 2000.*

Solutions

Workload Reduction Methods

Accelerate the searches in large-scale biometric identification systems

How?

- Search space reduction to a ***low number of comparisons*** (referring to *pre-selection methods*).
- Reduction of the computational cost of the ***individual template comparisons*** (referring to *feature transformation*).
- Others (e.g., fusion techniques, acceleration on software optimisation, etc) [1].

Issues

- ✓ Degradation of the ***biometric performance***.
- ✓ ***Scalability*** is questionable.
- ✓ Schemes do no incorporate ***privacy protection***.

[1] *Drozdowski P, Rathgeb C, Busch C. Computational workload in biometric identification systems: an overview. IET Biometrics. 2019 Jul 23;8(6):351-68.*

Solutions

Workload Reduction Methods

Accelerate the searches in large-scale biometric identification systems

How?

- Search space reduction to a ***low number of comparisons*** (referring to *pre-selection methods*).
- Reduction of the computational cost of the ***individual template comparisons*** (referring to *feature transformation*).
- Others (e.g., fusion techniques, acceleration on software optimisation, etc) [1].

Issues

- ✓ Degradation of the ***biometric performance***.
- ✓ ***Scalability*** is questionable.
- ✓ Schemes do no incorporate ***privacy protection***

[1] *Drozdowski P, Rathgeb C, Busch C. Computational workload in biometric identification systems: an overview. IET Biometrics. 2019 Jul 23;8(6):351-68.*

Privacy protection

Motivation

- Biometric data is ***sensitive*** [3].
- Different ***privacy threats*** [4].

Solutions

- Development of ***Biometric Template Protection*** (BTP) schemes.

Cancelables biometrics

Biometric cryptosystems

Homomorphic encryption

[3] European Union (EU) General Data Protection Regulation 2016/679.
[4] Gomez-Barrero M, Galbally J, Rathgeb C, Busch C. General framework to evaluate unlinkability in biometric template protection systems. IEEE Transactions on Information Forensics and Security. 2017 Dec 29;13(6):1406-20.

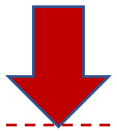
Biometric Template Protection

Advantages

- Designed for ***fuzzy biometric data*** [5].
- BTP must satisfy four main ***requirements*** (e.g., *unlinkability*, *irreversibility*, *renewability*, and *performance preservation*) from ISO/IEC IS 24745.
- Comparison in the ***protected domain***.

Issues

- ✓ High cost of comparison in the protected domain.



BTP schemes are less suitable for large-scale identification systems which perform ***exhaustive searches***

[5] Rathgeb C, Uhl A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security. 2011 Dec;2011(1):1-25.

Biometric Template Protection

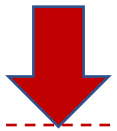
Advantages

- Designed for ***fuzzy biometric data*** [5].
- BTP must satisfy four main ***requirements*** (e.g., *unlinkability*, *irreversibility*, *renewability*,

Combine Workload Reduction (WR) strategies with BTP schemes

Issues

- ✓ High cost of comparison in the protected domain.



BTP schemes are less suitable for large-scale identification systems which perform ***exhaustive searches***

[1] *Drozdowski P, Rathgeb C, Busch C. Computational workload in biometric identification systems: an overview. IET Biometrics. 2019 Jul 23;8(6):351-68.*

Proposed Approaches

Proposed Approaches

Approach	WR category	BTP category	Exhaustive search
Wan *et al.* [6]	Pre-selection/Feature transformation	No traditional BTP	Yes
Murakami *et al.* [7]	Feature transformation	Cancelable biometrics	Yes
Dong *et al.* [8]	Feature transformation	Cancelable biometrics	Yes
Sardar *et al.* [9]	Feature transformation	Cancelable biometrics	Yes
Drozdowski *et al*. [10]	Feature transformation	Fully homomorphic encryption	Yes
Engelsma *et al.* [11]	Feature transformation	Fully homomorphic encryption	Yes

[6] *Wang Y, Wan J, Guo J, Cheung YM, Yuen PC. Inference-based similarity search in randomized Montgomery domains for privacy-preserving biometric identification. IEEE transactions on pattern analysis and machine intelligence. 2017 Jul 14;40(7):1611-24.*
[7] *Murakami T, Fujita R, Ohki T, Kaga Y, Fujio M, Takahashi K. Cancelable permutation-based indexing for secure and efficient biometric identification. IEEE Access. 2019 Apr 2;7:45563-82.*
[8] *Dong X, Kim S, Jin Z, Hwang JY, Cho S, Teoh AB. Open-set face identification with index-of-max hashing by learning. Pattern Recognition. 2020 Jul 1;103:107277.*
[9] *Sardar A, Umer S, Pero C, Nappi M. A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template. IEEE Access. 2020 Jun 3;8:105263-77.*
[10] *Drozdowski, P., Buchmann, N., Rathgeb, C., Margraf, M. and Busch, C., 2019, September. On the application of homomorphic encryption to face identification. In 2019 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-5).*
[11] *Engelsma JJ, Jain AK, Boddeti VN. HERS: Homomorphically Encrypted Representation Search. arXiv preprint arXiv:2003.12197. 2020 Mar 27.*

Proposed Approaches

Approach	WR category	BTP category	Exhaustive search
Wan *et al.* [6]	Pre-selection/Feature transformation	No traditional BTP	Yes
Murakami *et al.* [7]	Feature transformation	Cancelable biometrics	Yes
Dong *et al.* [8]			
Sardar *et al.* [9]			
Drozdowski *et al*		encryption	
Engelsma *et al.* [11]	Feature transformation	Fully homomorphic encryption	Yes

What can be done?

[6] *Wang Y, Wan J, Guo J, Cheung YM, Yuen PC. Inference-based similarity search in randomized Montgomery domains for privacy-preserving biometric identification. IEEE transactions on pattern analysis and machine intelligence. 2017 Jul 14;40(7):1611-24.*
[7] *Murakami T, Fujita R, Ohki T, Kaga Y, Fujio M, Takahashi K. Cancelable permutation-based indexing for secure and efficient biometric identification. IEEE Access. 2019 Apr 2;7:45563-82.*
[8] *Dong X, Kim S, Jin Z, Hwang JY, Cho S, Teoh AB. Open-set face identification with index-of-max hashing by learning. Pattern Recognition. 2020 Jul 1;103:107277.*
[9] *Sardar A, Umer S, Pero C, Nappi M. A novel cancelable FaceHashing technique based on non-invertible transformation with encryption and decryption template. IEEE Access. 2020 Jun 3;8:105263-77.*
[10] *Drozdowski, P., Buchmann, N., Rathgeb, C., Margraf, M. and Busch, C., 2019, September. On the application of homomorphic encryption to face identification. In 2019 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-5).*
[11] *Engelsma JJ, Jain AK, Boddeti VN. HERS: Homomorphically Encrypted Representation Search. arXiv preprint arXiv:2003.12197. 2020 Mar 27.*

Proposed System

What can be done?

Workload Reduction Methods

Accelerate the searches in large-scale face biometric identification systems

How?

- **Search space reduction to a *low number of comparisons* (referring to *pre-selection methods*).**
- Reduction of the computational cost of the *individual template comparisons* (referring to *feature transformation*).
- Others (e.g., fusion techniques, acceleration on software optimisation, etc).

Privacy protection

Development of *Biometric Template Protection* (BTP) schemes.

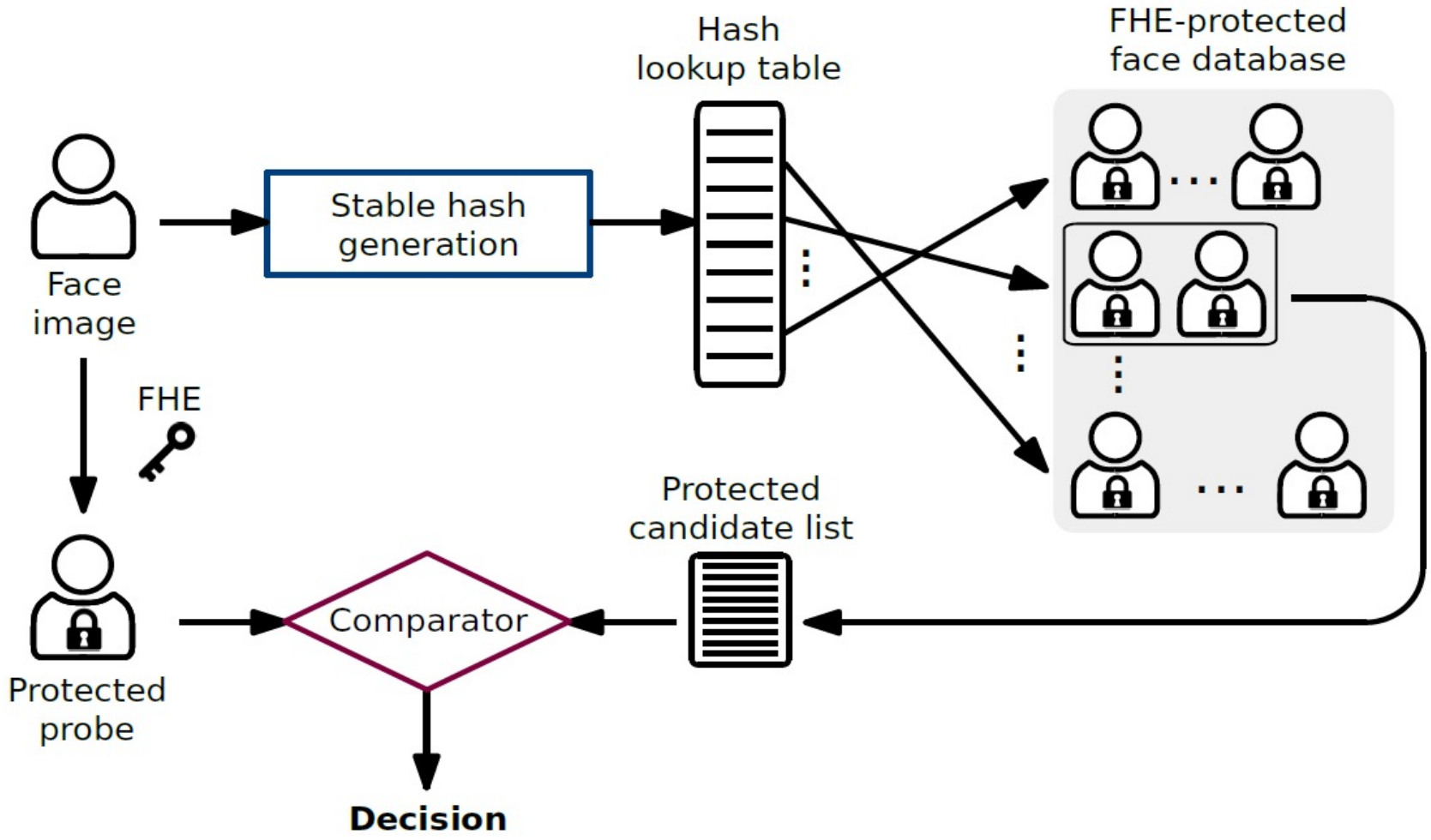
How?

Cancelables biometrics

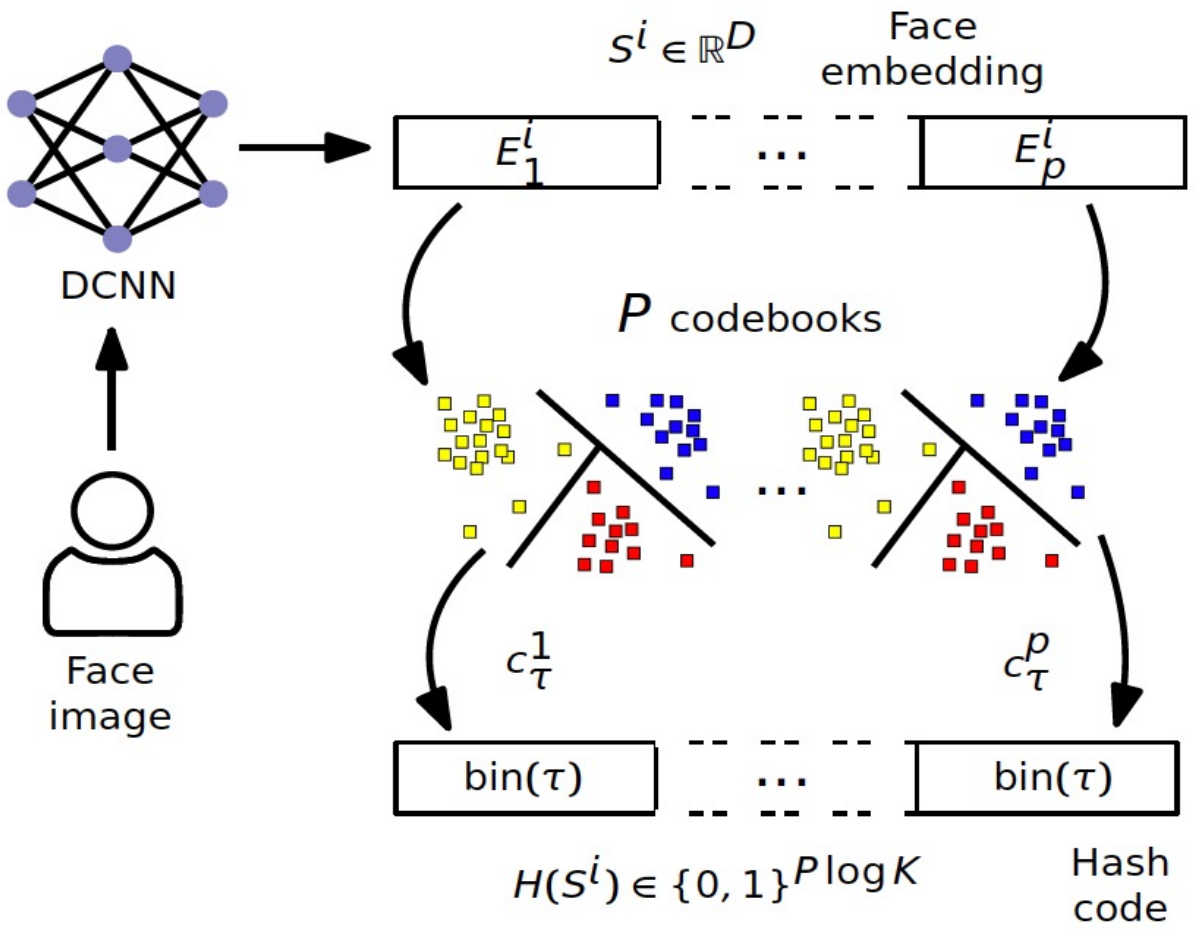
Homomorphic encryption

Biometric cryptosystems

Hash look-up table



Hash generation



- K-means
- K-medoids
- Gaussian mixture models (GMM)
- Affinity propagation (AP)

- Number possible of entries: K^P
  - P number of sub-vectors.
  - K number of centers.

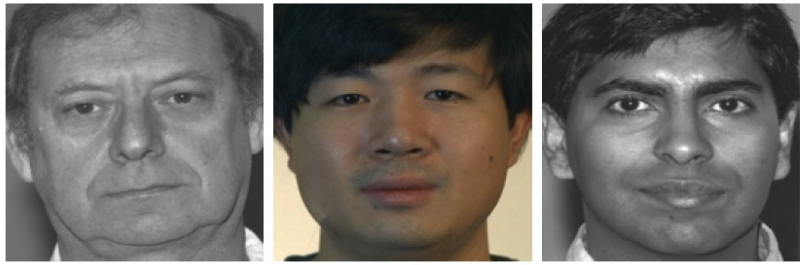
- Probability of collision:

$$f = \begin{cases} 1 & \text{if } N > K^P \\ \frac{N}{K^P} & \text{otherwise.} \end{cases}$$

Experimental Setup

Experimental Setup

- Databases:
  - FERET: Controlled subset.
  - FEI: Pose variability.
  - LFW: First dataset focused on the large-scale unconstrained face recognition problem.



(a) FERET

(b) FEI

(c) LFW

Experimental Setup

- Encoding scheme: Brakerski/Fan-Vercauteren (BFV) scheme.
- Face recognition:

Face recognition system	Pre-trained model	Feature embedding size	Loss function
FaceNet	Inception-ResNet-v1[1]	512	Triplet
ArcFace1	ResNet-100[2]	512	Additive Angular Margin
ArcFace2	MobileFaceNet[3]	128	Additive Angular Margin
VGG-Face2	Senet-50[4]	2048	Soft-max

[1] https://github.com/davidsandberg/facenet
[2] https://github.com/deepinsight/insightface/wiki/Model-Zoo
[3] https://github.com/deepinsight/insightface/wiki/Model-Zoo
[4] https://github.com/ox-vgg/vgg_face2

Protocols

Dataset	Scenario	Training	Enrolment	Search
LFW	Closed-set	2898	1830	4902
	Open-set O1	2898	1830	4902 genuines 1359 non-mated probes
	Open-set O2	2898	1830	4902 genuines 4069 non-mated probes
FERET	Closed-set	747	747	474
	Open-set	747	747	474 genuines 1476 non-mated probes
FEI	Closed-set	2000	2000	776
	Open-set	1890	1890	732 genuines 136 non-mated probes

Metrics

- Pre-selection error (Pe): Lower value is better (e.g., 0%)
- Hit-rate (1-Pe): Higher value is better (e.g., 100%)
- Cumulative Match Characteristic (CMC) curves.
- Detection Error Trade-off (DET) curves between False Positive Identification Rates (FPIR) and False Negative Identification Rates (FNIR).
- Workload (W).

Source: ISO/IEC JTC1 SC37

Experimental Results

Closed-set scenario

Table: Identification rate (%) at rank-1 on exhaustive search.

System	Dataset		
	FEI	FERET	LFW
ArcFace 1	100.00 %	100.00 %	99.84 %
ArcFace 2	98.97 %	100.00 %	99.67 %
FaceNet	99.74 %	100.00 %	85.08 %
VGGFace	99.82 %	99.79 %	99.84 %

- ✓ Model: ResNet-100
- ✓ Size: 512

- ✓ ArcFace 1 recognition system as a feature extractor (for baseline) achieves a high identification rate.
- ✓ Additive Angular Margin loss preserves better the similarity between samples from the same subject.
- ✓ Good indicator for clustering.

Closed-set scenario

Table: Pre-selection error rates (%).

Database	Centers	K-means			K-medoids			GMM			Affinity Propagation		
		$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$
FEI	64	**0**	0.05	1.31	6.75	18.74	46.65	**0**	0.41	15.70			
	128	**0**	**0**	0.13	5.00	11.21	30.93	**0**	**0**	2.37			
	256	0.05	0.15	0.98	1.98	5.28	12.73	0.05	0.1	0.54	**0**	0.03	0.05
	512	0.03	2.55	10.52	0.54	3.76	14.59	0.1	1.57	6.24			
	1024	**0**	6.16	17.5	**0.21**	9.36	13.46	0.08	5.21	13.76			
FERET	64	**0**	0.46	2.95	18.48	39.49	74.25	**0**	0.21	2.57			
	128	**0**	0.04	1.77	14.3	68.78	60.13	**0**	0.25	0.72			
	256	**0**	**0**	0	11.90	20.76	39.28	**0**	**0**	0.08	**0**	**0**	**0**
	512	**0**	5.49	13.38	**5.86**	12.28	32.15	**0**	4.09	14.3			
LFW	64	7.01	18.43	44.19	32.82	57.46	77.23	3.88	8.08	36.32			
	128	6.43	15.48	33.73	33.08	61.03	77.19	4.19	7.76	21.79			
	256	5.01	10.53	26.69	27.51	58.02	76.89	3.59	6.91	16.34			
	512	3.24	5.31	10.36	21.11	48.51	73.39	3.37	8.59	5.09			
	1024	**2.19**	**2.19**	2.45	**18.51**	33.5	61.9	**2.14**	2.26	3.09	2.28	**2.23**	3.14

Closed-set scenario

Table: Pre-selection error rates (%).

Database	Centers	K-means			K-medoids			GMM			Affinity Propagation		
		$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$
FEI	64	**0**	0.05	1.31	6.75	18.74	46.65	**0**	0.41	15.70			
	128	**0**	**0**	0.13	5.00	11.21	30.93	**0**	**0**	2.37			
	256	0.05	0.15	0.98	1.98	5.28	12.73	0.05	0.1	0.54	**0**	0.03	0.05
	512	0.03	2.55	10.52	0.54	3.76	14.59	0.1	1.57	6.24			
	1024	**0**	6.16	17.5	**0.21**	9.36	13.46	0.08	5.21	13.76			
FERET	64	**0**	0.46	2.95	18.48	39.49	74.25	**0**	0.21	2.57			
	128	**0**	0.04	1.77	14.3	68.78	60.13	**0**	0.25	0.72			
	256	**0**	**0**	0	11.90	20.76	39.28	**0**	**0**	0.08	**0**	**0**	**0**
	512	**0**	5.49	13.38	**5.86**	12.28	32.15	**0**	4.09	14.3			
LFW	64	7.01	18.43	44.19	32.82	57.46	77.23	3.88	8.08	36.32			
	128	6.43	15.48	33.73	33.08	61.03	77.19	4.19	7.76	21.79			
	256	5.01	10.53	26.69	27.51	58.02	76.89	3.59	6.91	16.34			
	512	3.24	5.31	10.36	21.11	48.51	73.39	3.37	8.59	5.09			
	1024	**2.19**	**2.19**	2.45	**18.51**	33.5	61.9	**2.14**	2.26	3.09	2.28	**2.23**	3.14

Closed-set scenario

Table: Pre-selection error rates (%).

Database	Centers	K-means			K-medoids			GMM			Affinity Propagation		
		$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$
FEI	64	**0**	0.05	1.31	6.75	18.74	46.65	**0**	0.41	15.70			
	128	**0**	**0**	0.13	5.00	11.21	30.93	**0**	**0**	2.37			
	256	0.05	0.15	0.98	1.98	5.28	12.73	0.05	0.1	0.54	**0**	0.03	0.05
	512	0.03	2.55	10.52	0.54	3.76	14.59	0.1	1.57	6.24			
	1024	**0**	6.16	17.5	**0.21**	9.36	13.46	0.08	5.21	13.76			
FERET	64	**0**	0.46	2.95	18.48	39.49	74.25	**0**	0.21	2.57			
	128	**0**	0.04	1.77	14.3	68.78	60.13	**0**	0.25	0.72			
	256	**0**	**0**	0	11.90	20.76	39.28	**0**	**0**	0.08	**0**	**0**	**0**
	512	**0**	5.49	13.38	**5.86**	12.28	32.15	**0**	4.09	14.3			
LFW	64	7.01	18.43	44.19	32.82	57.46	77.23	3.88	8.08	36.32			
	128	6.43	15.48	33.73	33.08	61.03	77.19	4.19	7.76	21.79			
	256	5.01	10.53	26.69	27.51	58.02	76.89	3.59	6.91	16.34			
	512	3.24	5.31	10.36	21.11	48.51	73.39	3.37	8.59	5.09			
	1024	**2.19**	**2.19**	2.45	**18.51**	33.5	61.9	**2.14**	2.26	3.09	2.28	**2.23**	3.14

Closed-set scenario

Table: Pre-selection error rates (%).

Database	Centers	K-means			K-medoids			GMM			Affinity Propagation		
		$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$
FEI	64	**0**	0.05	1.31	6.75	18.74	46.65	**0**	0.41	15.70			
	128	**0**	**0**	0.13	5.00	11.21	30.93	**0**	**0**	2.37			
	256	0.05	0.15	0.98	1.98	5.28	12.73	0.05	0.1	0.54	**0**	0.03	0.05
	512	0.03	2.55	10.52	0.54	3.76	14.59	0.1	1.57	6.24			
	1024	**0**	6.16	17.5	**0.21**	9.36	13.46	0.08	5.21	13.76			
FERET	64	**0**	0.46	2.95	18.48	39.49	74.25	**0**	0.21	2.57			
	128	**0**	0.04	1.77	14.3	68.78	60.13	**0**	0.25	0.72			
	256	**0**	**0**	0	11.90	20.76	39.28	**0**	**0**	0.08	**0**	**0**	**0**
	512	**0**	5.49	13.38	**5.86**	12.28	32.15	**0**	4.09	14.3			
LFW	64	7.01	18.43	44.19	32.82	57.46	77.23	3.88	8.08	36.32			
	128	6.43	15.48	33.73	33.08	61.03	77.19	4.19	7.76	21.79			
	256	5.01	10.53	26.69	27.51	58.02	76.89	3.59	6.91	16.34			
	512	3.24	5.31	10.36	21.11	48.51	73.39	3.37	8.59	5.09			
	1024	**2.19**	**2.19**	2.45	**18.51**	33.5	61.9	**2.14**	2.26	3.09	2.28	**2.23**	3.14

Effect of the image quality

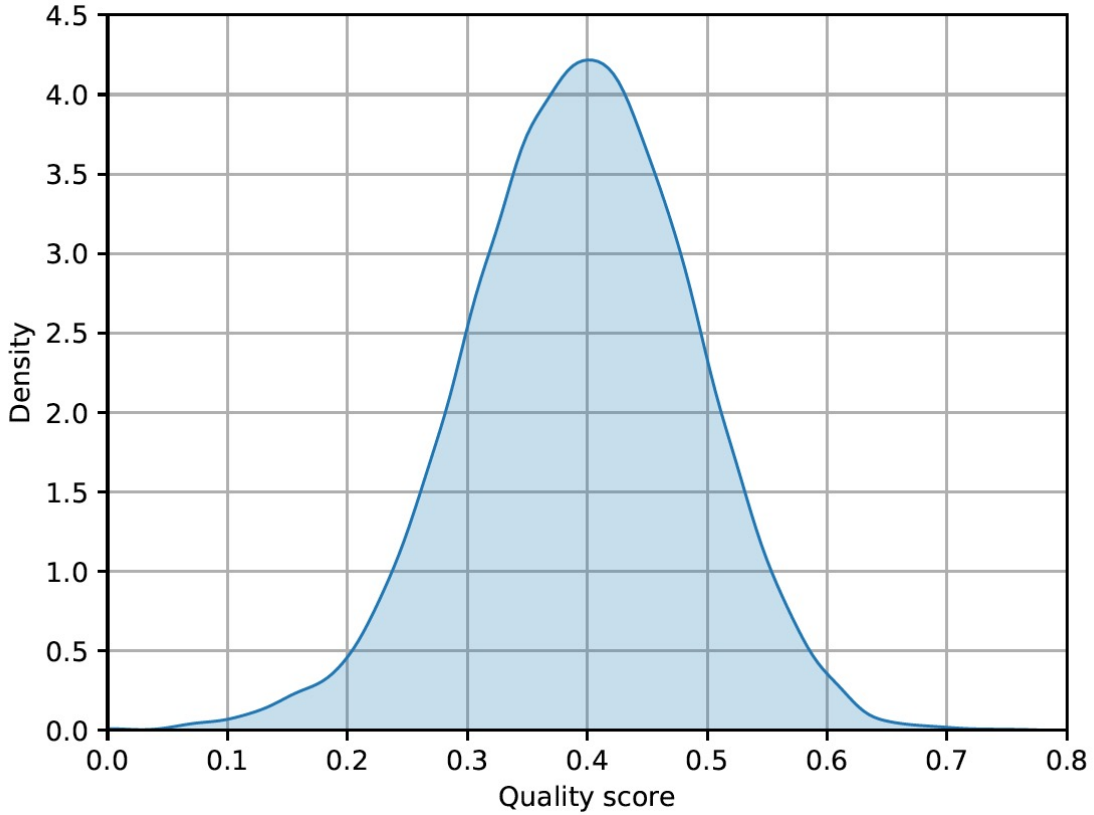


Figure: Quality scores computed by FaceQNet on the LFW database.

✓ Most samples in LFW (around 80%) pose an image quality score below 0.5.

Effect of the image quality

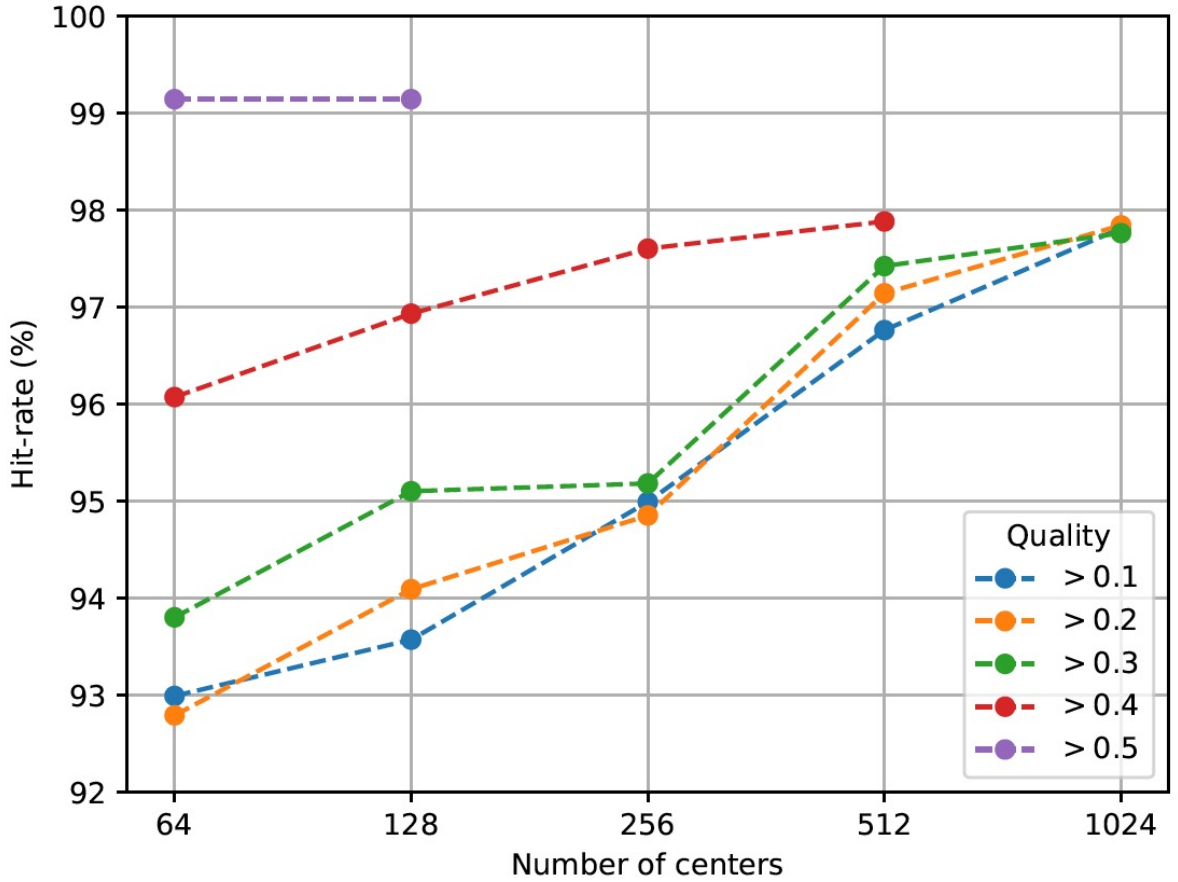


Figure: Impact of the quality on K clusters for P = 1.

- ✓ Hit-rates on different ***K*** improve as increase the image quality.
- ✓ Soundness of our hashing-based system to correctly identify high-quality face images.
- ✓ Smaller clusters ***K*** to get low intra-class variability.

Effect of the number of samples

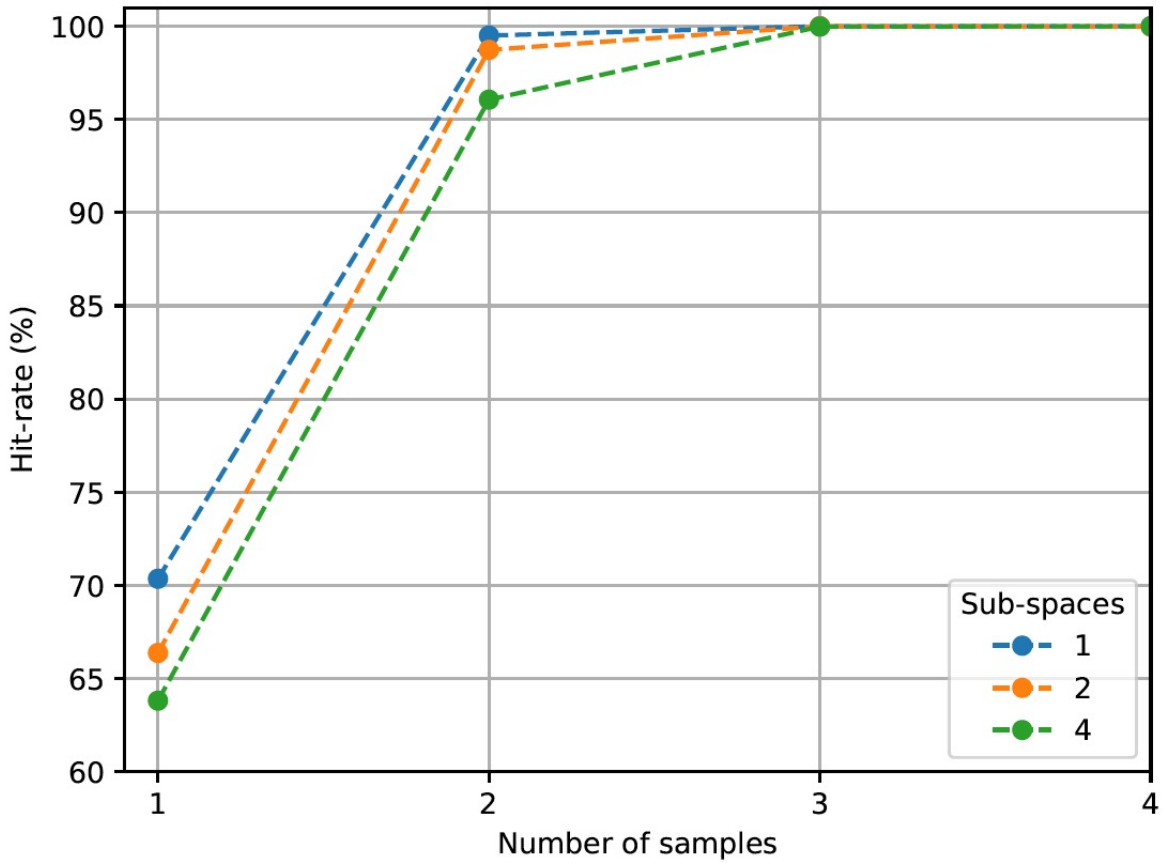


Figure: Analysis of the number of samples used for training our Hash generation scheme by using AP.

- ✓ High biometric performance by using only three samples for training on the FEI database.

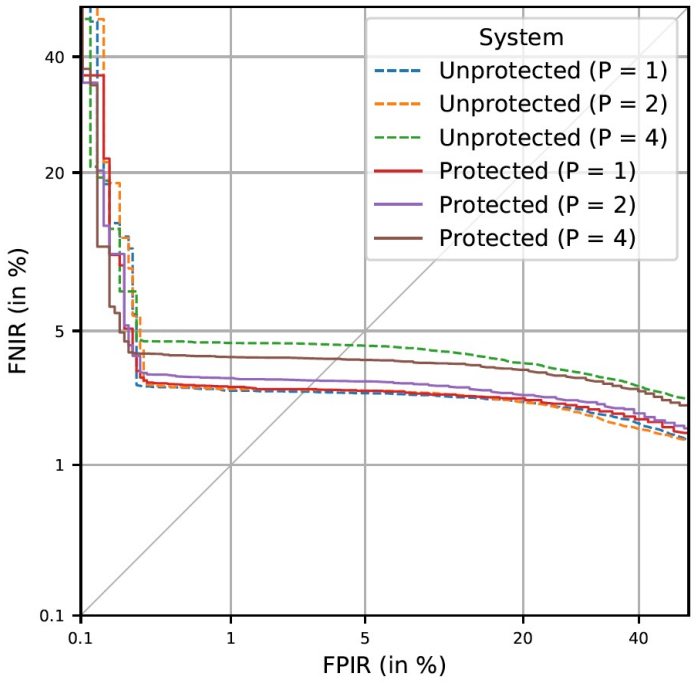
Experimental Results in closed-set scenario

Table: Identification rate (%) at rank-1 of our hash generation w.r.t baseline.

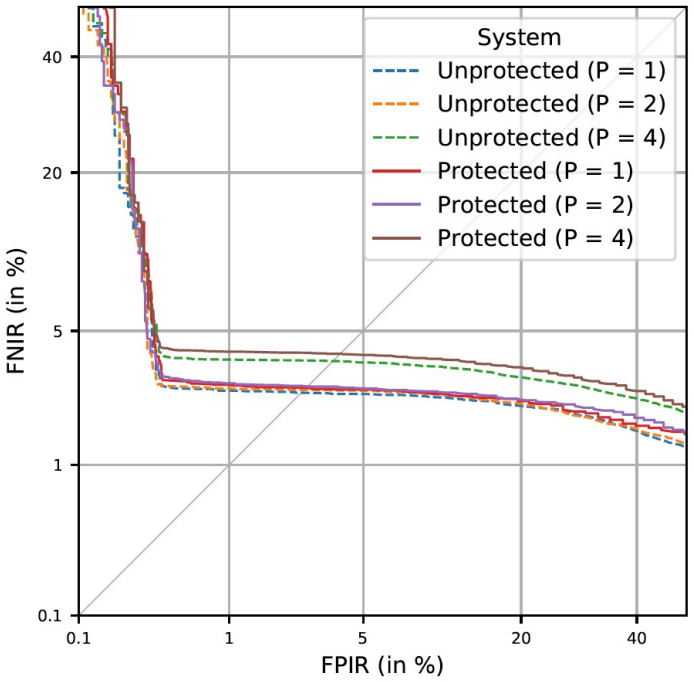
Dataset	GMM			AP			Baseline
	$P=1$	$P=2$	$P=4$	$P=1$	$P=2$	$P=4$	
FEI	100.00	99.98	99.38	100.00	100.00	100.00	100.00
FERET	100.00	100.00	100.00	100.00	100.00	100.00	100.00
LFW	99.67	99.81	98.87	99.84	99.68	99.68	99.84

- ✓ First position of the candidate list (greater 98.87%).
- ✓ AP for open-set scenarios.

DET curves



LFW(O1)



LFW(O2)

- ✓ AP as best performing hash generation.
- ✓ FERET with FNIR=0.2% (here FPIR=0.0%).
- ✓ FEI with FNIR=0.0% (here FPIR=0.0%).
- ✓ LFW with FNIR=2.5% (here FPIR=1.0%)

Experimental Results in open-set scenario

(a) probe: quality = 0.39

(b) references: quality < 0.43

Figure: Example of false match between a non-mated probe and references.

- ✓ Effect of the image quality in open-set scenario.

Workload reduction

Table: Average workload reduction results.
N= 1177, Theta= 750ms, Beta= 0.003ms

K	Metrics	$P=1$	$P=2$	$P=4$
64	γ	18.3906	1.3282	1.0020
	p	156×10^{-4}	11×10^{-4}	8×10^{-4}
	W	13.77×10^{3}	0.97×10^{3}	0.71×10^{3}
128	γ	9.1953	1.1444	1.0007
	p	78×10^{-4}	10×10^{-4}	9×10^{-4}
	W	6.88×10^{3}	0.88×10^{3}	0.79×10^{3}
256	γ	4.5977	1.0815	1.0022
	p	39×10^{-4}	9×10^{-4}	9×10^{-4}
	W	3.44×10^{3}	0.79×10^{3}	0.79×10^{3}
512	γ	2.2988	1.0591	1.0022
	p	20×10^{-4}	9×10^{-4}	9×10^{-4}
	W	1.77×10^{3}	0.79×10^{3}	0.79×10^{3}
1024	γ	1.1424	1.0148	1.0012
	p	10×10^{-4}	9×10^{-4}	9×10^{-4}
	W	0.88×10^{3}	0.79×10^{3}	0.79×10^{3}

Workload reduction $$W = N \times p \times \theta + \beta$$

Penetration rate $$p = \frac{\gamma}{N} \times 100$$

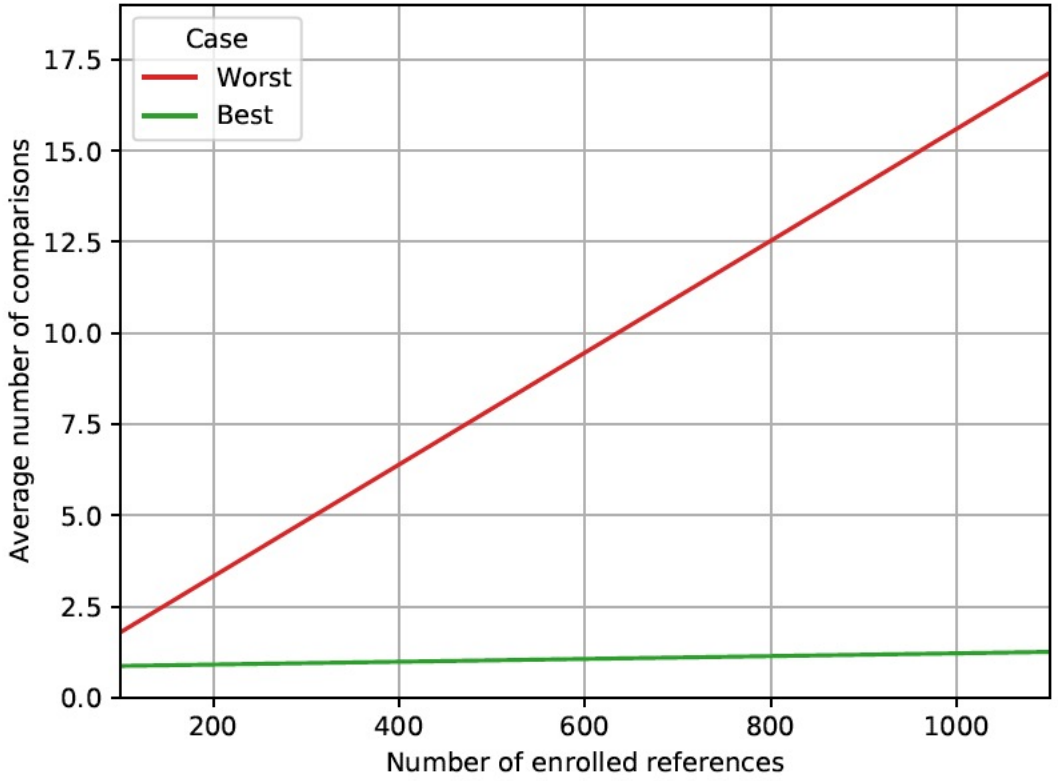
Legend:

- N Number of enrolled subjects (only 1 sample per subject was enrolled).
- p Average proportion of the database that must be searched.
- θ Cost of one-to-one comparison in the encrypted domain.
- β Cost of indexing in the hash look-up table.
- γ Average number of comparisons per hash code when a lookup is carried out.

$W_B = 88.27 \times 10^4$ Baseline

Linear regression

Figure: Relation between the number of enrolled subjects (N) and number of comparisons per hash code.



- ✓ Linear relation between N and number of comparisons.
- ✓ Penetration rate (p) for N = 1 million would be p= 0.03% for K= 1024 (Best) and p= 1.53% for K= 64 (Worst).

Benchmark with the state-of-the-art

Table: Benchmark, in terms of FPIR and FNIR (%), of our identification system for the best performing hash generation on open-set scenarios in the LFW database.

System	WR Category	BTP Category	O1 (FNIR=1000)	O1 (FNIR100)	O2 (FNIR1000)	O2 (FNIR100)
Random IoM [19]	Feature Transformation	Cancelable	40.47	**2.37**	**10.97**	2.37
LIoM [19]	Feature Transformation	Cancelable	45.81	2.43	14.37	**2.25**
Proposed ($P = 1$)	Pre-selection (hash look-up table)	FHE	36.40	2.68	74.07	2.60
Proposed ($P = 2$)	Pre-selection (hash look-up table)	FHE	**34.99**	2.97	70.06	2.80
Proposed ($P = 4$)	Pre-selection (hash look-up table)	FHE	37.63	3.76	88.22	3.10

Conclusions and Future Work

Conclusions

- Compact hash codes generated by Product Quantisation (PQ) are used for efficient indexing via a hash look-up table.
  - ✓ Workload reduction down to 0.1%.
  - ✓ Low pre-selection error rate of less than 1%.
  - ✓ Hash codes for indexing does not leak information from a biometric information.
  - ✓ Trade-offs between biometric performance, workload, and privacy protection.
- PQ-based indexing scheme showed its feasibility over scenarios more challenging (e.g., open-set scenarios) and hence its high level of security.
- Workload Reduction (WR) strategies may be combined with FHE-based schemes to improve its workload and hence its feasibility in real applications.

Future Work

- Dependence of the variability within-subjects in Affinity Propagation (graph-based clustering technique) can be guided through probabilistic approaches.
- More stable hash code may achieved by combining PQ with binary representations and clustering in Hamming.
- Combine pre-selection method with feature transformation to improve the comparison time in the encrypted domain.

Thank you for your attention!
Questions ?