Deep Face Template Protection in the Wild

2022 KMS Spring Meeting
2022. 04. 28

Hanyang University
Hankuk University of Foreign Studies
Sunpill Kim*, Jae Hong Seo, Hoyong Shin

Contents.

Contents.

Part 1,

Motivation

ID/PW: What you know

Decryption Key: What you have

Biometrics: Who you are

Cloud environment may cause serious privacy concerns

- Celebrity's private image leakage
- ID/PW-based access control

Private cloud using data encryption/decryption

- Risk in cryptographic key management
- Server: Secret key protection
  Client: Device loss and hard to applicable to MDE

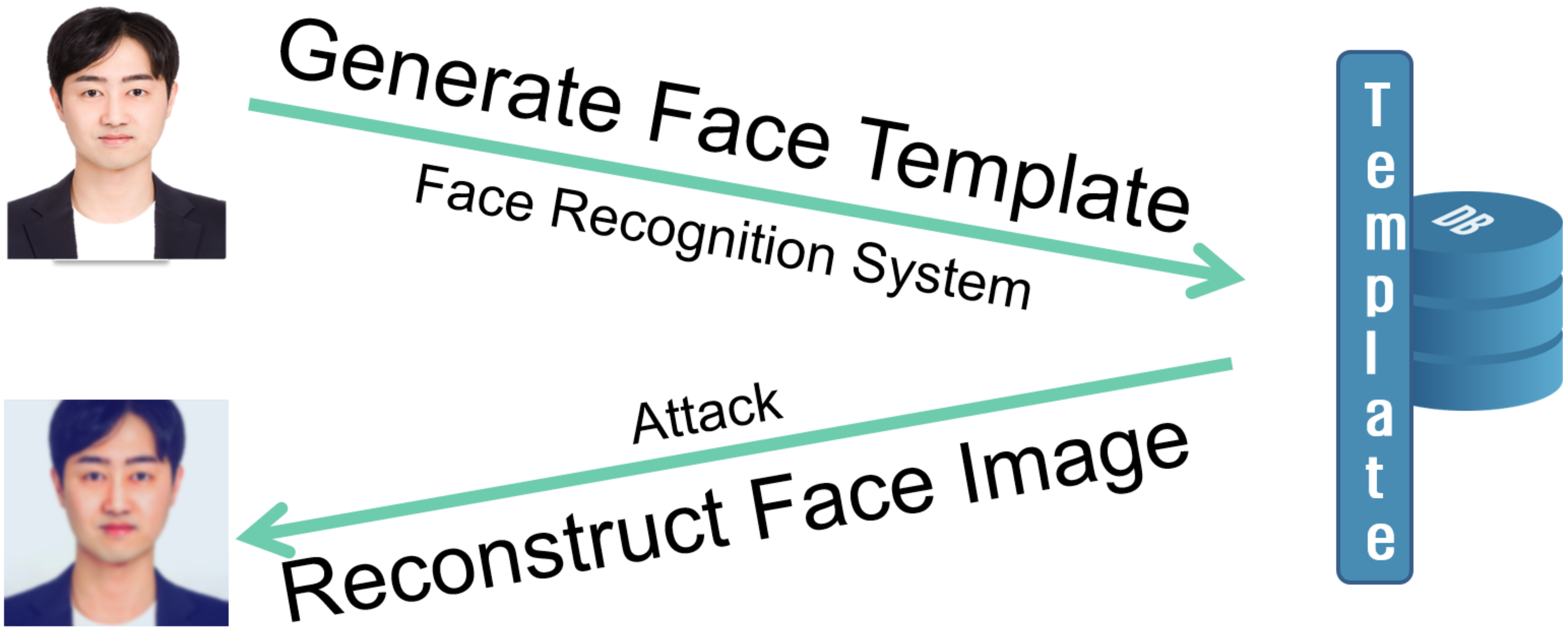
A new solution of data privacy protection in MDE environment

- Real-value based Error Correcting Code
- Fuzzy extractor (IronMask) for biometric-based data encryption

MDE: Multi-Device Environment

Part 1,

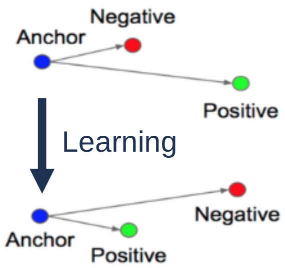
Motivation

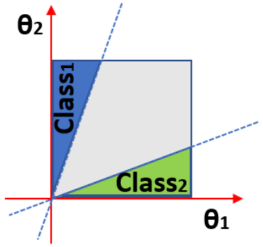


딥러닝 기반 얼굴인식 기술

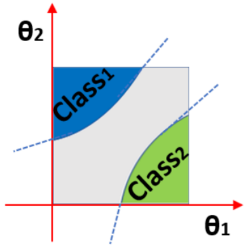
2014
DeepFace[1]
CVPR

2015
VGG-Face[2]
BMVC

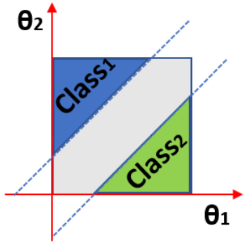




SphereFace

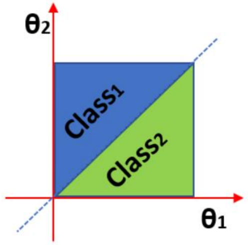


CosFace

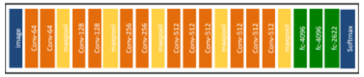


ArcFace

2020
GroupFace[7]
CVPR



Softmax

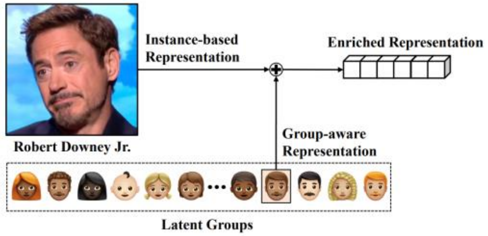

Deeper layer than DeepFace

2015
FaceNet[3]
CVPR

2017
SphereFace[4]
CVPR

2018
CosFace[5]
CVPR

2019
ArcFace[6]
CVPR



[1] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). Deepface: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).
[2] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition.
[3] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).
[4] Liu, W., Wen, Y., Yu, Z., Li, M., Raj, B., & Song, L. (2017). Sphereface: Deep hypersphere embedding for face recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 212-220).
[5] Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D., Zhou, J., ... & Liu, W. (2018). Cosface: Large margin cosine loss for deep face recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 5265-5274).
[6] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4690-4699).
[7] Kim, Y., Park, W., Roh, M. C., & Shin, J. (2020). Groupface: Learning latent groups and constructing group-based representations for face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5621-5630).

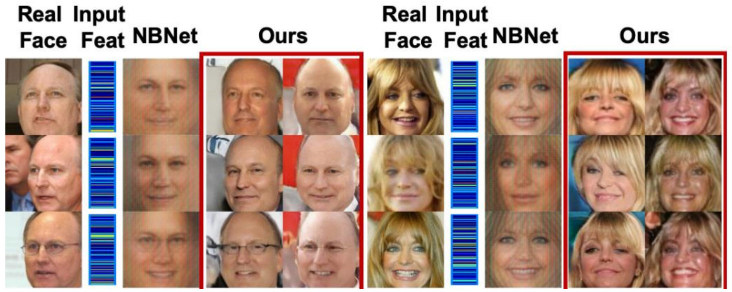
Motivation

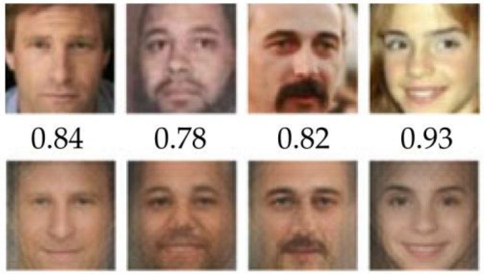
딥러닝 기반 얼굴인식 기술에서의 생체정보 추출 위협

2018

NbNet[8]

IEEE TPAMI





(a) Successful match

2020

Vec2Face[9] (DiBiGAN)

CVPR

Original ArcFace: 0.978 FaceNet: 0.721

2020

[RKK+20]

ECCV Workshop

2021

[RKUP21]

ArXiv

Original		
Ours (RGB)		
ArcFace	0.99	0.99
FaceNet	0.77	0.82

[8] Mai, G., Cao, K., Yuen, P. C., & Jain, A. K. (2018). On the reconstruction of face images from deep face templates. IEEE transactions on pattern analysis and machine intelligence, 41(5), 1188-1202.
[9] Duong, C. N., Truong, T. D., Luu, K., Quach, K. G., Bui, H., & Roy, K. (2020). Vec2Face: Unveil Human Faces From Their Blackbox Features in Face Recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 6132-6141).
[RKK+20] Razzhigaev, A., Kireev, K., Kaziakhmedov, E., Tursynbek, N., & Petiushko, A. (2020, August). Black-Box Face Recovery from Identity Features. In European Conference on Computer Vision (pp. 462-475). Springer, Cham.
[RKUP21] Razzhigaev, A., Kireev, K., Udovichenko, I., & Petiushko, A. (2021). Darker than Black-Box: Face Reconstruction from Similarity Queries. arXiv preprint arXiv:2106.14290.

Contents.

Preliminary

딥러닝 기반 얼굴인식 모델의 안전성을 위한 요구조건

Security Requirements

- Irreversibility: It is computationally infeasible to recover original biometric data from the protected template.
- Revocability: It is possible to issue new protected templates to replace the compromised one.
- Unlinkability: It is computationally infeasible to retrieve any information from protected templates generated in two different applications.

Preliminary

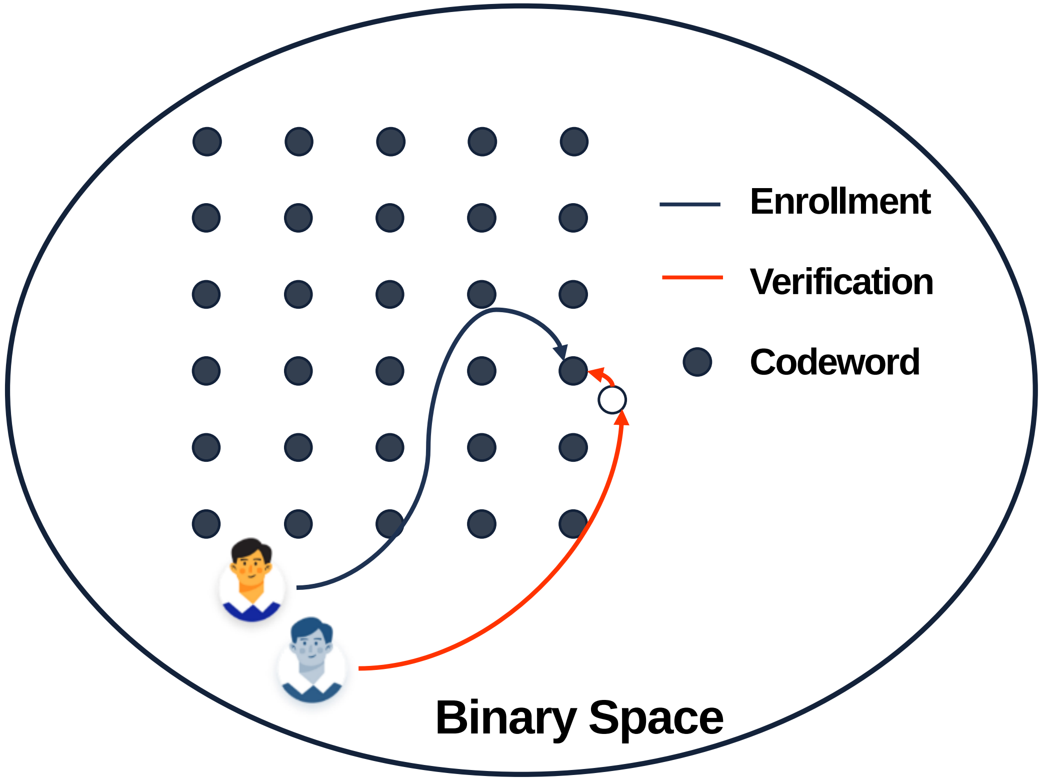
딥러닝 기반 얼굴인식 모델의 템플릿

Deep Face Template

- Space: S^{511} (subset of $\mathbb{R}^{512}$)
- Threshold: $\approx 80^{\circ}$ (degree)

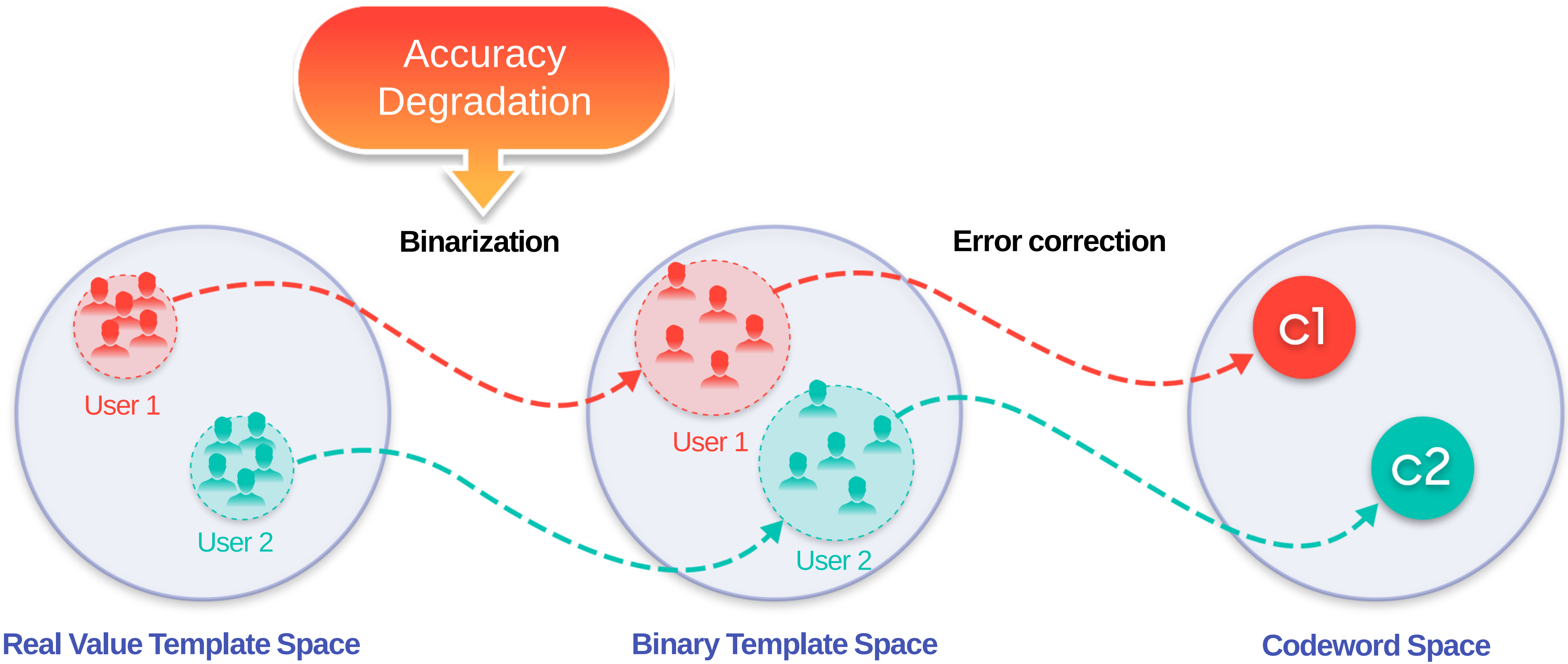
How to control the noise?

- Applying an error correction code
- Reed-Solomon Code, etc



Preliminary

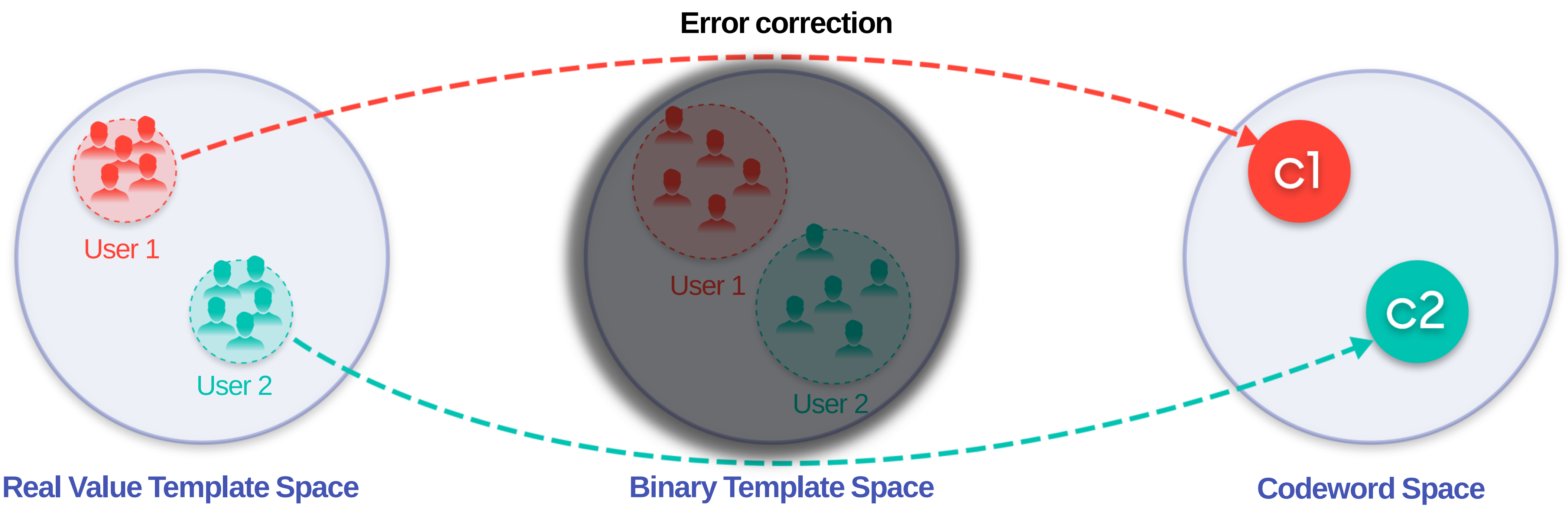
템플릿의 이진화로 인한 성능 저하



IronMask

Construction

- Design a new error correcting code over S^{n-1} for real-valued template
- Generate an orthogonal matrix that keep angular distance between templates after transformation



[CVPR21] Kim, Sunpill, Yunseong Jeong, Jinsu Kim, Jungkon Kim, Hyung Tae Lee, and Jae Hong Seo. "IronMask: Modular architecture for protecting deep face template." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 16125-16134. 2021.

IronMask

ECC for S^{n-1}

- Error correcting code over S^{n-1} with the cosine similarity metric
- For any positive integer α, $\mathcal{C}_\alpha$ is defined as a set of all unit vectors whose entries consist of only three real numbers $-\frac{1}{\sqrt{\alpha}}, 0$, and $\frac{1}{\sqrt{\alpha}}$. Then, each codeword in $\mathcal{C}_\alpha$ has exactly α nonzero entries.

e.g., $\mathcal{C}_1$ over S^3 = {($\pm$1,0,0,0), (0,$\pm$1,0,0), (0,0,$\pm$1,0), (0,0,0,$\pm$1)}

$\mathcal{C}_2$ over S^3 = $\{(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0), (\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}, 0), \ldots, (0, 0, -\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})\}$

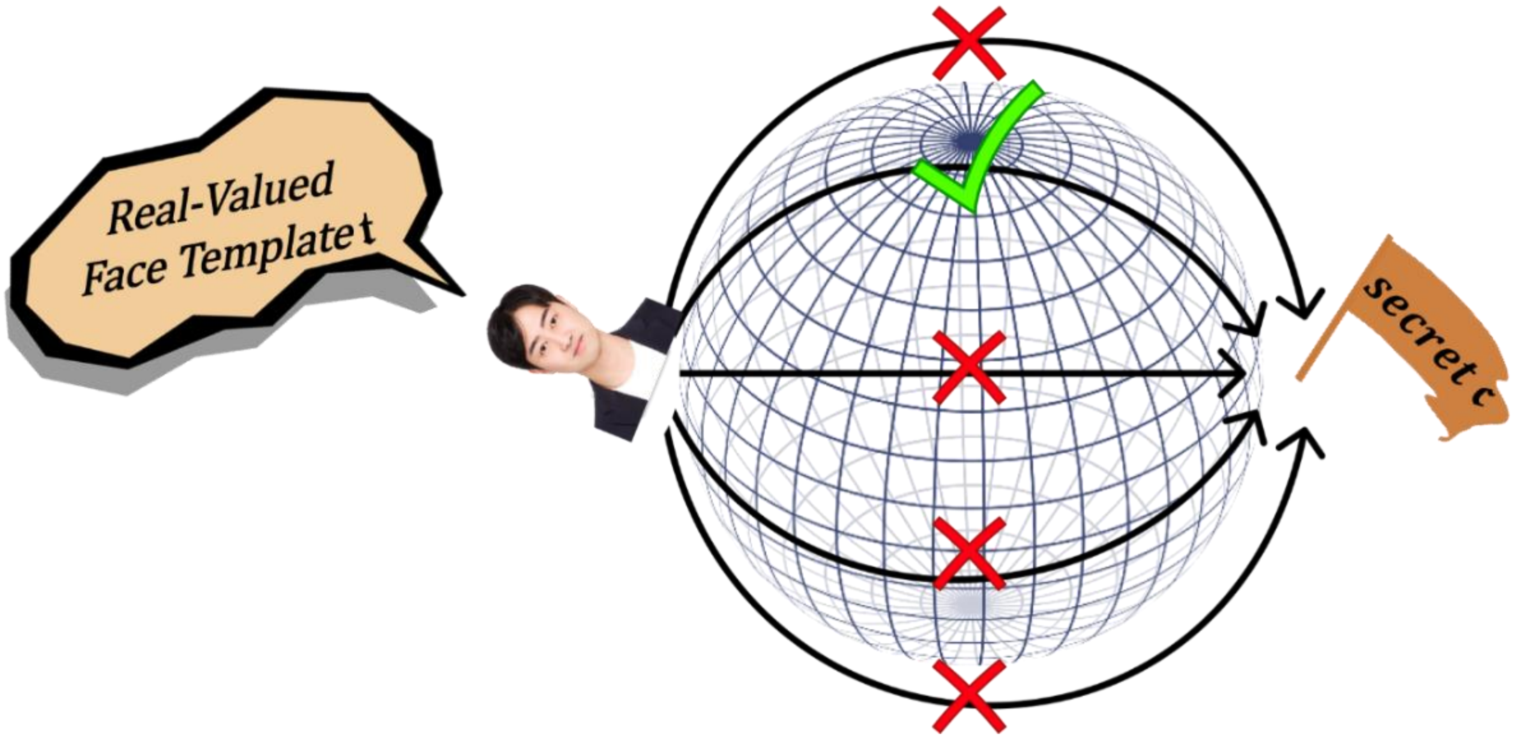
$\mathcal{C}_{16}$ over S^{511} = $\{(\frac{1}{4}, \frac{1}{4}, \ldots, \frac{1}{4}, 0, 0), \ldots, (-\frac{1}{4}, 0, \ldots, \frac{1}{4}, \ldots, -\frac{1}{4}\ 0), \ldots, (0, 0, -\frac{1}{4}, \ldots, -\frac{1}{4})\}$

$$|\mathcal{C}_{16}| = \binom{512}{16} \times 2^{16} \approx 2^{115}, \qquad \mathcal{C}_{16} \subset S^{511}$$

IronMask

Transformation to codeword

- Generate an isometry P randomly among rotation matrices that rotate template to codeword



Contents.

Deep Face Template Protection in the Wild

Analysis of IronMask

Type	Dataset	TAR@FAR
ArcFace	LFW	99.67@3e-4
		99.53@0
	AgeDB	97.00@7e-3
		95.13@0
	CFP-FP	98.11@3e-3
		96.49@0
	IJB-C	97.72@1e-3
		96.60@1e-4
		94.93@1e-5
		90.55@1e-6
		76.48@1e-7

Table 1. ArcFace

Type[3]	i	D(∠)[4]	A(∠)/M(∠)[4]	Sec[4]	Dataset	TAR@FAR
IM	16	20.36	42.15/55.28	115-bit	LFW	57.72@0
					AgeDB	4.58@0
					CFP-FP	5.50@0
					IJB-C	70.56@1e-7
GIM	18	19.19	40.97/53.10	127-bit	LFW	48.79@0
	17	19.75	41.50/54.16	121-bit		53.08@0
	15	21.04	42.62/56.57	109-bit		58.64@0
	14	22.62	43.17/57.17	103-bit		63.09@0
	13	23.56	43.62/58.36	97-bit		72.59@0
	12	24.62	44.15/58.68	91-bit		77.72@0
	11	25.84	44.62/60.84	84-bit		82.08@0

Table 2. IronMask and Generalized IronMask

[3] ‘IM’ and ’GIM’ indicate IronMask and generalized IronMask, respectively.
[4] ‘D’, ‘A’, ‘M’, and ‘Sec’ indicate minimum distance, average(A)/max(M) value of angles between two vectors of accepted pair, and security, respectively.

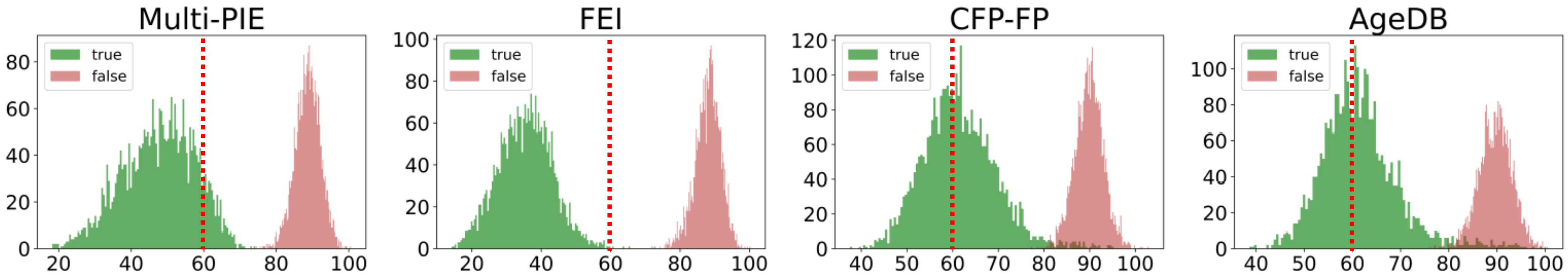
Part 3,

Deep Face Template Protection in the Wild

Analysis of IronMask

Datasets

- Angle distributions of positive and negative pairs from datasets
- The x-axis and y-axis represent angle and number of both positive and negative pairs each
- The graphs for CFP-FP and AgeDB are much more overlapped than those of Multi-PIE and FEI
- IronMask used Multi-PIE and FEI as testsets



Analysis of IronMask

Codeword for S^{n-1}

- For fixed dimension n, number of non-zero element is strongly related to both security and accuracy in completely opposite ways
- Let $\mathcal{C}_i^m \coloneqq \mathcal{C}_i$ over S^{m-1}. Then, we can manipulate threshold for balancing between security and performance using $\mathcal{C}_i^n$ with $n > m$

e.g., $\left|\mathcal{C}_{16}^{512}\right| \approx \binom{512}{16} \times 2^{16} \approx 2^{115}$, providing at least 115-bit security against known attacks

$\left|\mathcal{C}_{10}^{512}\right| \approx \binom{512}{10} \times 2^{10} \approx 2^{78}$, providing at least 78-bit security against known attacks

$\left|\mathcal{C}_{14}^{1024}\right| \approx \binom{1024}{14} \times 2^{14} \approx 2^{118}$, providing at least 118-bit security against known attacks

$\left|\mathcal{C}_{12}^{2048}\right| \approx \binom{2048}{12} \times 2^{12} \approx 2^{115}$, providing at least 115-bit security against known attacks

$\left|\mathcal{C}_{10}^{4096}\right| \approx \binom{4096}{10} \times 2^{10} \approx 2^{108}$, providing at least 108-bit security against known attacks

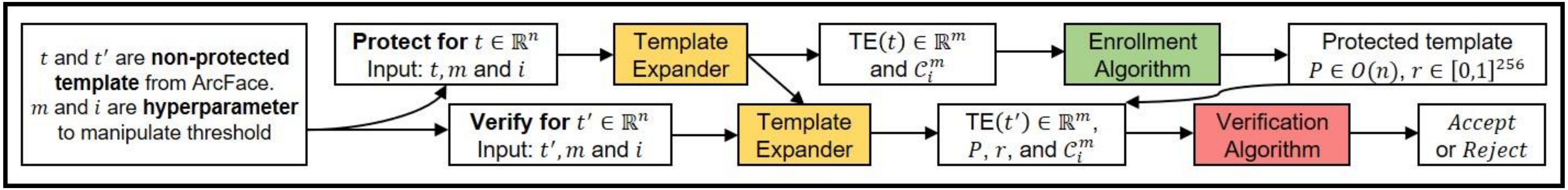
Deep Face Template Protection in the Wild

Abstract Construction

Pipeline of Ours

- Our main ingredient to go beyond IronMask is a combination of generalization of real-valued ECC and newly proposed template expander TE that takes template as an input and generates an expanded template in a secure way

- By expanding the dimension, we get more flexibility in choosing hyper-parameters to trade off between security and accuracy.



Linear Approach

Semi-orthogonal matrices

- We can consider semi-orthogonal matrices $W \in \mathbb{R}^{n \times m}$ as efficiently computable isometry between from $\mathbb{R}^m$ to $\mathbb{R}^n$ for $n \geq m$
- However, using a semi-orthogonal matrix cannot be security enhancing.
- In the face recognition system, there is no secret except the template the target of privacy protecting, and thus it is reasonable to assume conservatively that the attacker can easily access to the semi-orthogonal matrix W
- In paper, we show that W can be used to reduce the computational cost for breaking the irreversibility.

Non-linear Approach

Mazur-Ulam Theorem [10]

- $If\ V\ and\ W\ are\ normed\ spaces\ over\ \mathbb{R}\ and\ a\ mapping\ T: V \rightarrow W\ is\ a\ surjective\ isometry,\ then, T\ is\ affine, where\ an\ affine\ map\ is\ combination\ of\ a\ translation\ and\ a\ linear\ map.$

  Unfortunately, non-linear transformation cannot perfectly preserve the angle due to the Mazur-Ulam Theorem stated above.

Definition) Almost Isometry

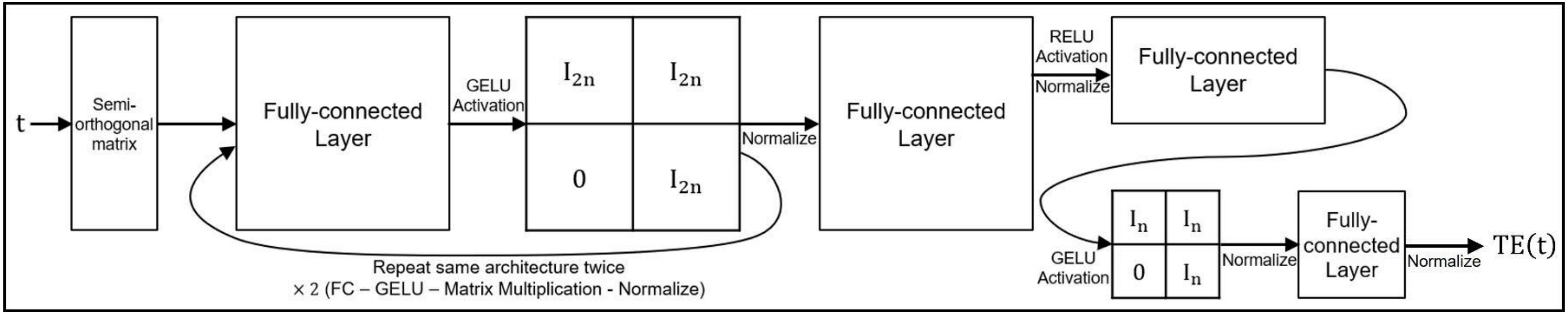
- $Given\ a\ positive\ real\ number\ \varepsilon, an\ \varepsilon-isometry\ or\ almost\ isometry\ is\ a\ map\ T: V \rightarrow W\ between\ metric\ spaces\ V\ and\ W\ such\ that\ for\ v, v' \in V\ on\ has\ |d_W(T(v), T(v') - d_V(v, v')| < \varepsilon,\ and\ for\ any\ point\ w \in W\ there\ exists\ a\ point\ v \in V\ with\ d_W\big(w, T(v)\big) < \varepsilon, where\ d_V\ and\ d_W\ are\ metrics\ of\ V\ and\ W, respectively.$

[10] Mazur, Stanisław, and Stanisław Ulam. "Sur les transformations isométriques d'espaces vectoriels normés." CR Acad. Sci. Paris 194, no. 946-948 (1932): 116.

Deep Face Template Protection in the Wild

Isometric Neural Network INN for Template Expander

- Maintaining the almost isometry
- Choosing suitable non-linear activations
- Reducing the use of learnable parameters as much as possible
- Increasing the depth of neural network



Deep Face Template Protection in the Wild

Performance Evaluation

- We use four popular datasets LFW, AgeDB-30, CFP-FP, and IJB-C which are widely used for the accuracy evaluation of face recognition system.
- These four sets are significantly more challenging compared to Multi-PIE, FEI, and Color FERET datasets that consists of face images acquired in a controlled environment.
- We experiment in various settings of hyper-parameters m and i of $\mathcal{C}_i^m$.

Type	Dataset	TAR@FAR
ArcFace	LFW	99.67@3e-4
		99.53@0
	AgeDB	97.00@7e-3
		95.13@0
	CFP-FP	98.11@3e-3
		96.49@0
	IJB-C	97.72@1e-3
		96.60@1e-4
		94.93@1e-5
		90.55@1e-6
		76.48@1e-7

Table 1. ArcFace

Type[3]	i	D(∠)[4]	A(∠)/M(∠)[4]	Sec[4]	Dataset	TAR@FAR
IM	16	20.36	42.15/55.28	115-bit	LFW	57.72@0
					AgeDB	4.58@0
					CFP-FP	5.50@0
					IJB-C	70.56@1e-7
GIM	18	19.19	40.97/53.10	127-bit	LFW	48.79@0
	17	19.75	41.50/54.16	121-bit		53.08@0
	15	21.04	42.62/56.57	109-bit		58.64@0
	14	22.62	43.17/57.17	103-bit		63.09@0
	13	23.56	43.62/58.36	97-bit		72.59@0
	12	24.62	44.15/58.68	91-bit		77.72@0
	11	25.84	44.62/60.84	84-bit		82.08@0

Table 2. IronMask and Generalized IronMask

Template	Mem.[11]	Sec.	Dataset	TAR@FAR
$\mathcal{C}_{14}^{1024}$	4.2MB +62.9MB	118-bit	LFW	82.33@0
			AgeDB	20.03@0
			CFP-FP	22.29@0
			IJB-C	81.61@3e-7
$\mathcal{C}_{12}^{2048}$	16.8MB +252MB	115-bit	LFW	97.47@0
			AgeDB	69.6@0
			CFP-FP	67.69@0
			IJB-C	92.10@4e-6
$\mathcal{C}_{10}^{4096}$	67.1MB +1.01GB	108-bit	LFW	99.53@0
			AgeDB	92.23@0
			CFP-FP	92.06@0
			IJB-C	96.05@9e-5
$\mathcal{C}_{10}^{8192}$	268MB +4.03GB	118-bit	LFW	99.63@0
			AgeDB	95.73@1e-3
			CFP-FP	96.91@3e-4
			IJB-C	97.40@8e-3

Table 5. Template Protection with Neural Network based Template Expander

Q&A

Thank you !