SoftmaxOut Transformation-Permutation Network for Facial Template Protection

Hakyoung Lee, Cheng Yaw Low and **Andrew Beng Jin Teoh**
Yonsei University, South Korea
{discone9410, chengyawlow, bjteoh}@yonsei.ac.kr

Multimedia Security Lab

Contributions

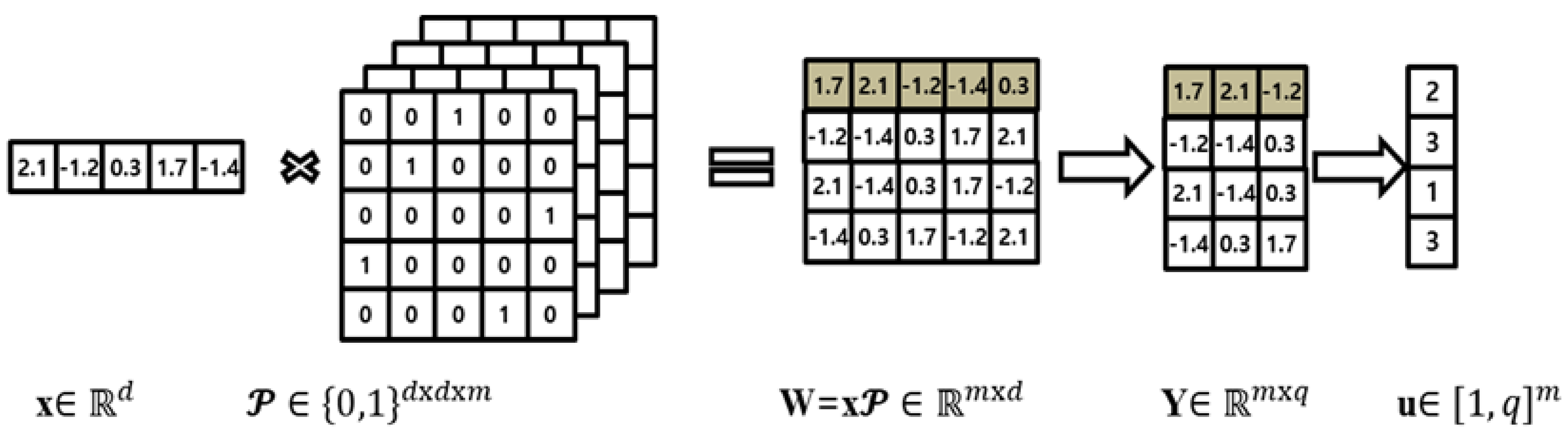
This paper is to propose a **cancellable biometric system** that uses supervised-learning algorithm.

1. Softmaxout Permutation-Transformation Network(SOTPN) inspired by RPM transformation [1]
2. Satisfy four design criteria of cancellable biometrics, i.e. noninvertible, renewability, unlinkability and accuracy performance
3. Pairwise arcface loss function which is inspired by the Arcface loss function [2] and code-balancing loss that triggers hash code to have high entropy.

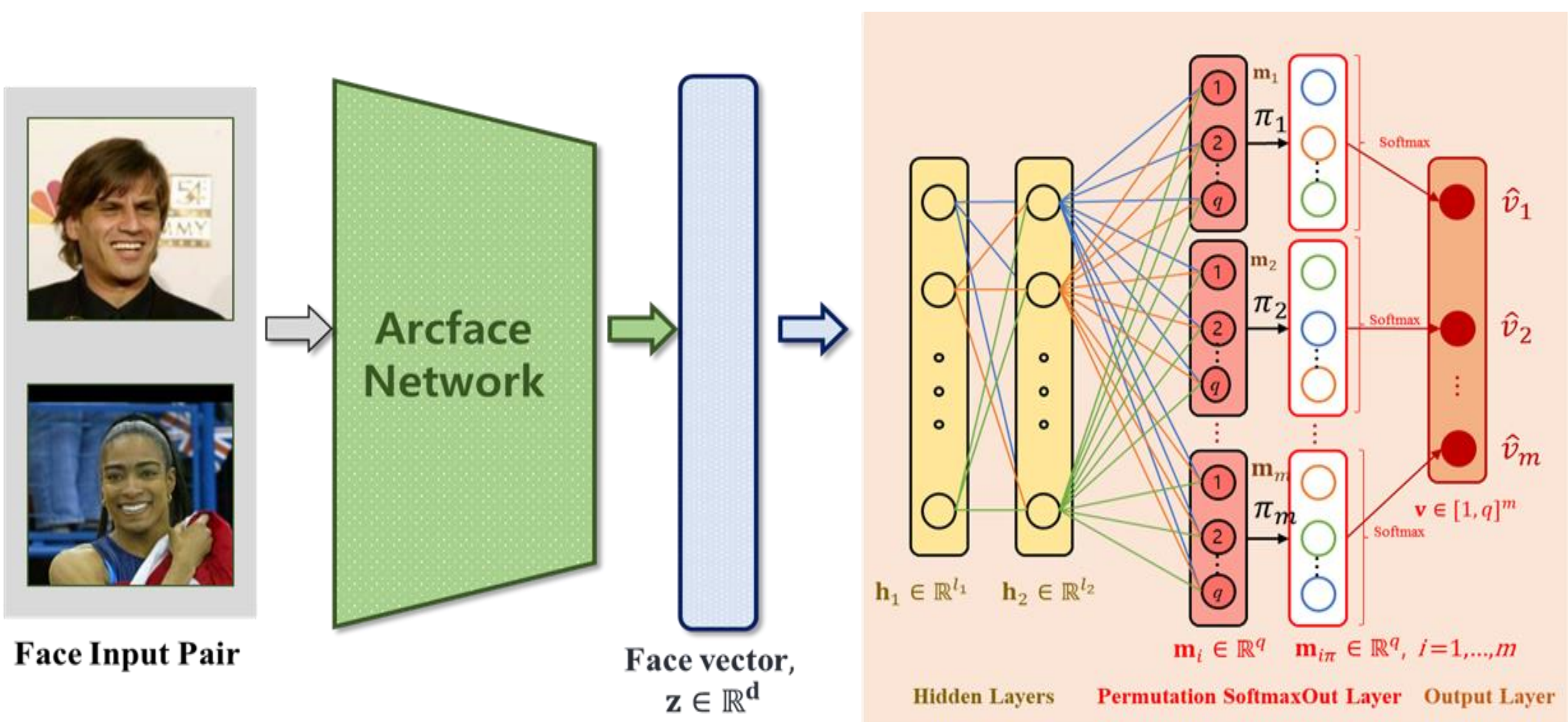
Methodology

Our proposed method builds on top of **Random Permutation Maxout (RPM) transformation** [1] to protect original biometric template **from being inverted**.

The progression of **RPM transformation** :



The progression of **our proposed method** :



SoftmaxOut Transformation-Permutation Network

Specially designed softmaxout layer approximates the winner-takes-all algorithm of the RPM transformation so that entire network is differentiable.

The proposed pairwise arcface loss function and code balancing loss is:

$$PA_{ij} = -\log\left[s_{ij}\left(\frac{e^{\gamma\cos(\theta+\alpha)}}{e^{\gamma\cos(\theta+\alpha)}+e^{\gamma\sin\theta}}\right)\right] - \log\left[(1-s_{ij})\left(\frac{e^{\gamma\sin(\theta+\alpha)}}{e^{\gamma\sin(\theta+\alpha)}+e^{\gamma\cos\theta}}\right)\right]$$

$$CB_{ij} = \sum_{b=1}^{B}\sum_{k=1}^{m}\left\{\,\left|\,\mathrm{mean}(v_i^{bk}) - \frac{q+1}{2}\,\right| + \left|\,\mathrm{mean}(v_j^{bk}) - \frac{q+1}{2}\,\right|\,\right\}$$

Datasets

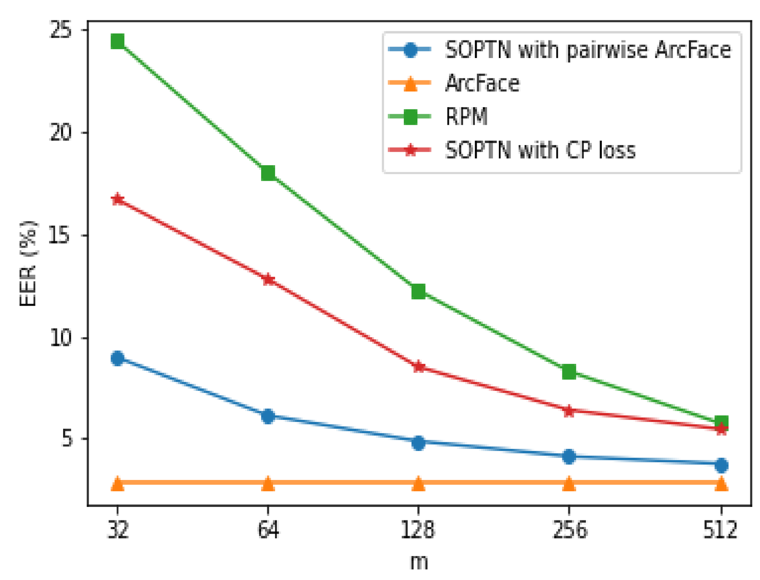
Our experiments are carried out under face datasets LFW, YTF and FS. Following the LFW standard evaluation protocol, we applied pre-determined 3,000 matched pairs and 3,000 non-matched pairs

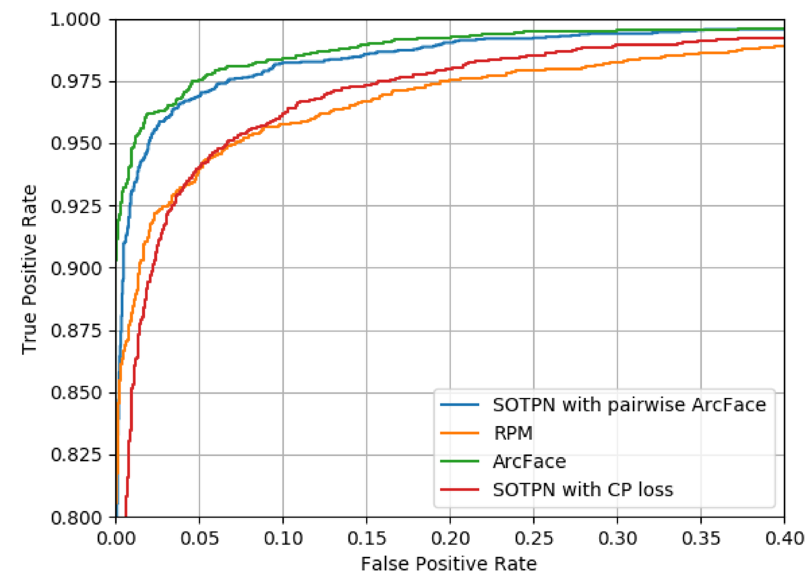
Experimental Results

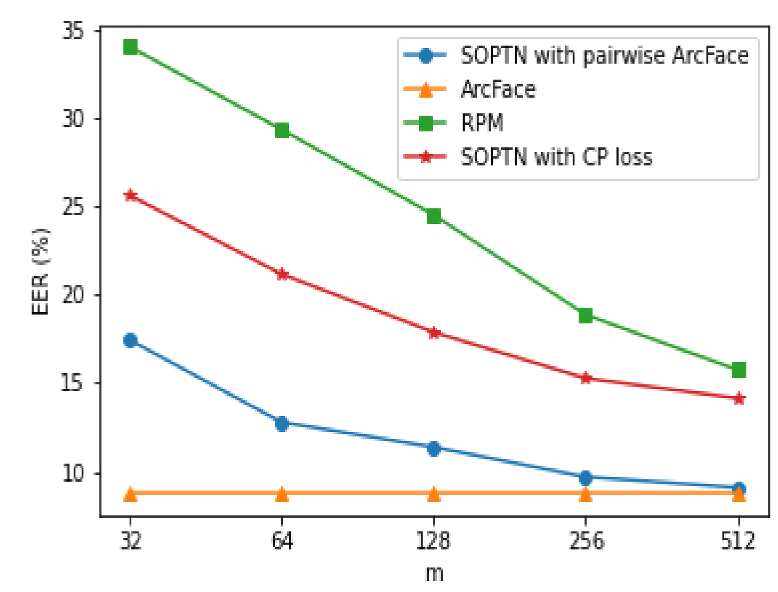
The EER of SOTPN with respect to different setting of m and q, where m is the length of the SOTPN hash code, and q is the maximum of code value.

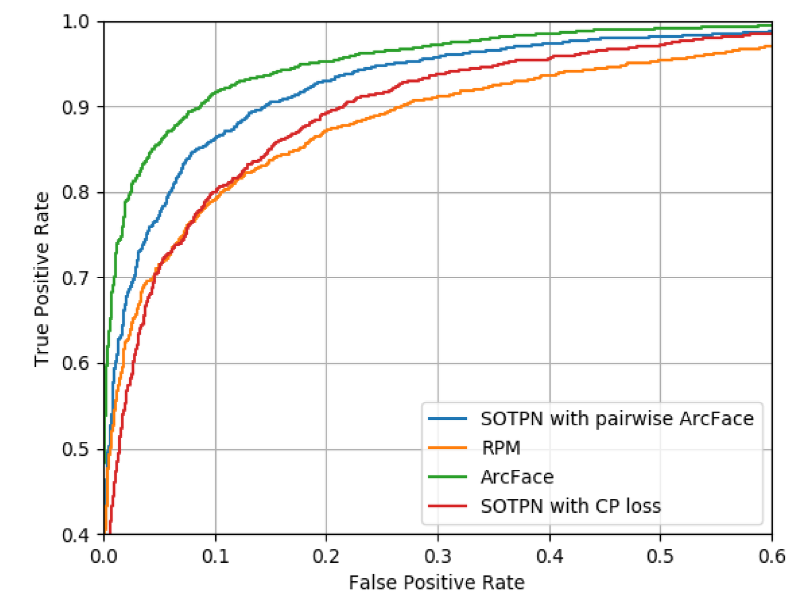
Training/Testing	m				
	32	64	128	256	512
FS/LFW	9.47	6.20	5.00	4.23	3.97
FS/YTF	17.44	12.80	11.40	9.72	9.12
LFW/FS	10.06	5.60	4.04	3.30	3.22

Training/Testing	q				
	8	16	32	64	128
FS/LFW	3.90	3.83	3.97	3.73	4.77
FS/YTF	11.60	11.76	9.12	9.86	9.50
LFW/FS	3.12	3.00	3.22	3.24	3.48









In the effect of the parameters, we demonstrate that the performance is better as the length of code m, however q depends on the datasets.

Analysis

1. Ablation study
   We verified the effectiveness of each component of the SOTPN by the ablation study.

SOTPN Configuration	EER (%)
PA loss with $\beta = 9$ + CB Loss	**3.53**
PA loss with $\beta = 9$, without CB loss	4.07
PA loss with $\beta = 1$ + CB loss	4.50
PA loss with $\beta = 1$, without CB loss	5.70

2. Renewability and Unlinkability
   Since we can permute the order of the neuron, we can renew the SOTPN hash code whenever we need.

References

[1] Teoh, Andrew Beng Jin, Sejung Cho, and Jihyeon Kim. "Random permutation Maxout transform for cancellable facial template protection." Multimedia Tools and Applications 77.21 (2018): 27733-27759.
[2] Deng, Jiankang, et al. "Arcface: Additive angular margin loss for deep face recognition." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2019.