Multibiometric Secure System Based on Deep Learning

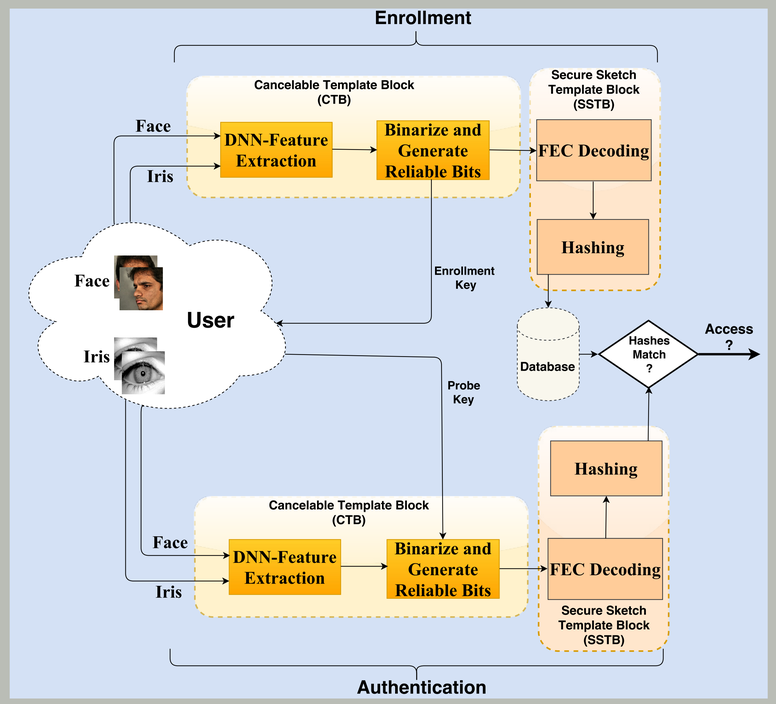
Veeru Talreja, Matthew C. Valenti, and Nasser M. Nasrabadi

Lane Department of Computer Science and Electrical Engineering, West Virginia University, U.S.A.

Motivation

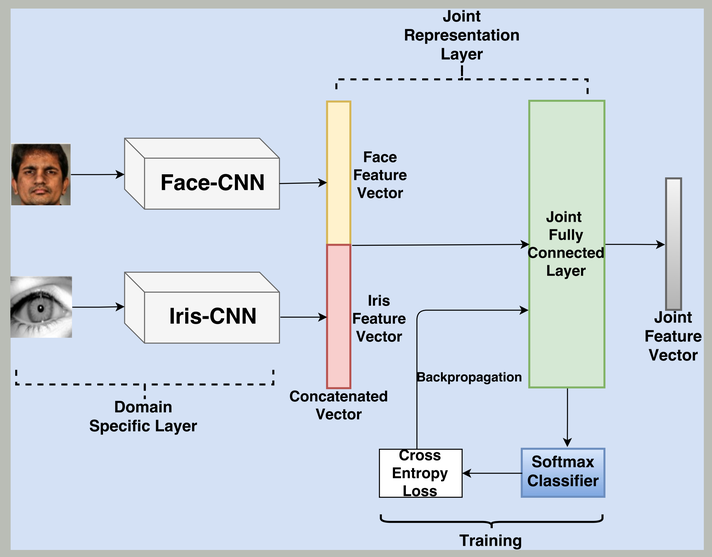
- Biometrics are being used for authentication in access control system.
- Biometric traits cannot be replaced or regenerated in case of identity theft or data-base compromise.
- Biometric systems obtain feature vector representing person's identity and
- These feature vectors (templates) cannot be secured using cryptographic hash due to intra-class variability in multiple acquisitions of biometrics.
- To counter this inta-user variability, we use forward error correcting (FEC) codes.
- As long as enrollment and probe feature vectors are within error correcting distance of the FEC code, authentication will succeed.
- Multibiometric systems offer improved accuracy, flexibility, coverage and better protection against spoofing compared to unimodal systems [1].

System Model



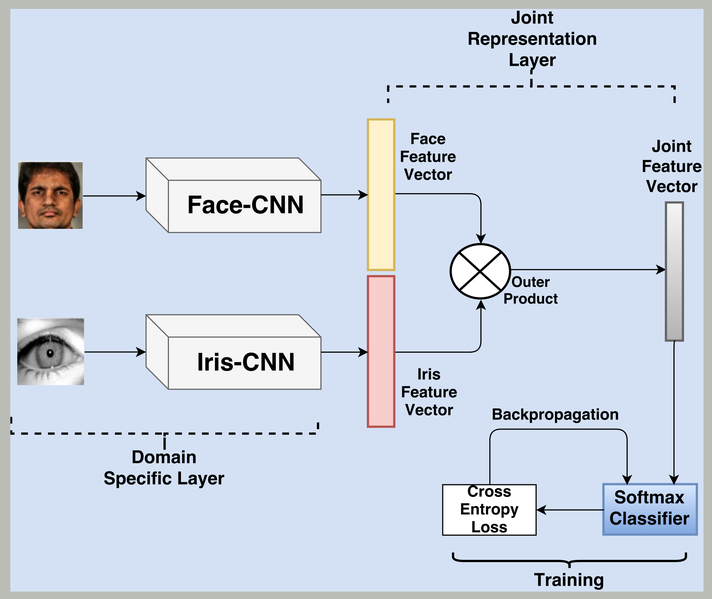
- Cancelable Template Block (CTB)
  - Uses deep neural network (DNN) for feature extraction.
  - DNN output is binarized and user-specific reliable bits are generated to form the cancelable template.
- Secure Sketch Template Block (SSTB)
  - The output of CTB is considered to be the noisy codeword of N symbols.
  - This noisy codeword is decoded with a forward error correction (FEC) decoder.
  - The output of the FEC decoder is the multibiometric secure sketch.

Deep Neural Network-Fully Connected Architecture (FCA)



- The outputs of the Face-CNN and Iris-CNN are concatenated vertically and passed through a fully connected layer.
- Size of face feature vector = 4096; Size of iris feature vector = 4096; Size of joint feature vector = 4096

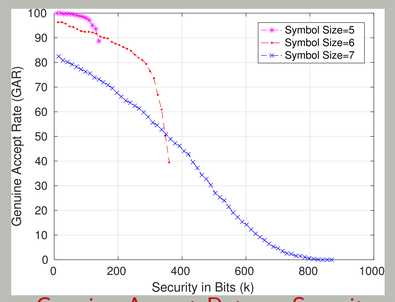
Deep Neural Network-Bilinear Architecture (BLA)

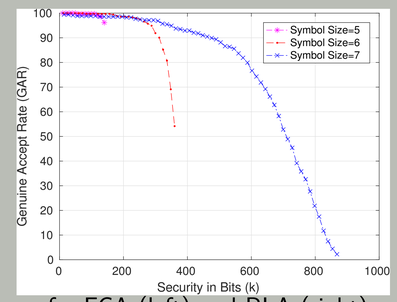


- The outputs of the Face-CNN and Iris-CNN are combined using the matrix outer product of the face and iris feature vectors.
- Size of face feature vector = 64; Size of iris feature vector = 64; Size of joint feature vector = 4096

Experiments and Numerical Results

- VGG-19 [2] used as a starting point for the Face and Iris CNNs in DNN.
- The DNN is fine-tuned on WVU multimodal database [3].
- Testing conducted on 50 disjoint subjects (not seen in training) from the WVU multimodal database.
- Reed-Solomon code used for FEC decoding and generating the secure sketch.





Genuine Accept Rate vs Security curve for FCA (left) and BLA (right).

Symbol Size (m)	n	Security (k)	k/n	GAR FCA	GAR BLA
5	155	53	0.34	99.65%	99.85%
		80	0.52	98.86%	99.7%
		100	0.65	98%	99.68%
6	378	53	0.14	94.55%	99.99%
		80	0.21	93%	99.75%
		100	0.26	92.5%	99.7%
7	889	53	0.06	79.5%	98.9%
		80	0.09	77.5%	98.9%
		100	0.11	76.2%	98.5%

Genuine Accept Rates of FCA and BLA for a security level of 53, 80 and 100 bits using different symbol size.

Benefits and Conclusions

- Feature extraction capability of convolutional neural networks utilized to generate a robust multibiometric shared representation.
- The system gives high matching performance in addition to high security.
- Error correcting capabilities of a Reed-Solomon code utilized to counter the intra-user variability of biometrics measurements.

References

[1] K. Nandakumar and A.K. Jain, "Multibiometric template security using fuzzy vault," *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Sept 2008.

[2] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[3] http://biic.wvu.edu/

mvalenti@wvu.edu