Fingerprint Verification with Siamese Networks

Cédric Vachaudez[2], Baiyu Chen[1], Luke Wang[1], Meysam Madadi[4], Isabelle Guyon[2, 3], Sergio Escalera[5], Bernhard Boser[1]

1. University of California Berkeley 2. UPSudy Paris-Saclay 3. ChaLearn 4. Computer Vision Center 5. University of Barcelona

Background

Biometrics play an increasingly important role in security to ensure privacy and identity verification. However, false negatives, in part due to poor image quality when fingers are wet or dirty, and false positives due to the ease of forgery are two prevailing issues. Optical sensors can be compromised with a simple fingerprint photo-copy. Capacitive sensors' performance decreases when common contaminants are present, e.g. water, lotion, condensation, etc. The recently developed **ultrasound fingerprint reader** [3] addresses the shortcomings of current technologies. **It permits reading both the epidermis (surface) layer and the dermis (below the surface) layer of the finger**, which makes it extremely hard to counterfeit a fingerprint. Furthermore, the technology is insensitive to humidity and dirt on fingers.

Siamese Network Structure

Our research uses "Siamese neural network" [2] to solve fingerprint verification. Proposed initially in the 1990's for signature verification [2] and concurrently applied to optical fingerprint verification [1], this network structure presents distinctive qualitative advantages and its performances can be boosted with appropriate pre-processing.

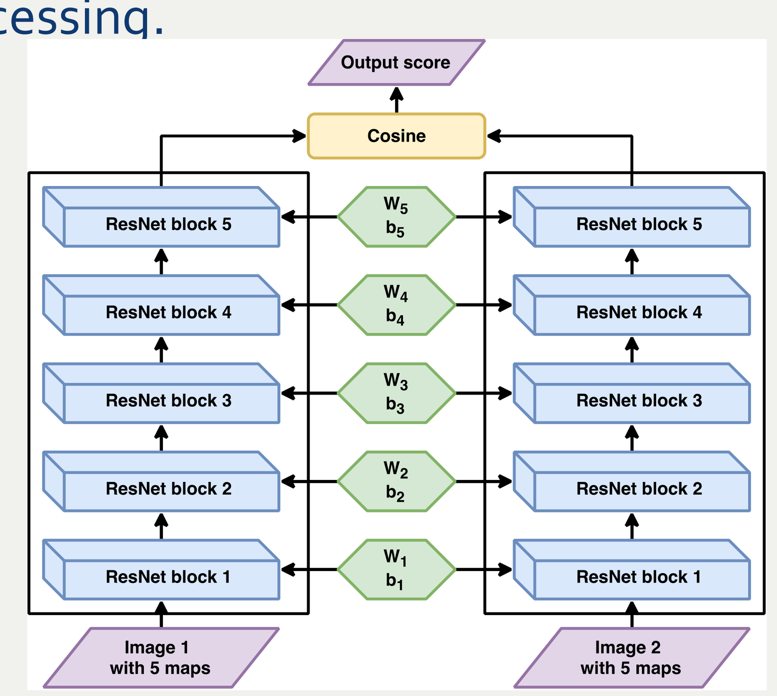

Figure 1. Structure of the Siamese Neural Network

Technical Details

Input images are preprocessed using standard signal processing steps:

(1) Delimitation of fingerprints and application of enhancement: median filter, contrast enhancement, and other noise reduction;

(2) Alignment of the two fingerprints (angle and position);

(3) Creation of local orientation, frequency, and variance maps.

The maps thus computed, shown in Figure 2, are provided to the network. Although the convolutional network is, in principle, capable of computing such maps, the preprocessing steps saves some training effort. **Two sides of the network are identical and have shared weights**. The similarity between the final outputs from each side is calculated using a **cosine similarity function**. To assess our new method, we have assembled a **large database of thousands of optical fingerprints from various public sources**. Using a model of the ultrasound sensor, we can transform the optical fingerprints to closely resemble the ultrasound images captured by the fingerprint sensor, of which we have sample images. With a subset of the available data we obtained promising preliminary results.

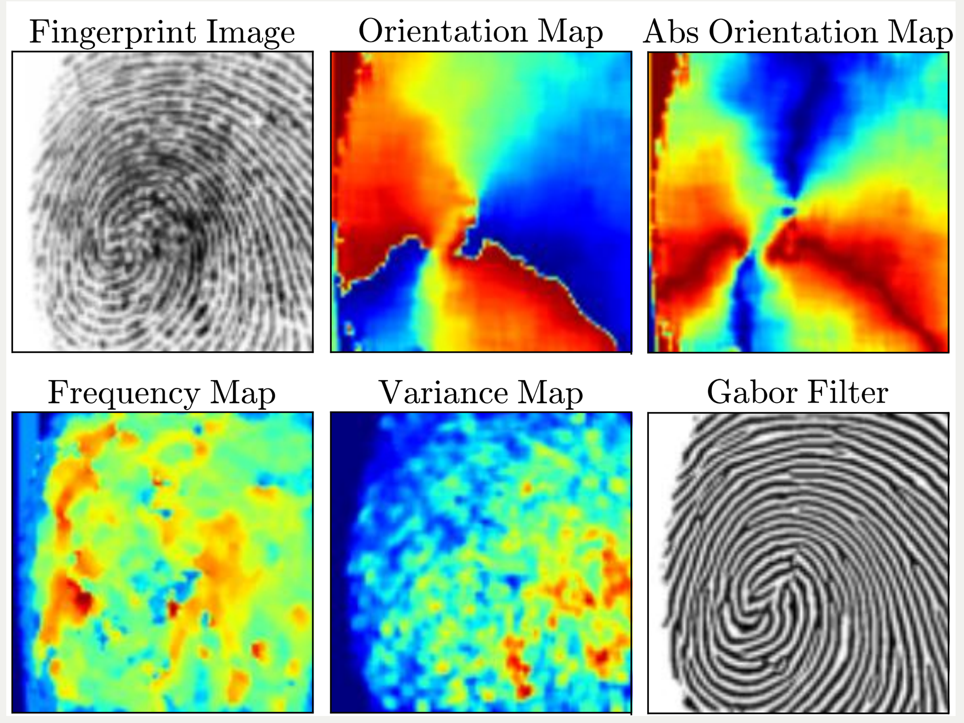

Figure 2. Raw Image and Preprocessing Output

Technical Details

Compared to the most prevalent fingerprint verification techniques, which are based on minutiae detection, the Siamese network is particularly adequate for the use case we are interested in. Methods based on feature maps, such as convolutional neural networks, are more **robust to occlusions**. This is one of the motivations towards using the (convolutional) Siamese networks. Furthermore, the genuine fingerprint templates may eventually be compromised. Therefore, **it is advisable not to store the fingerprints themselves, but a coded representation, which is offered by the upper layer internal representation of the network. It is relatively difficult to invert, and easy to replace if , which is very much like providing a new password if a password in compromised.**

Results and Discussion

The results of this Siamese network are shown through the progress of "Area Under the Curve" (AUC) of the Receiver operating characteristic (ROC). The neural network performs better than the preprocessed maps (although not very significantly yet). Further improvements could be gained by incorporating the preprocessing into the neural network architecture as convolutional trained layers and fine tuning the end-to-end system. In addition, the quality of the dataset we are presently using is not very high, and contains fingerprints often containing marks and smudges,. We are working towards obtaining a large amount of simulated fingerprints to perform massive training. Figure 3 shows the activation maps from different inner layers of the network of Figure 1, showing that it is able to perform some form of feature extraction.

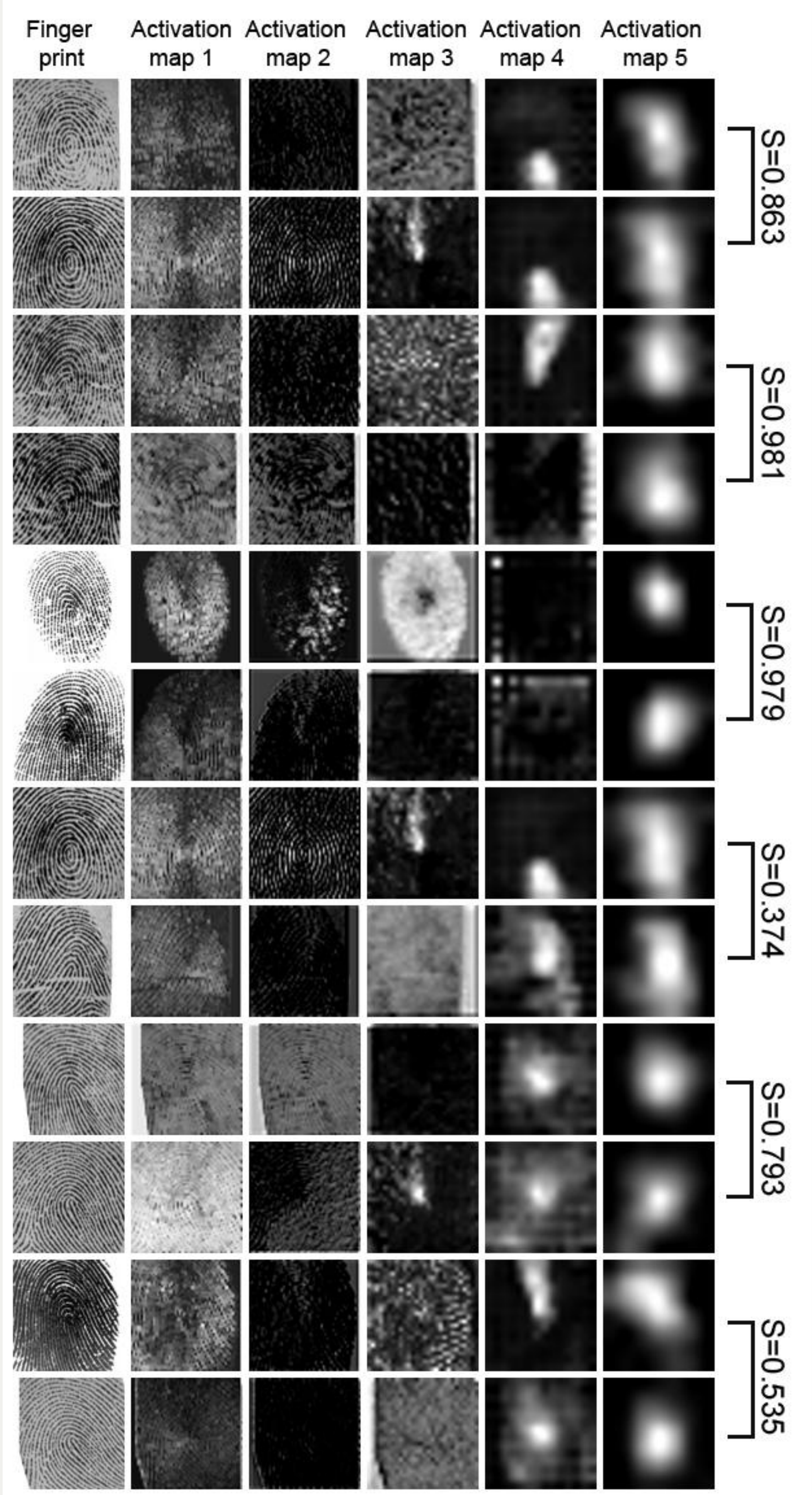

Figure 3. Activation Maps in the various layers of the network of Figure 1.

	Fingerprint	Orientation map	Abs orientation map	Frequently map	Variance map	Gabor Filter
AUC before NN	0.484	0.555	0.707	0.784	0.553	0.708
AUC after NN	0.834	0.754	0.789	0.792	0.636	0.824
Performance before NN	0.54	0.51	0.72	0.70	0.58	0.64
Performance after NN	0.79	0.69	0.70	0.70	0.62	0.75

Table 1. Performance comparisons for different prerocessings before and after passing data through the neural network. Cosine Is used as similarity function.

Contact:

Baiyu Chen

(510) 502 6352 | baiyu@berkeley.edu

M.S. Computer Science 2017, University of California, Berkeley

Reference:

[1] Pierre Baldi and Yves Chauvin, Neural Networks for Fingerprint Recognition. Neural Comp. 5(3), 1993.

[2] Jane Bromley et al, Signature Verification using a ``Siamese" Time Delay Neural Network. In NIPS 1994.

[3] Hao-Yen Tang et al, 11.2 3D ultrasonic fingerprint sensor-on-a-chip, in IEEE conf. ISSCC Proc. 2016.