Abstract

Biometrics has nowadays become the universal interest for the security application such as forensics and identification. Among the various biometrics information (e.g. fingerprint, face, palm, veins, iris, gait), "face" is the most popular one since face recognition only needs a camera which is available on most of the smart-phones. Due to the rapid development of face recognition technology (e.g. deep learning), face recognition has been applied to many applications, such as the "smile to pay" facial recognition system based on Alipay's mobile phone app.

Despite the success of face recognition system, it is vulnerable to spoofing attack (with a special medium). An attacker can easily bypass the face recognition system with printed photo/replay video of an authenticated user. Due to the security issue raised by face spoofing, face anti-spoofing has recently emerged as an active topic with great significance for both academia and industry. Recently, numerous face spoofing detection schemes have been proposed based on either hand-crafted features or deep learning features. However, these methods are limited in their scope that the face images (videos) for training and the images (videos) for testing are all collected from the similar condition, which constrains the application of such face spoofing detection methods since the environments of face capturing can be diverse in practice. In light of this, we aim to address the face anti-spoofing problem by improving the generalization capability to practical face capturing conditions in this thesis.

The reason which prevents the current methods from the practical application is due

to the large performance drop since the classifier obtained by training data can not be well generalized to testing data. It is indeed that we cannot collect face data from all possible conditions and environments. However, it is possible to collect a limited number of data based on a specific scenario (e.g. door controlled access). We expect to build a more robust face spoofing detection classifier by leveraging the limited number of face data we collected by ourselves and the large amount of face data which are publicly available. Based on this motivation, we aim to improve the generalization capability with only limited face data in an application-specific domain by leveraging data from a richer — and related — domain, seeking to learn meaningful features, through neural network distilling, to distinguish presentation attack samples from genuine ones in a setup with limited training data. In particular, we first train a deep neural network based on the sufficient labeled data set in an attempt to "teach" a neural network for the application-specific domain. Subsequently, we form training sample pairs, from the two domains, and formulate a novel optimization function, dedicated to capture spoofing-specific information and train a discriminative deep neural network on the application-specific domain.

It is also possible to conduct face anti-spoofing in an "off-line" fashion. More specifically, we first collected face data and conduct face spoofing detection by leveraging these "unlabeled" testing data after a period of time. Such motivation is practical based on applications such as face registration. In light of this, we introduce an unsupervised domain adaptation face anti-spoofing scheme to address the problem that learns the classifier for the target domain based on training samples in a different source domain. In particular, an embedding function is first imposed based on source and target domain data, which maps the data to a new space where the distribution similarity can be measured. Subsequently, the Maximum Mean Discrepancy between the latent features in source and target domains is minimized such that a more generalized classifier can be learned. State-of-the-art representations including both hand-crafted and deep neural

network learned features are further adopted into the framework to quest the capability of them in domain adaptation.

Finally, we aim to address the problem that no testing face data information is available during training the phase. This scenario is important for practical application where face spoofing detection is conducted in a "real-time" fashion. In particular, we propose a novel framework leveraging the advantages of the representational ability of deep learning and domain generalization for face spoofing detection. In particular, the generalized deep feature representation is achieved by taking both spatial and temporal information into consideration, and a novel network architecture tailored for the spatial-temporal input is proposed. The network is first initialized by training with augmented facial samples based on cross-entropy loss and further enhanced with a specifically designed generalization loss, which coherently serves as the regularization term to train the network in an end-to-end fashion. The training samples from different domains can seamlessly work together for learning the generalized feature representation by manipulating their feature distribution distances.

Author's Publications

1. **Haoliang Li**, Wen Li, Hong Cao, Shiqi Wang, Feiyue Huang and Alex C. Kot, "Unsupervised Domain Adaptation for Face Anti-Spoofing,", IEEE Transactions on Information Forensics and Security (in press).

2. **Haoliang Li**, Peisong He, Shiqi Wang, Anderson Rocha, Xinghao Jiang and Alex C. Kot, "Learning Generalized Feature Representation for Face Anti-spoofing,", IEEE Transactions on Information Forensics and Security (Accepted with Minor Revision).

3. **Haoliang Li**, Shiqi Wang, Peisong He, Anderson Rocha and Alex C. Kot, "Deep Neural Network Distilling for Face Spoofing Detection,", submitted to IEEE Transactions on Circuits and Systems for Video Technology.

4. **Haoliang Li**, Sinno J Pan, Shiqi Wang and Alex C. Kot, "Heterogeneous Domain Adaptation via Matrix Factorization in RKHS,", submitted to IEEE Transactions on Neural Network and Learning Systems.

5. **Haoliang Li**, Wen Li, Sinno J Pan and Alex C. Kot, "Discovering and Incorporating Latent Target-Domains for Domain Adaptation,", to be submitted to IEEE Transactions on Image Processing.

6. **Haoliang Li**, Sinno J Pan, Shiqi Wang and Alex C. Kot, "Domain Generalization with Adversarial Feature Learning,", in Proceeding of IEEE International Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

7. **Haoliang Li**, Shiqi Wang and Alex C. Kot, "Image Recapture Dection with Convolutional and Recurrent Neural Network", in Proceeding of Electronic Imaging, IS&T, 2017

8. **Haoliang Li**, Alex C. Kot and Leida Li, "Color Space Identification from Single Images", in Proceeding of IEEE Isnternational Symposium on Circuits and System (ISCAS), 2016

9. Leida Li, Dong Wu, Jinjian Wu, **Haoliang Li**, Weisi Lin, Alex C. Kot, "Image Sharpness Assessment by Sparse Representation". IEEE Transactions on Multimedia, vol.18, no.6, pp.1085 - 1097, June 2016

10. Leida Li, Yu Zhou, Jinjian Wu, Weisi Lin and **Haoliang Li**, "GridSAR: Grid Strength and Regularity for Robust Evaluation of Blocking Artifacts in JPEG Images," Elsevier Journal of Visual Communication and Image Representation, vol.30, pp.153-163, July 2015.

11. Khosro Bahrami, Alex ChiChung Kot, Leida Li and **Haoliang Li**, "Blurred Image Splicing Localization by Exposing Blur Type Inconsistency", IEEE Transactions on Information Forensics and Security, vol.10, no.5, pp.999–1009, April 2015