Chapter 1

Introductory Chapter: Machine Learning and Biometrics

Jucheng Yang, Yarui Chen, Chuanlei Zhang,
Dong Sun Park and Sook Yoon

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.79346

1. Introduction

We are entering the era of artificial intelligence and big data, and thus, systems are becoming more intelligent with performance even to a human level in limited applications. We also connect every part of the globe with ultrahigh-speed Internet to share information in almost real time, and innovatively make changes on the life style of people. At the core of artificial intelligence, machine learning algorithms contribute to semiautomatically or automatically develop highly intelligent systems by overcoming existing difficulties for various fields including applications on engineering, business, science, and pure art.

Biometrics are emerging as essential technologies for Internet-era intelligent systems to ensure both computer and network securities as well as security for stand-alone equipment. To achieve a very high-level performance and more intelligent as intended, recent machine learning algorithms with state-of-the-art architectures can be applied to those biometric systems. In the book, we introduce some representative biometrics, discuss major characteristics of samples from corresponding biometric, and also describe their effective features and descriptors. We also introduce the well-known supervised machine learning algorithms and deep learning in separate chapters along with their applications to biometric studies.

2. Biometrics

Biometrics has rapidly developed in recent years with its worldwide applications for daily life. Biometrics authentication or recognition is to identify individuals based on the biometrics characteristics using a variety of types of algorithms [1]. Biometrics can be broadly categorized

into two depending on their characteristics: physiological characteristics and behavioral characteristics. Biometrics with physiological characteristics contains direct physical evidence of discriminative features in their samples. This category includes biometrics such as face, fingerprints, palm veins, DNA, retina, iris, and ears. On the other hand, discriminative features from biometrics with behavioral characteristics can be indirectly extracted from samples, and this category includes biometrics such as typing rhythm, gait, and voice.

A biometric system for identification or recognition can be designed and implemented either feature-based using a handcrafted feature extraction or automatic feature generation-based using an end-to-end training based on a machine learning algorithm. For a feature-based biometric system, the selection of feature types and descriptors, and a following classifier design become very important to reduce the variability and the computational complexity of original characteristics. Each feature descriptor has its own strength for specific type of patterns. For example, the Gabor filter has better direction selectivity and frequency selectivity, so it can be used to apply time-frequency analysis for input images. Texture coding operators such as LBP and its variants are generally robust to changes from illumination and facial expression in images. Hence, it is critical to select right features according to the applications. Performance of a feature-based system mainly relies on capability of human experts, and it often results in low generalization for variations on input data. Recent automatic feature generation-based approaches such as deep learning can be an excellent alternative to deal with such difficulties. In this type of system, feature extraction/selection and classifier parts are trained together with large amount of data, and it generally shows better performance than a feature-based system. One disadvantage of this approach is that it usually consists of large number of parameters and takes a rather long time to train them.

Biometric systems for security require to have very high accuracy with favorably low computational complexity. In addition, a reliable biometric system should generalize well for unseen samples, and highly robust to various type of challenges including geometric transformation, illumination change, intraclass variation, and presence of noise. For a real-world security application, we need to construct a system endurable to various types of attacks such as counterfeiting. In order to make a system with higher security, multimodal biometrics [2] has attracted wide attentions in recent years and becomes a hot research topic. A multimodal system, for example, with input of finger vein and finger print images, has higher reliability, broader applicability, and stronger security and can provide a more reliable and stronger security in practical applications than unimodal one.

3. Machine learning

Machine learning is a procedure to learn from examples and, more specifically, it is a field of optimizing system parameters, which are defined on an architecture, to meet the evaluation criteria using a set of training examples. We often use statistical techniques to give computers the ability to "learn." Once the intended goal of learning is met, we may use the resulting

system to automatically predict the category of unseen data, to estimate location in the feature space, or to generate artificial examples depending on different applications. Machine learning algorithms are typically classified into three broad categories: supervised learning, unsupervised learning, and reinforcement learning.

For supervised learning problems, the training data comprises examples of the input vectors along with their corresponding target vectors. When the target vectors are categorical, the problems are known as classification or pattern recognition, and when the target vectors are real-valued, the problems are known as regression. Loss or distance functions are defined between the current output vector and the target vector for each input vector, and optimization is performed to minimize the loss over all training examples. By teaching the system with known input and target pairs, we expect to respond correctly even if unseen data are presented to the trained system.

For unsupervised learning problems, no targets are defined so that the training data consist of only a set of input vectors. The goal of unsupervised learning is to automatically discover "interesting statistical structure" in the data. It can also be explained as latent knowledge discovery from examples, and a variety of clustering algorithms are canonical examples of unsupervised learning.

Reinforcement learning [3] is to learn how to act or behave in a given situation for given reward or penalty signals. In this type of learning, a state for current status is defined and environment, usually a criterion function, evaluates the current state to generate a proper reward or penalty action through a set of policies. Instead of having exact target values, it learns with critics.

Deep learning [4] has been inspired from human brain and has been proving its powerful ability in detection, classification, segmentation, key point estimation, to activity classification. It generally consists of huge number of parameters with multiple nonlinear layers. Deep learning architectures include two popular categories: convolutional neural networks (CNN) for automatic feature extraction and recurrent neural networks (RNN) for sequence estimation. They have been applied to computer vision, speech recognition, natural language processing, audio recognition, social network filtering, machine translation, and bioinformatics with outstanding performances. In addition, generative models such as variational encoders and generative adversarial networks (GAN) are also becoming popular with their artificial sample generation capability.

4. Conclusion

A biometric system for security should be very reliable and accurate. Feature-based biometric systems can be designed and implemented with their relatively high accuracy and fast response. For more reliable and accurate systems, machine learning techniques can be applied to biometrics and their application areas. Especially, novel powerful algorithms, such as deep learning algorithms, can be excellent candidates for solving the challenging biometrics problems.

Acknowledgements

This paper is supported by the National Natural Science Foundation of China under Grant No. 61502338.

Author details

Jucheng Yang[1]*, Yarui Chen[1], Chuanlei Zhang[1], Dong Sun Park[1,2] and Sook Yoon[3]

*Address all correspondence to: jcyang@tust.edu.cn

1 Tianjin University of Science and Technology, Tianjin, China

2 Chonbuk National University, Jeonbuk, Republic of Korea

3 Mokpo National University, Jeonnam, Republic of Korea

References

[1] Brunelli R, Falavigna D. Person identification using multiple cues. IEEE Transactions on Pattern Analysis and Machine Intelligence. 1995;**17**(10):955-966

[2] Yang J, Sun W, Liu N, Chen Y, Wang Y, Han S. A novel multimodal biometrics recognition model based on stacked ELM and CCA methods. Symmetry. 2018;**10**(4):96

[3] Mnih V, Kavukcuoglu K, Silver D, et al. Human-level control through deep reinforcement learning. Nature. 2015;**518**(7540):529

[4] Hinton GE, Salakhutdinov RR. Reducing the dimensionality of data with neural networks. Science. 2006;**313**(5786):504-507