POZNAN UNIVERSITY OF TECHNOLOGY

Analysis of

Deep Learning in Biometrics: A Survey*

Sofya Aksenyuk, 150284
Uladzimir Ivashka, 150281
Oleksandr Yasinskyi, 150570

---

*Alberto Botana López, L 2019, *Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 8, no. 4

Keywords

Deep Learning
Biometrics
Fingerprint
Ocular recognition
Convolutional Neural Networks
Electrocardiogram

Purpose of the studies

The mobile phone and wearable device industries have been rapidly growing in recent years, as well as their importance. For example, mobile banking, health insurance, password management apps, etc., all of these services deal with highly sensitive information and hence require secure protection.

Nowadays, graph patterns or PIN codes for these services are simply insufficient, because of the development of the hacking tactics used to defeat these barriers.

Biometric approaches, such as fingerprint reading, ocular scanning, or facial recognition, are the most efficient for these purposes, but their effectiveness is limited.

This survey investigates how current technological achievements, such as deep learning, can assist improve the efficiency of established approaches and perhaps propose new ones.

Problems and their methodologies

1 - Twin Ocular Identification

Distinguishing twins has been proven to be one of the hardest issues in the field. Ocular biometrics is not limited to a single region, rather, it includes several sub-parts such as the iris, cornea, pupil, retina, lens, and some others, all of which may be used to extract discriminating information. The iris and its surrounding region will receive special attention in this study.

First, CNN-Siamese Framework was used. Its architecture is as follows: 8 weighted layers, each consisting of 5 convolutional and 1 pooling layer, and 3 fully connected layers in the end.

The second option was MCNN-Siamese Framework. It is CNN with modified architecture. The multi-scale convolution layer is applied, a single convolution layer and downsampling in the end. At the output of the MCNN, padding has been applied so that it has the same shape as the input.

2 - Fingerprint spoofing

Fingerprints are the most popular biometrics key today. People confirm mobile payments and log in wherever possible with it. Fingerprint authentication has proven to be relatively good compared with its main competitors. However, fingerprint authentication is not perfect and thus is an object of spoofing attacks. In this section, a method is proposed to detect fake fingerprints by performing histogram equalization on input images.

The modified framework of CNN was used to predict whether the input image is faked. Compared to previous models, the new one has lower training parameters, but a higher recognition rate.

3 - ECG user recognition

The main advantage of wearable devices is that they constantly collect various information, that can be used. While fingerprints or ocular biometrics can be spoofed, the user's beating pulse is much safer. In this section, an ECG signal was used.

CNNs are mainly used for two-dimensional data like images, but recent studies are conducted on the analysis of 1-D time series using this kind of network. Three separate CNNs (ConvNet-1, ConvNet-2, and ConvNet- 3) were tested. ConvNet-1 and ConvNet- 2 has the same structure of 3 convolution layers, each with a max-pooling layer, and 3fully connected layers, they differ in learning rate. ConvNet-3 is smaller than the first two having only 2 convolution layers.

Findings

1 - Twin Ocular Identification

Results of the twin ocular identification problem examination using Siamese CNNs and Siamese Multi-layer CNNs against the CASIA-Iris-Twins database showed that the best results were performed by NASNet-Large-Siamese framework with an accuracy of 96.40%. However, it is important to mention, that average accuracy results give 92.93%. It gives us a standard deviation of 2.16%, meaning that the accuracies from all the examined frameworks are set around the mean.

Summing up, both frameworks yield results of approximately same accuracy.

2 - Fingerprint spoofing

The model's results, which obtained remarkably high accuracy, were validated using 10-fold cross-validation after being tested against well-known fingerprint benchmarks.

The tests were conducted to find the threshold of a given dataset, which will be used to identify a certain fingerprint between genuine and forged. Such a threshold is needed for the system to withstand spoofing attacks.

The proposed framework shows an accuracy higher that 99% for all of the benchmarks, leading to the conclusion that it can be qualified as robust, allowing it to be used to secure fingerprint-based devices.

3 - ECG user recognition

The ECG user recognition problem was tested on dataset comprised of 18 people: 5 male and 13 female, whose ECG were classified in 12 different types of signals depending on the location of the sensors.

Results are showing that the ensemble network shows an improvement of a 0.8% in accuracy towards the single network for fiducial ECG signals.

When it comes to non-fiducial signals, a minimum performance improvement of 0.4% and maximum of 1% within a period of 1 second is detected, and a maximum of 1.3% for a n-second period.

Meaning that despite of its type of signals which is unique to each individual and significantly harder to fake in general, the newly proposed ECG user recognition method is still capable of utilizing the ECG to recognize different users.

Analysis of the innovativeness of developed solutions

Nowadays digital security is of the utmost significance.

No one is fully protected from personal devices hacking, where we store our most valuable information. Biometrics is one of the ways to prevent it from happening.

However, as it was stated in the *Purpose of the studies* section, the effectiveness of biometric identification is insufficient to provide high security - there is always a chance of malicious attacks, etc.

Due to the absence of technological resources, such as availability of Machine Learning and Deep Neural Network training dataset limitation or computational power limitation, the progress in the field of biometrics had stopped for quite some time.

Fortunately, these issues are resolved by now, and therefore, it is possible to focus on gaps in biometrics particularly.

This is exactly what is done in the survey of Alberto Botana López.

The proposed Deep Learning methods has shown excellent results in enhance the protection of biometrics - something everyone uses to some extent nowadays.

The developed solution concerns three most common ways of identification, that take place in everyday life basis of every one of us - directly or not.

The author has improved the performance of something already existing and widely used, concentrating on one of the main needs of human-beings - security and protection.

Everything said above is sufficient enough to state that the discussed development is indeed innovative and has a constant need of enlarging its capabilities.

Personal findings

The researches on tackling ocular identification of twins may become revolutional, since modern commercial technologies of iris recognition have outweighing flaws.

Fingerprint biometrics today is a well-known technology and with the help of Deep Learning (DL), the identification is done via analysis, not measuring. It can be implemented much cheaper and, most importantly, in extraordinary ways as the bleeding-edge sensors are not needed.

Last but not least, ECG user recognition is, as mentioned, a brand new approach to digital biometrics and DL with contemporary signal-processing techniques is exactly what makes it possible.