Pattern Recognition Letters 77 (2016) 58–65

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

# Deep belief network based statistical feature learning for fingerprint liveness detection[☆]

Soowoong Kim[a], Bogun Park[b], Bong Seop Song[b], Seungjoon Yang[a,*]

[a] School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology, Ulsan 689-798, Republic of Korea
[b] Suprema Inc., 16F Parkview Office Tower of Jeongja-dong, Bundang-gu Seongnam, Gyeonggi 463-863, Republic of Korea

ARTICLE INFO

*Article history:*
Received 14 July 2015
Available online 8 April 2016

*MSC:*
41A05
41A10
65D05
65D17

*Keywords:*
Fingerprint liveness detection
Fingerprint anti-spoofing
Deep belief network
Deep learning
Statistical feature extraction
Livdet2013

ABSTRACT

Fingerprint recognition systems are vulnerable to impersonation by fake or spoof fingerprints. Fingerprint liveness detection is a step to ensure whether a scanned fingerprint is live or fake prior to a recognition step. This paper presents a fingerprint liveness detection method based on a deep belief network (DBN). A DBN with multiple layers of restricted Boltzmann machine is used to learn features from a set of live and fake fingerprints and also to detect the liveness. The proposed method is a systematic application of a deep learning technique, and does not require specific domain expertise regarding fake fingerprints or recognition systems. The proposed method provides accurate detection of the liveness with various sensor datasets collected for the international fingerprint liveness detection competition.

## 1. Introduction

Fingerprint recognition is one of the biometric authentication methods that has been widely used in forensic, civilian, and commercial applications [17]. Fingerprint recognition systems usually consist of relatively inexpensive components, and yet can provide highly accurate authentication [4]. However, fingerprint recognition systems are vulnerable to impersonation by fake, or spoof, fingerprints. Fake fingerprints can be made of materials such as silicon or play-doh under cooperative or non-cooperative scenarios using various methods [18]. Countermeasures to prevent false authentication by detecting the liveness of fingerprints are being developed [8]. Methods to detect the liveness of fingerprints can be divided into hardware-based and software-based methods.

Hardware-based systems utilize auxiliary hardware components such as oxygen saturation sensors [24], multispectral imaging systems [22], or optical coherence tomography scanning systems [27] to detect features that separate live fingers from fake fingers. The addition of hardware components usually increases costs of otherwise inexpensive recognition systems significantly. Hardware-based systems that employ additional modality are found to be venerable to false authentication scenarios in which a fake fingerprint is used for the fingerprint sensor and a live finger is used for the other modality [1].

Software-based methods utilize dynamic or static features that are available using existing hardware. Dynamic features such as changes of skin elasticity [13] or perspiration pattern [23] during the fingerprint scanning process can be observed to detect the liveness of a given fingerprint. The use of dynamic features has a disadvantage that detection time is increased to extract features that change over time. Static features that separate live fingerprints from fake fingerprints can be observed from a single impression of a fingerprint to detect the liveness. For example, active sweat pores can be detected by a high pass filtering to detect live fingerprints [19]. One can utilizes the fact that materials used to fabricate artificial fingerprints have different textural details and hence different high frequency spectrum components [21]. Features that do not change during the fabrication of fake fingerprints can also be used for liveness detection [7,9]. The performance of static feature based liveness detection methods depend heavily on the choice of features selected in a hand-designed manner according to domain knowledge and experience.

Recently, it has become more common to attempt to learn features through supervised or unsupervised learning [2]. Features

[☆] This paper has been recommended for acceptance by Ajay Kumar.
[*] Corresponding author. Tel.: +82 52 217 2110; fax: +82 52 217 2299.
*E-mail address:* syang@unist.ac.kr (S. Yang).

http://dx.doi.org/10.1016/j.patrec.2016.03.015
0167-8655/© 2016 Elsevier B.V. All rights reserved.

automatically derived via machine learning have advantages of not requiring specific domain expertise and potentially yielding a much larger set of features for a classifier. There have been researches on learning features for fingerprint liveness detection. In [6], the independent component analysis (ICA) is used to automatically learn a set of filters that extract textural features to be used in classification by a support vector machine (SVM). The filters obtained via ICA are learned using a set of natural images not by a set of fingerprint images. Examples of learned filters are mostly edge detectors at various angles and phases, and are not specifically trained for fingerprint applications. In [5], a convolutional network (CN) is used to extract features, whose dimension is reduced by the principal component analysis (PCA), to be used by a SVM for fingerprint liveness detection. The weights of the CNN are set to random values without any learning process. Even though the CN can work with random weights, the CN is not specifically trained for fingerprint applications. The learned principal components are eigen images that are suitable for applications that require energy compaction.

This paper presents a fingerprint liveness detection method based on a deep belief network (DBN). DBN is a deep learning architecture that has been used in various applications such as character recognition [26], speech recognition [20], facial expression recognition [16], music information retrieval [10], and so forth. DBN has been also used in fingerprint applications for enhancement of scanned fingerprint images [25]. The generative properties of DBN allow better understanding of the performance, and provide a simpler solution for the classification tasks [12]. We use a DBN to learn features from a set of live and fake fingerprints and also to determine the liveness of fingerprints. The restricted Boltzmann machine (RBM) [12] is used at each layer of the DBN. The RBMs are trained sequentially from the first layer to the second to last layer by unsupervised learning with layer-wise greedy algorithm. Then the DBN, including the last layer, is trained by supervised learning with back propagation with a labeled set of live and fake fingerprints. The DBN output is the posterior probability that a patch taken from a given fingerprint belongs to a live or fake fingerprint. A hypothesis test is set up with outputs of the DBN with multiple patches taken from a given fingerprint as inputs to determine the liveness.

The proposed method is a systematical application of deep learning to the problem of fingerprint liveness detection. Liveness detection as well as learning of features appropriate for the liveness detection is performed within an established framework of deep learning without relying on specific domain expertise. In particular, the proposed method is trained for multiple datasets without any information about the sensors, images, or pre-processing steps. Different features are learned for each dataset to be used in the liveness detection with a particular fingerprint recognition system.

The proposed fingerprint liveness detection method is evaluated with datasets collected using four different optical sensors for the international fingerprint liveness detection competition (LivDet2013) [8]. The liveness detection results show that the proposed method can provide high performance in terms of the false rejection rate (FRR) and the false acceptance rate (FAR). With the DBN topology being simple, the computational complexity of the detection method is relatively low. The proposed method provides efficient and effective software based fingerprint liveness detection.

This paper is organized as follow. Section 2.1 explains a preprocessing step to prepare patches of inputs from a scanned fingerprint image. Section 2.2 presents the topology and modeling of the proposed DBN. Section 2.3 provides a training method including pre-training with unsupervised learning and fine-tuning with supervised learning. Section 2.4 provides a hypothesis testing with outputs of the DBN with multiple inputs from a given fingerprint. Experimental results and discussions are given in Section 3. Section 4 concludes the paper.

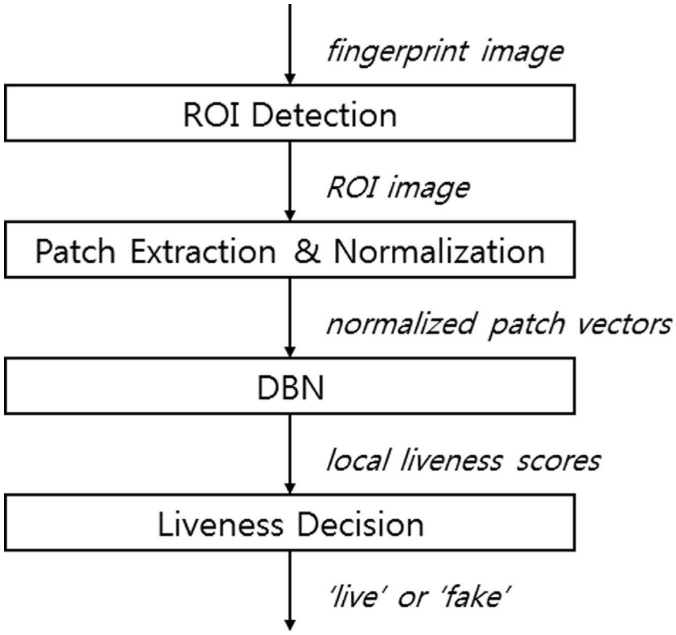

**Fig. 1.** Flowchart of the proposed fingerprint liveness detection process.

## 2. Proposed fingerprint liveness detection algorithm

The proposed fingerprint liveness detection system consists of the following steps. From a query fingerprint image, region of interest (ROI) is detected. Small size patches from the ROI image are extracted, normalized, and reshaped as vectors. The outputs of the DBN with the patches as inputs are collected and fed into a liveness detection routine. A flowchart of the proposed fingerprint liveness detection system is shown in Fig. 1. The following sections describe detail operations.

### *2.1. ROI detection and input patch Ppeparation*

A query image composed of a fingerprint on scanner platen background is captured by a fingerprint sensor. The fingerprint image is not always at the center of a captured image. The ROI that contains only the fingerprint image is extracted from a captured image. Salient points of the fingerprint image are detected using the two dimensional Harris corner detector. The average location of the detected salient points is calculated. Region inside a rectangle of a fixed size centered at the average location is used as an ROI. Fig. 2 shows an example of the detected ROI. The blue points indicate the locations of salient points detected by the Harris corner detector. The red point is the average location of the salient points. The image inside the red rectangle is the ROI of the captured image.

Patches of the size $H_p \times W_p$ are extracted from the image inside the ROI. Patches are allowed to overlap the other patches by $t$ pixels. Pixels in each patch are reshaped as a vector to form a vector $\mathbf{p}$ of the size $M \times 1$, where $M = H_p \times W_p$. The vectors are normalized to have zero mean and unit variance.

### *2.2. DBN*

A DBN is used for the fingerprint liveness detection. Fig. 3 shows a schematic of the DBN for the proposed liveness detection. There are $K$ layers of RBMs superimposed such that the visible unit