Fingerprint Liveness Detection using MobileNet-SVM combination

Abderrahmane Herbadji
Department of Electronics
University of Setif
Setif 19000, Algeria
herbadjiabder@gmail.com

Noubeil Guermat
Department of Electronics
Faculty of Technology
University of Msila
M'sila 28000, Algeria

Djamel Herbadji
Department of Electronics
University of Skikda
Skikda 21000, Algeria

Hichem Kahia
LMSE laboratory
University of Biskra
Biskra 7000, BP145, Biskra, Algeria

***Abstract*—Fingerprint is a crucial biometric trait thanks straightforwardness to its unique characteristics, high reliability, and low cost. This has led to a widespread use in border control applications as well as personal identification systems. Meanwhile, fingerprint recognition systems have shown some vulnerabilities related to security issues such as spoof presentation attacks. In order to protect these systems, fingerprint liveness detection has been regarded as a primary countermeasure for protecting the fingerprint recognition systems from spoof presentation attacks. Towards this aim, in this paper we propose a machine learning method to distinguish live fingerprints. In this study, we use Convolutional Neural Networks (CNN) for fingerprint liveness detection. More specifically, the proposed method combines Mobilenet for features extraction and SVM for fingerprint images classification. Experimental results on a publicly available dataset (i.e., LivDet 2023 dataset) show that the proposed framework for fingerprint liveness detection purpose achieve promising results. Most importantly, our cross-sensor evaluation depicts that MobileNet-SVM approach showed very promising generalization capabilities, where an ACER equals to 1.67% was obtained.**

***Index Terms*—Fingerprint liveness detection, MobileNet, SVM, Deep learning, Artificial Intelligence**

I. Introduction

In order to identify individuals in a reliable and fast manner, biometrics authentication is regarded as more reliable than traditional tokens and passwords, and is widely used in many areas, such as public security finance, military, as well as in daily life [1]–[3]. Although biometrics brought considerable convenience to our lives, it is easily threatened by some human factors (e.g. spoofing attacks).

Fingerprint authentication has been the prominent biometric to verify users' identity according to their fingerprints' characteristics. However, these biometrics systems suffer from numerous security and privacy troubles, for instance, artificial fingerprints could be used to trick the fingerprint recognition system and access privacy information. To overcome these problems, a fingerprint liveness detection (FLD) or fingerprint presentation attack detection algorithm should be designed to prevent direct attacks to the scanner, by discriminating live fingers images from fake ones. There are two types of FLD, software-based (e.g. image quality based, perspiration based, and skin deformation based) and hardware-based (e.g. skin distortion, blood pressure, and visual based).

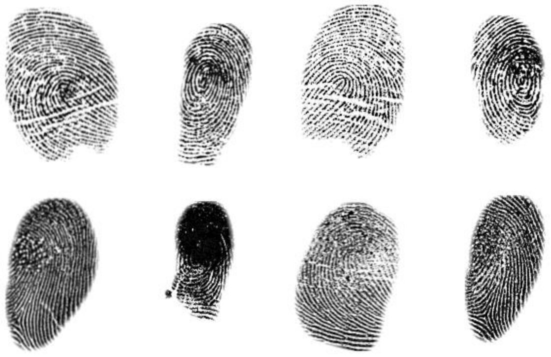

Fig. 1 *Fingerprint images of LivDet 2023 database: top row (live samples), bottom row (fake samples). These samples are collected using Dermalog sensor.*

Research on fingerprint livness detection has mainly been focusing on feature extraction algorithms [4], [5]. Therefore, to extract different features of given fingerprint images, various feature extraction techniques based on hand-crafted [6]–[8] and deep learning [9]–[11] methods have been proposed.

While previously proposed algorithms have shown promising results on individual datasets, the generalization capabilities of these algorithms were questionable [5]. One of the potential solutions to vanquish these drawbacks is formulating a new model that should be computationally inexpensive and has high generalization capabilities for discriminating live fingerprints from fake ones. Figure 1 shows an example of live and fake fingerprint imagers from LivDet2023 database.

Towards this aim, in this study, we present a software based algorithm for fingerprint liveness detection. Here, a machine learning based framework has been proposed through the use of a pre-treained neural network called MobileNet [12] in combination with a shallow classifier (SVM).MobileNet provides advantages like smaller model size and smaller complexity. In addition, it is able to perform better than other pre-trained models such as VGG16, ResNet50, GoogleNet, etc. We have tested our method on a publicly available database (i.e. LivDet

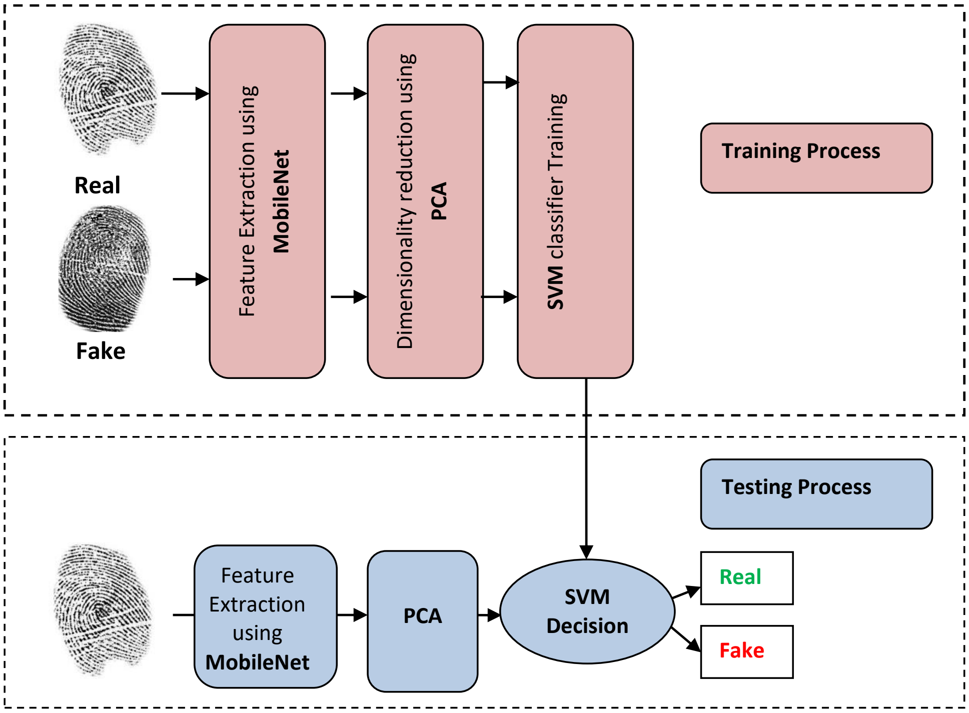
Real
Fake
Feature Extraction using MobileNet
Dimensionality reduction using PCA
SVM classifier Training
Training Process
Testing Process
Feature Extraction using MobileNet
PCA
SVM Decision
Real
Fake

Fig. 2 *Proposed framework for fingerprint liveness detection using MobileNet and SVM classifier*

2023) and shown that the proposed approach is able to achieve a high liveness detection accuracy.

We organise the remainder of this study as follows. Experimental analysis of the proposed model for fingerprint livness detection is given in Section II. Performance metrics and classification results are discussed in section III. Finally, conclusions are drawn in SectionIV.

II. EXPERIMENTAL ANALYSIS

In this section, we first describe briefly the used dataset and the setup that has been used in our experiments. Then, an analysis of the MobileNet-SVM based approach is provided.

A. Experimental Setup

To evaluate the effectiveness of our proposed liveness detection technique, we considered the LivDet 2023 database. The LivDet 2023 database contains images of real and fake fingerprints. The real fingerprints have been collected from 25 genuine subjects, where the fake fingerprints were made from high quality records of genuine fingerprints. This dataset consists of real fingerprint images and fake ones collected using four different scanners which are GreenBit, Dermalog, and two other scanners. The images are in the size of 500x500. It should be noted that we have used only images collected via Greenbit and dermalog scanners. Table I tabulates different characteristics of each scanner.

TABLE I *Detailed information about the fingerprint scanners used in LivDet 2023*

Scanner	Type	Model	Resolution (dpi)
Dermalog	Optical	LF10	500
GreenBit	Optical	DactyScan84c	500
Scanner 1	Optical		500
Scanner 2	Hybrid		500

B. MobileNet based Features extractor and PCA dimension reduction

Features extraction is an essential step in any liveness detection application, since higher liveness detection directly depends on the feature extraction method. To this end, in this study we consider an efficient pre-trained DNN for features extraction called MobileNet. It is worth noting that this DNN was trained on a huge database (i.e. ImageNet) that contains about 1.2 million images for 1000 object classes. Since features extracted from different layers of the same artificial network could achieve different classification performances, we have performed itemized search on MobileNet' layers to determine the layer that lead better to attain better accuracy. The extracted deep features are of high dimensionality, this makes training the classifier computationally very expensive, and thereby, the PCA technique is used for dimensionality reduction purposes.

TABLE II *Liveness Detection performance using MobileNet-SVM method. Bold values indicate best performances.*

Database		SVM-linear			SVM-RBF			SVM-poly(2)			SVM-RBF
Training	*Testing*	APCER(%)	BPCER(%)	ACER(%)	APCER(%)	BPCER(%)	ACER(%)	APCER(%)	BPCER(%)	ACER(%)	ACC(%)
Dermalog	Dermalog	2.5	9.8	6.15	1.16	6.4	3.78	1.5	8.0	4.75	96.45
GreenBit	GreenBit	0.66	6.0	3.33	0.33	4.6	2.46	1.16	4.8	2.98	97.42

PCA is a standard dimensionality reduction technique and has been widely applied in various computer vision challenges like face recognition, signal processing and so on. PCA can extract only the most important features that can describe the original information, thus reducing the dimensionality of the feature vector. Implementing PCA algorithms is nothing new, but the advantages of PCA are that it reduces the amount of computing and storing information.

Once the rich features have been extracted from the fingerprint images, PCA is used to reduce the dimensionality of the feature vector. Then, the new feature vectors are fed into the Support Vector Machine (SVM) classifier for training. The general schematic diagram for fingerprint liveness detection is shown in Figure 2

III. Performance metrics and classification results

The metrics we used in this paper for evaluating the performance of presentation attack detection are attack presentation classification error rate (APCER), bona fide presentation classification error rate (BPCER), and average classification error rate (ACER) which are considered as a standard metric for evaluating the LivDet competitions. ACER is defined as1:

$$ACER = (APCER + BPCER)/2 \tag{1}$$

Where APCER is proportion of attack presentations using the same presentation attack instrument (PAI) species incorrectly classified as bona fide, and BPCER is the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario.

In this first set of experiments, we have divided each database into train and test sub-datasets. For the training, we used images collected from the first 15 subjects (i.e. 1650 real and fake imgaes). For testing we deployed images collected from the last 10 subjects (i.e. 1100 real and fake images).

Table II presents the classification results using MobileNet for feature extraction besides a shallow classifier (SVM) using different metrics. From this table, we can observe that, although Complex classifiers, like SVM-RBF might be more sensitive to over-fitting than simpler classifiers (i.e. SVM-linear), they achieve better presentation attack detection on both databases Dermalog and Greenbit. For example an ACER equals to 6.15% is obtained on dermalog database using SVM classifier with linear function, whereas ACER equals to 3.78% when SVM with RBF is used for classification on the same dataset. Also, we can notice that images acquired with GreenBit scanner have been easy to classify and this has improved the liveness accuracy on this dataset. The liveness accuracy on Dermalog and GreenBit is 96.45% and 97.42 %, respectively.

To gain insight into the generalization capabilities of MobileNet-SVM based method for fingerprint liveness detection, we conducted a cross-sensor evaluation. Here, the countermeasure has been trained and tuned on one full database (Dermalog or GreenBit) and then tested on the other database. The classification results of these experiments are listed in Table III. First, we use Dermalog dataset for training and images captured via GreenBit sensor for testing. Table III reports an ACER value of 1.3% on the testing dataset. In the second set of experiments, Geenbit images are used for training and tuning our model whilst Dermalog dataset is used for testing. This last set of expriments refers to attain an overall liveness detection accuracy of 98%. Our results using a cross-sensor evaluation provide evidence that the proposed framework has very high generalization capabilities and show very interesting accuracies, that are better than ones obtained for the intra-test (using the same database for training and testing).

TABLE III *Inter-Test liveness detection results using MobileNet-SVM method*

Database		SVM-RBF			
Training	*Testing*	APCER	NPCER	ACER	ACC
GreenBit	Dermalog	1.46	2.64	2.05	98
Dermalog	GreenBit	2.4	1.28	**1.3**	98.10

Our proposed approach is compared with previous liveness fingerprint algorithms (from the state of the art). In fact, our FLD algorithm is compared with Gragnaniello et al. method (WLD) [6], Yuan et al. method (multi-sqale LPQ and PCA) [7], Nogueira et al. method (CNN-VGG, CNN-Alexnet, and CNN-random) [10] and Zhang et al. method (Slim-ResCNN) [13]. We can observe in Table IV that the proposed liveness detection method with SVM-RBF classifier outperformed not only hand-crafted based methods but also some deep learning approaches such as CNN-random [10] and DenseNet [14]. While, the FLD systems developed in [10] via CNN-VGG and CNN-Alexnet have shown to attain results in line with those by the proposed MobileNet-SVM system.

TABLE IV *Average Performance comparison of the proposed framework with some state of the art systems*

Approach	Database	Test	ACER(%)	Reference
WLD	LivDet2011	Intra-test	15.4	[6]
Jia’s method	LivDet2011	Intra-test	9.95	[15]
Multi-scale LPQ + PCA	LivDet2011	Intra-test	8.62	[7]
CNN-VGG	LivDet2013	Intra-test	2.32	[10]
CNN-Alexnet			2.85	
CNN-Random			3.5	
Slim-ResCNN	LivDet2015	Intra-test	2.65	[13]
DensNet	LivDet2015	Intra-test	4.87	[14]
MobileNet + SVM	LivDet2023	Intra-test	3.12	Proposed framework
MobileNet + SVM	LivDet2023	Cross-sensor	**1.67**	Proposed framework

IV. Conclusion

Biometrics-based automated person recognition systems are being used by individuals, industries as well as by governments at large scales (e.g. at border crossing). However, it is not a secret that most of existing fingerprint recognition systems are vulnerable to spoofing attacks (i.e. presenting a fake fingerprint in front of the sensor). To detect spoofing attacks, in this paper, we suggested a framework for fingerprint liveness detection in biometrics recognition systems based on MobileNet-SVM combination. Extensive experiments on LivDet 2023 database showed excellent results. Besides, in our inter-database evaluation, MobileNet-SVM showed very promising generalization capabilities. As a future work, we aim to evaluate the method under big data and wide-ranging scenarios

References

[1] A. Jain, R. Bolle, and S. Pankanti, “Introduction to biometrics,” in *Biometrics*. Springer, 1996, pp. 1–41.

[2] H. Abderrahmane, G. Noubeil, Z. Lahcene, Z. Akhtar, and D. Dasgupta, “Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems,” *IET Biometrics*, vol. 9, no. 3, pp. 91–99, 2020.

[3] A. Herbadji, Z. Akhtar, K. Siddique, N. Guermat, L. Ziet, M. Cheniti, and K. Muhammad, “Combining multiple biometric traits using asymmetric aggregation operators for improved person recognition,” *Symmetry*, vol. 12, no. 3, p. 444, 2020.

[4] G. Orrù, R. Casula, P. Tuveri, C. Bazzoni, G. Dessalvi, M. Micheletto, L. Ghiani, and G. L. Marcialis, “Livdet in action-fingerprint liveness detection competition 2019,” in *2019 International Conference on Biometrics (ICB)*. IEEE, 2019, pp. 1–6.

[5] L. Ghiani, G. L. Marcialis, F. Roli, and P. Tuveri, “User-specific effects in fingerprint presentation attacks detection: Insights for future research,” in *2016 International Conference on Biometrics (ICB)*. IEEE, 2016, pp. 1–6.

[6] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Fingerprint liveness detection based on weber local image descriptor,” in *2013 IEEE workshop on biometric measurements and systems for security and medical applications*. IEEE, 2013, pp. 46–50.

[7] C. Yuan, X. Sun, and R. Lv, “Fingerprint liveness detection based on multi-scale lpq and pca,” *China Communications*, vol. 13, no. 7, pp. 60–65, 2016.

[8] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, “Local contrast phase descriptor for fingerprint liveness detection,” *Pattern Recognition*, vol. 48, no. 4, pp. 1050–1058, 2015.

[9] Z. I. Özkiper, Z. Turgut, T. Atmaca, and M. A. Aydın, “Fingerprint liveness detection using deep learning,” in *2022 9th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2022, pp. 129–135.

[10] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, “Fingerprint liveness detection using convolutional neural networks,” *IEEE transactions on information forensics and security*, vol. 11, no. 6, pp. 1206–1213, 2016.

[11] C. Yuan, Z. Xia, L. Jiang, Y. Cao, Q. J. Wu, and X. Sun, “Fingerprint liveness detection using an improved cnn with image scale equalization,” *IEEE Access*, vol. 7, pp. 26 953–26 966, 2019.

[12] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, “Mobilenets: Efficient convolutional neural networks for mobile vision applications,” *arXiv preprint arXiv:1704.04861*, 2017.

[13] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, and Z. Li, “Slim-rescnn: A deep residual convolutional neural network for fingerprint liveness detection,” *IEEE Access*, vol. 7, pp. 91 476–91 487, 2019.

[14] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, “Densely connected convolutional networks,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 4700–4708.

[15] X. Jia, X. Yang, Y. Zang, N. Zhang, R. Dai, J. Tian, and J. Zhao, “Multi-scale block local ternary patterns for fingerprints vitality detection,” in *2013 international conference on biometrics (ICB)*. IEEE, 2013, pp. 1–6.