A New Multi-filter Framework with Statistical Dense SIFT Descriptor for Spoofing Detection in Fingerprint Authentication Systems

Rodrigo Colnago Contreras[1(✉)], Luis Gustavo Nonato[1], Maurílio Boaventura[2], Inês Aparecida Gasparotto Boaventura[2], Bruno Gomes Coelho[3], and Monique Simplicio Viana[4]

[1] University of São Paulo, São Carlos, SP 13566-590, Brazil
contreras@usp.br, gnonato@icmc.usp.br
[2] São Paulo State University, São José do Rio Preto, SP 15054-000, Brazil
maurilio.boaventura@unesp.br, ines@ibilce.unesp.br
[3] New York University, New York, NY 10012, USA
bgc5612@nyu.edu
[4] Federal University of São Carlos, São Carlos, SP 13565-905, Brazil
monique.viana@ufscar.br

Abstract. Fingerprint-based authentication systems represent what is most common in biometric authentication systems. Today's simplest tasks, such as unlocking functions on a personal cell phone, may require its owner's fingerprint. However, along with the advancement of this category of systems, have emerged fraud strategies that aim to guarantee undue access to illegitimate individuals. In this case, one of the most common frauds is that in which the impostor presents manufactured biometry, or spoofing, to the system, simulating the biometry of another user. In this work, we propose a new framework that makes two filtered versions of the fingerprint image in order to increase the amount of information that can be useful in the process of detecting fraud in fingerprint images. Besides, we propose a new texture descriptor based on the well-known dense Scale-Invariant Feature Transform (SIFT): the statistical dense SIFT, in which their descriptors are summarized using a set of signal processing functions. The proposed methodology is evaluated in benchmarks of two editions of LivDet competitions, assuming competitive results in comparison to techniques that configure the state of the art of the problem.

Keywords: Liveness detection · Spoofing detection · Fingerprint authentication system · Dense SIFT · Pattern recognition

1 Introduction

Currently, confirmation of a person's identity is indispensable in carrying out the simplest tasks, such as logging in to a webpage, as well as in the most important routines, such as freeing access in work environments that demand a high degree of security and employees control [1]. Thus, studies on biometric authentication systems (BAS) [18]

L. Rutkowski et al. (Eds.): ICAISC 2021, LNAI 12855, pp. 442–455, 2021.
https://doi.org/10.1007/978-3-030-87897-9_39

are increasingly needed, which validate the identity of users of certain services through the recognition of properties that preserve the individuality of each person. In this case, these properties are defined mainly by two types of characteristics [38]: physiological, such as fingerprints [3], faces [33], ears [5], etc.; and behavioral, such as voice [46], walking mode [26], etc. Also, systems that make use of more than one characteristic of the individual to perform authentication are not uncommon [11].

In the universe of BAS, we highlight those who use fingerprints [29] to perform the recognition of individuals, which are called fingerprint authentication system (FAS). This biometry is the most used in this context due to the ease of conducting its collection and the high amount of techniques [19] and software packages [41] available in the literature that helps in the improvement of theories involving this theme. Thus, BAS based on fingerprints are biometric systems that receive more and more attention in the academic environment and business solutions.

The convenience provided by the use of fingerprints as biometrics, combined with advances in image recognition and classification technologies, has provided a considerable expansion in the use of FAS in practical solutions. As an example, we can mention its popularization in usual applications in which it was more common to use passwords, such as access tasks involving smartphones [44]. However, the threat of fraud, that is, *spoofing attacks*, remains a disadvantage in this type of system since the security of such applications can be compromised by imposters [20]. Notably, one of the most common forms of FAS fraud is that known as *spoofing presentation attack* (SPA) [24], which consists of the improper presentation of a fingerprint manufactured using synthetic materials [7] to simulate the biometrics of a legitimate user of the system. To encourage the development of techniques to soften this situation, several competitions have been proposed in recent years [42], the first being held in 2009 [25]. The Liveness Detection (LivDet) Competition gave rise to a series of databases composed of a large volume of examples of legitimate fingerprints and synthetic fingerprints produced from different materials. These bases currently form the benchmarks that are considered for evaluating methodologies in works on this theme.

Recently, some methodologies have been proposed in an attempt to circumvent the SPA threat in FASs. Most of these strategies are based mainly on three categories of methods [30]:

C_1 methods based on texture descriptor analysis and other characteristics inherent to digital printing;
C_2 methods composed of deep learning networks,
C_3 hybrid methodologies or framework-based methods.

The first category of techniques, which is the most widely used in this theme [2], is defined by creating the artificial characteristics, or hand-crafted features (HCF) [27], extracted from the image of a fingerprint to perform the classifier training. Among these features, those obtained from the texture descriptors [16] and image quality measures [9] are recurrent. The methods that define the second category of problems are those that analyze the natural characteristics of fingerprints and generally make use of deep learning neural networks (DNN) [43], for which those particularly known as Deep Convolutional Neural Network (D-CNN) [31] present good results in the state-of-the-art for SPA treatment. Finally, the last category of methods is defined by strategies that make

use of both HCF and DNNs [37,45]. This category also comprises those that define elaborated frameworks for the extraction of features, with pre-processing steps, dimensionality reduction, and training of classifiers [35].

In this work, our advances are concentrated in the categories C_1 and C_3. Specifically, we innovate on two main fronts:

- with the proposal of a new framework for the extraction of characteristics of fingerprint images,
- with a new micropattern descriptor based on measurements taken from the well-known Dense Scale-Invariant Feature Transform (DSIFT).

The paper is organized into 5 sections. In Sect. 2, we discuss some fundamentals of the used descriptor (DSIFT). The formulation of the proposed method and the details of all its functionalities are presented in Sect. 3. Our framework is evaluated in the benchmarks of three different editions of the LivDet competition and the experimental results obtained are presented in Sect. 4. The manuscript ends with conclusions and proposals for future work in Sect. 5.

2 Dense SIFT Fundamentals

The pattern descriptor known as SIFT [23] is widely used in pattern recognition and detection tasks in images [21]. In summary, its operation is conducted from the analysis of gradient histograms present in the neighborhood of some points of interest present in the image. This measure is invariant to scale and rotation transformations, however, the characteristics represented by its descriptors are sparse, since they are dependent on the set of determined keypoints. Thus, Liu et al. [22] propose a modification of the method that takes into account all the points of an image for construct its descriptors: the DSIFT.

In recent years, many variants of this pattern descriptor have been proposed to improve its representation capacity. In this work, we will make use of one of its most robust representations: the *Pyramid Histogram Of visual Words* (PHOW) [6]. In detail, we can define this technique mathematically through 5 steps, detailed below:

1. **Step 1:** Consider the image I and a grid mesh $\mathcal{M}$ defined over I so that its nodes are spaced apart by S pixels. Also, let's assume that the $\mathcal{M}$ nodes are equally spaced representations of N pixels of I, which make up the set $\mathcal{P} = \{P_1, P_2, ..., P_N\}$.
2. **Step 2:** A set of 4 neighborhoods is made around each pixel P_i of $\mathcal{P}$, that is, $\mathcal{V} = \{V_{i,1}, V_{i,2}, V_{i,3}, V_{i,4}\}$. Each neighborhood $V_{i,j}$ is centered on the pixel P_i and is formed by grids of dimension 4×4, with each cell of these grids having dimension $\sigma_{i,j} \times \sigma_{i,j}$. Besides that, $\sigma_{i,1} < \sigma_{i,2} < \sigma_{i,3} < \sigma_{i,4}$.
3. **Step 3:** Then, the gradients [10] are calculated in each of the 16 cells of each neighborhood in $\mathcal{V}$ so that only the main 8 directions of the plan are considered, which are presented in Δ:

$$\Delta = \{(0,1); (1,0); (0,-1); (-1,0); (1,1); (1,-1); (-1,-1); (-1,1)\}.$$

In addition, gradients with a magnitude below a pre-established threshold δ are disregarded.

4. **Step 4:** With the gradients in hand, the histogram of the directions present in each cell in each neighborhood is calculated in $\mathcal{V}$. Thus, for each cell, a histogram of 8-bins is associated. Consequently, for each neighborhood $4 \cdot 4 = 16$ of these histograms are associated and, therefore, for each pixel P_i, 4 histograms of $16 \cdot 8 = 128$-bins are associated or, for simplification purposes, four vectors $\vec{d}_{i,j}$, $j = 1, 2, 3, 4$, of 128 coordinates.
5. **Step 5:** Finally, as a result of the DSIFT technique, we have a set of $4N$ descriptors in the form of 128 coordinate vectors. Thus, given an image I, the descriptors extracted with the DSIFT can be represented in their matrix form:

$$D_I = \begin{bmatrix} | & | & | & | & | & & | \\ \vec{d}_{1,1} & \vec{d}_{1,2} & \vec{d}_{1,3} & \vec{d}_{1,4} & \vec{d}_{2,1} & \cdots & \vec{d}_{N,4} \\ | & | & | & | & | & & | \end{bmatrix} \in \mathbb{R}^{128 \times 4N}. \tag{1}$$

Throughout the text, for ease of notation, we will consider D_I to be $(d_{i,j})_{i,j} \in \mathbb{R}^{128 \times 4N}$. In addition, in this work, we will follow the same parameterization of Bosch, Zisserman, and Munoz [6]. In detail, we will define on I a grid mesh with uniform spacing of $S = 5$ pixels; the dimensions of the four neighborhoods are defined by $(\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4}) = (5, 7, 10, 12), \forall i$; and let's disregard gradients of magnitude less than $\delta = 10^{-6}$.

3 Proposed Multi-filter Framework and Statistical Dense SIFT for Liveness Detection in Fingerprints

In this section, we present the components that form the proposed method for detecting SPAs in FPASs. For this, we detail the operation of all strategies used through algorithms and flowcharts that facilitate the understanding and reproducibility of the developed material. Specifically, we present the following innovations obtained with the proposed work:

- A new framework for the extraction and classification of characteristics of fingerprint images to conduct the discrimination of these images into two distinct groups: the set of legitimate fingerprints and the set of fingerprints manufactured from synthetic materials;
- A new descriptor of local patterns based on measurements taken from DSIFT histograms, presented in Eq. (1),
- The proposed method is presented in the form of a generalization, and it is functional in many configurations. Therefore, we present a practical instance of it.

3.1 Multi-filter Framework

Pattern descriptors, especially those dedicated to representing textures [34], may be dependent on illumination conditions [40]. In this way, a correction step conducted by histogram equalization strategies should be used to enhance the ability to represent the pattern descriptor used. This being one of the initial steps of the proposed framework.

It is known that, in the analysis of fingerprint images, some natural phenomena associated with the human finger may occur, which end up compromising the image collection performance by the sensor used [28]. As an example, we can mention the cases in which the fingers are too wet or too dry, are dirty, are excessively oily, among others. Thus, the characterization of the collected fingerprint is impaired in these situations and the use of a smoothing filter can be used to mitigate these difficulties. However, the use of this type of technique can make it difficult to detect important features of a fingerprint, which can be crucial for the classification step, since they are dissolved in the image using these filters. This problem is intensified in cases where the image captured by the sensor does not fit into any of the problem situations mentioned and, therefore, does not have any noise class in its composition. For this reason, using the original image together with its smoothed version is a powerful strategy in the task of representing the texture. Also, we propose the use of a sharpening filter so that the characteristics that are not very outstanding can be highlighted in the image and, consequently, are used in the task of representing the image together with the features extracted from the original image and the smoothed image.

In the special case of the synthetic fingerprint recognition problem, some authors [32] have already highlighted classes of patterns that are inherent to the counterfeiting process, such as artifacts in the form of "holes" present inside of the finger and in the form of extensive homogeneous regions that have lost many details through the manufacturing process. For these situations, the filtering can also be useful in highlighting substantial differences compared to the original image, since the effect of the filtering can be more intense in images of synthetic fingers. For example, in Fig. 1, three versions of the fingerprint image from the same individual, whose code is "002_4_0" in the database LivDet 2015 [15], is presented.

(a) Original. (b) Latex. (c) Gelatin.

Fig. 1. Fingerprint of index "002_4_0" from "Hi_Scan 2015" train database. Highlighted in red are the patterns and artifacts generated in the fingerprints during the production process.

Specifically, in Fig. 1b, we see an artifact inside the fingerprint manufactured with latex, highlighted by a red rectangle, which defines a region of high frequencies. In this image, a smoothing would be much more efficient, and therefore more significant, than it would be in the real fingerprint, shown in Fig. 1a. On the other hand, when analyzing

the finger construction made with gelatin, shown in Fig. 1c, we notice the presence of a very homogeneous region, highlighted by the red triangle, in which the use of sharpening filtering would be more effective than it would be in the real image. In summary, extracting the descriptor from three different versions of the same fingerprint should increase the representational capacity of the descriptor, since the difference between the features extracted from each of the three versions of the same image must be more intense in manufactured fingerprints, due to the presence of artifacts, than in legitimate fingerprints.

Thus, the proposed framework for SPA detection in FPAS consists of conducting the following steps:

- **Parameter initialization**: to use the framework, it is necessary to define a pattern descriptor that will be used to represent the images. Then, a histogram equalization technique is defined. Also, the used filtering techniques are defined, one being smoothing and one sharpening.
- **Definition of the database**: the method demands the use of a set of images of fingerprints known to be legitimate and of fingerprints known to be manufactured since it is necessary to carry out the training of a classifier.
- **Illumination unbalance correction:** In this phase of the method, the histogram of the fingerprint image is equalized.
- **Filtering:** A smoothed version and a sharpened version of the original image are calculated.
- **Pattern extraction:** A feature vector is extracted from the three versions considered in the image using the selected pattern descriptor.
- **Construction of feature vector:** In this step, the feature vector of each of the three versions of the fingerprint image is concatenated to compose only one feature vector that represents the image. Then, according to the descriptor used, it may be necessary to carry out the normalization of the characteristic vector, as well as to conduct some feature selection process.
- **Definition of the recognition model:** After extracting a feature vector from each of the considered fingerprint images, it is necessary to define a classifier, usually based on some machine learning technique, using the fingerprints in which its category is known. In other words, a training base is used to make the selected classifier capable of separating the feature vectors between vectors extracted from legitimate fingerprints and vectors extracted from manufactured fingerprints. Finally, after training, the spoofing-detection model is defined based on the classifier.

In summary, in Fig. 2, a flowchart of the proposed framework is presented.

3.2 Statistical Dense SIFT

In this work, we propose a new way of summarizing the descriptors extracted from the fingerprint image using DSIFT: the Statistical DSIFT (sDSIFT). In other words, given an image I, we propose to represent its DSIFT descriptors D_I, presented in Eq. (1), by a vector of real coordinates, which must be obtained using simple measures extracted from the 128 lines of D_I. A preliminary strategy, which proved to be very effective

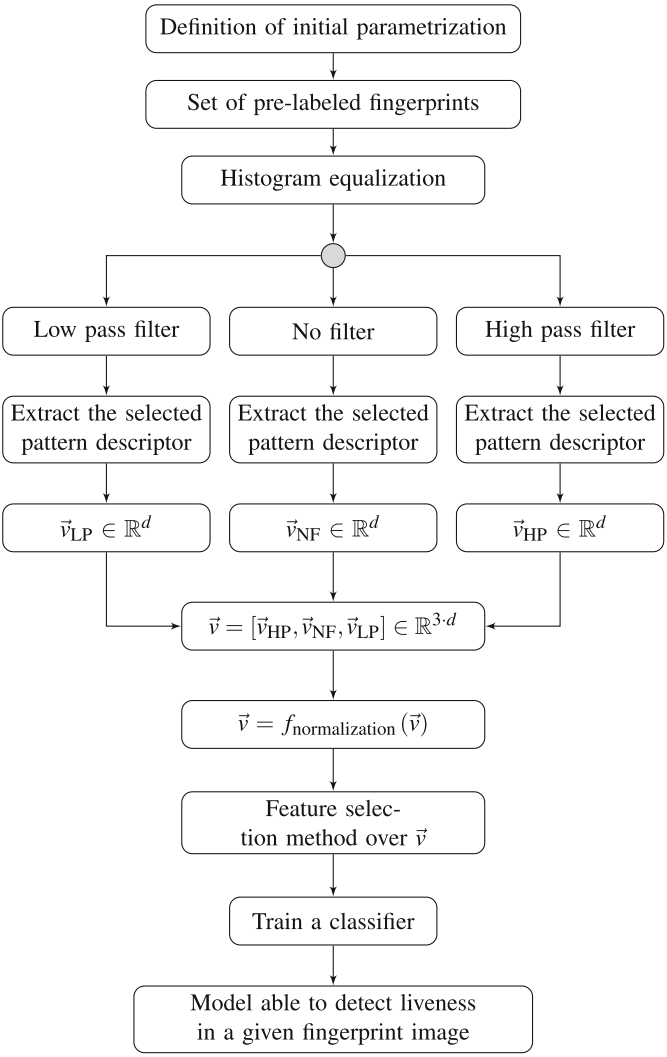

Fig. 2. Flowchart of the proposed framework. In this case, d is the dimension of the feature extracted from the image.

in the task of representing texture images, was proposed by Erpenbeck et al. [13], in which the authors summarize the SIFT descriptors of 36 keypoints considered using the mean and standard deviation. Our technique consists of a generalization in which, specifically, given a matrix of descriptors D_I in the form presented in Eq. (1), we extract from this matrix a set of vectors in $\mathbb{R}^{128}$ using a pre-established set of K functions $\mathcal{F}_{\text{SP}}$, as defined in Eq. (2), and finally, we concatenate all these vectors to form the feature vector that represents I.

$$\mathcal{F}_{\text{SP}} := \{f_1, f_2, f_3, \ldots, f_K\}, \tag{2}$$

in which, f_j is, for every j, a function defined in the form of the Eq. (3):

$$\begin{aligned} f_j : \mathbb{R}^{128\times N'} &\longrightarrow \quad \mathbb{R}^{128} \\ D \quad &\longmapsto f_j(D) := \overrightarrow{v}_j, \end{aligned} \tag{3}$$

where $N' = 4N$, and N is the pixel number considered in the DSIFT calculation.

Therefore, the proposed descriptor associates to a given image I, a vector $\vec{v} \in \mathbb{R}^{128K}$, formed by statistics or measurements of the descriptors D_I of the considered image. In Algorithm 1, we present in detail, the operation of the proposed technique.

Algorithm 1. Proposed Statistical DSIFT.

Input:	I	A given image.
	$\mathcal{F}_{\text{SP}}$	The set with K measures to be extracted from the DSIFT descriptors.

1: $D :=$ DSIFT(I) ▷ Extract DSIFT descriptor from I.
2: **for** $f_j \in \mathcal{F}_{\text{SP}}$ **do**
3: $\quad \overrightarrow{v}_j := f_j(D)$ ▷ Calculate the statistics of the descriptors (D) using f_j.
4: **end for**
5: $\overrightarrow{v}_{\text{sDSIFT}} := [\overrightarrow{v}_1, \overrightarrow{v}_2, ..., \overrightarrow{v}_K]$ ▷ Join the vectors.

Output:	$\overrightarrow{v}_{\text{sDSIFT}}$	The Statistical DSIFT feature vector extracted from I.

3.3 Proposed Instance

The proposed method, described in the two previous Sects. 3.1 and 3.2, is a generalization that allows several configurations, since our framework allows the use of any histogram equalization technique, smoothing filtering, sharpening filtering, and even pattern descriptor. The same goes for our sDSIFT, as the definition of this descriptor is dependent on the set of measures $\mathcal{F}_{\text{SP}}$. Thus, it is necessary to establish a specific instance to make use of the proposed method in the detection of SPAs in FPASs. Below, we indicate in detail the parameterization proposed and used in this paper:

– **Framework:**
  - We use as histogram equalization technique, the *automatic contrast-limited adaptive histogram equalization* (ACLAHE) [8], which is a technique based on the adaptive histogram equalization that makes use of textural information from blocks of the Image.
  - As a smoothing filter, we are using a Gaussian filter defined by a standard deviation kernel equal to 1.
  - To perform the sharpening, we use a Laplace filter, in which the mask that defines it is a matrix 5×5 with a central coordinate equal to 24 and other coordinates equal to -1.

- The pattern descriptor that we use in the framework is the proposed sDSIFT.
- We evaluate two normalization functions used in isolation in the framework. In this case, the functions $f_{\text{normalization},1}$ and $f_{\text{normalization},2}$ used are, respectively, the well-known normalizations Min-Max and z-score [17].
- The feature selection is done with a recent technique based on the meta-heuristic genetic algorithm [36].
- To classify the images, we use a linear support vector machine (SVM).

– **sDSIFT parameters**: we use five measures ($K = 5$) to summarize the DSIFT descriptors of the images. In this case, these used measures are [12]: the average (f_1), the standard deviation (f_2), the maximum value (f_3), the average energy (f_4) and the entropy (f_5) between the columns of the descriptor matrix. Mathematically, considering the matrix $D = (d_{i,j})_{i,j} \in \mathbb{R}^{128\times N'}$, the functions of $\mathcal{F}_{\text{SP}}$ are presented in Eq. (4):

$$f_1(D) := \frac{1}{N'}\left[\sum_{j=1}^{N'} d_{1,j}, \ldots, \sum_{j=1}^{N'} d_{128,j}\right], \tag{4a}$$

$$f_2(D) := \frac{1}{N'}\left[\sum_{j=1}^{N'}\left(d_{1,j} - \sum_{r=1}^{N'}\frac{d_{1,r}}{N'}\right)^2, \ldots, \sum_{j=1}^{N'}\left(d_{128,j} - \sum_{r=1}^{N'}\frac{d_{128,r}}{N'}\right)^2\right], \tag{4b}$$

$$f_3(D) := \left[\max_{j\in\{1,2,\ldots,N'\}}\{d_{1,j}\}, \ldots, \max_{j\in\{1,2,\ldots,N'\}}\{d_{128,j}\}\right], \tag{4c}$$

$$f_4(D) := \frac{1}{N'}\left[\sum_{j=1}^{N'} d_{1,j}^2, \ldots, \sum_{j=1}^{N'} d_{128,j}^2\right], \tag{4d}$$

$$f_5(D) := -\left[\sum_{j=1}^{N'} p_{1,j}\cdot\log_2\left(p_{1,j}+\varepsilon\right), \ldots, \sum_{j=1}^{N'} p_{128,j}\cdot\log_2\left(p_{128,j}+\varepsilon\right)\right], \tag{4e}$$

in which, $p_{i,j} := \dfrac{d_{i,j}}{\sum_{r=1}^{N'} d_{i,r}}$ and $\varepsilon := 10^{-10}$.

4 Experiments and Results

To validate the proposed material, we conduct practical assessments on the most well-known benchmarks on the topic. The results show that the framework is able to increase the fraud detection efficiency in FPASs with the use of sDSIFT. In this case, the two most used editions of the Liveness Detection competition were considered for evaluations. In detail, we consider the LivDet 2013 base [14], which consists of three sensors[1]: Biometrika, Italdata, and Swipe; and we consider the LivDet 2015 base [15], consisting

[1] The CrossMatch sensor has a cataloging error, so we do not consider it in the evaluations.

of four sensors: CrossMatch, GreenBit, Digital, and Hi_Scan. To carry out the training, we apply the proposed methodology in the form of the framework to each sensor in each base, making no exchange of information between sensors or bases.

To conduct our experiments, we developed a computational prototype of our framework in MATLAB R2018a. To implement the proposed sDSIFT descriptor, we used the VL_Feat library [39], widely used in image processing and recognition tasks.

For our analysis, we consider three different versions of the proposed method:

V1 (sDSIFT + SVM): In this version, we are evaluating only the proposed descriptor without considering any stage of the framework. At the end of the extraction of the descriptor of each sensor, we conduct training and classification using a linear SVM.

V2 (FW + sDSIFT + $f_{\text{normalization},1}$): In this version, we consider the proposed descriptor and all the steps of the defined instance of the framework, and the step of feature vector normalization is done by the normalization function $f_{\text{normalization},1}$.

V3 (FW + sDSIFT + $f_{\text{normalization},2}$): A version similar to the previous one, with the exception that we are using in this the normalization function $f_{\text{normalization},2}$.

In Table 1, we present the results obtained using the three proposed versions of the method and compare them with the performance of methods that define the state of the art. In detail, for comparison, we consider: the winners of each edition of fingerprint liveness detection competition [14,15]; three different techniques by Tan et al. [35]; and the Alshdadi et al. [4] method. These last two were chosen because they are recent techniques that are similar to the proposed methodology.

Table 1. Comparison of accuracy (Acc), in percentage (%), obtained by three versions of the proposed method. The best values are highlighted in bold. **Avg** represents the average accuracy for each method considering all the sensors in each year of the competition. **AVG** represents the average accuracy of each method considering all the sensors and all the years of competition.

Edition	2013				2015					
Method	Biometrika	Italdata	Swipe	Avg	Hi_Scan	CrossMatch	Digital	GreenBit	Avg	**AVG**
V1	95.85	90.3	92.34	92.83	86.88	90.74	83.68	90.26	87.89	90.01
V2	98.8	**99.85**	**97.3**	**98.65**	**99.20**	**99.49**	92.40	91.50	95.65	**96.93**
V3	**99.6**	96.6	96.5	97.57	98.40	99.35	**98.10**	94.40	**97.56**	**97.56**
CoALBP [35]	97	99.4	95.8	97.40	92.16	97.29	93.24	92.79	93.87	95.38
CoALBP-GIF [35]	96.7	98.6	95.2	96.83	90.16	97.18	93.24	94.83	93.85	95.13
Guided filter [35]	98.1	**99.85**	96.3	98.08	93.36	98.77	94.08	94.27	95.12	96.39
Winner [14,15]	95.3	96.5	85.93	92.58	94.36	98.1	93.72	95.4	95.40	94.19
Q-FFF [4]	98.7	98.8	96.5	98.00	96.4	96.73	91	**97.37**	95.38	96.5

According to the obtained results, we can see that, even though it is a very simple descriptor, the proposed sDSIFT, used in isolation for the training of a linear SVM and represented by **V1**, was able to overcome the winner's results of the 2013 edition of the LivDet competition. However, the other results presented by this technique are inferior to the majority of the results that configure the state of the art in the specialized

literature. As an example, we can note that this technique was the only one considered to have an average accuracy of less than 90% in the 2015 edition. This fact is useful to highlight the importance of using the framework, represented by the other two versions of the proposed technique (**V2** and **V3**) that use the framework together with the sDSIFT descriptor since the results presented by these are much better than the results presented with the isolated use of sDSIFT. Mathematically, the use of the framework compared to the isolated use of sDSFIT improved 6.92% the accuracy obtained by the method in **V2** and 7.55% in **V3**. Indeed, these techniques have the two best average accuracy results (**AVG**) considering all sensors from the 2013 and 2015 competitions.

When we use the proposed descriptor together with the framework with normalization performed by $f_{\text{normalization},1}$ (**V2**), we obtain the best accuracy value in most of the considered sensors. In addition, this version of the technique presents, on average, the best accuracy when considering only the 2013 edition of the competition. In the case of the 2015 competition, **V2** has the second-best average accuracy value among the considered techniques, having shown accuracy greater than 99% in the classification of two sensors from this base.

The use of sDSFIT together with the normalization function $f_{\text{normalization},2}$ in the framework (**V3**) seems to add greater stability to the method since this technique presented the best overall average accuracy (**AVG**) among all the other techniques. Being its worst performance presented in the GreenBit sensor of LivDet 2015, in which it presented 94.4% accuracy, which configures a result similar to those presented by the techniques of Tan et al. [35] and only 1% less compared to the result presented by the winner of the respective edition of the competition. Furthermore, when considering only the 2015 edition, **V3** presents more than 2% of better average accuracy compared to the methods that represent the state of the art.

Thus, we can see that the results obtained by the proposed descriptor, although adequate in some instances, have been considerably improved with the use of two different versions of the proposed framework. Thus, the versions **V2** and **V3** of the proposed method differ slightly from each other, presenting competitive results to those that represent the state of the art.

5 Conclusion

In this work, we propose a new texture descriptor, sDSIFT, and a new framework that intends to improve the ability of descriptors to detect SPAs in FPASs. The method is very wide and, therefore, it is necessary to define a specific instance of it to conduct its use and, finally, classify fingerprints as being spoofings or legitimate.

Three different versions of the method were evaluated, one composed solely of the proposed texture descriptor (**V1**) and two other versions composed of different configurations of the framework used in conjunction with sDSIFT (**V2** and **V3**). In this case, the results presented by these last two proved to be much superior to the results presented by the isolated use of sDSIFT in solving the problem, which serves as an indication for the proof that the use of the proposed framework can improve the representation capacity of a pattern descriptor. Besides, the results presented by **V2** and **V3** compare, or even surpass, the techniques that represent the state of the art in the problem.

We intend to analyze each of the stages of the proposed framework in isolation and how they influence the ability to improve representation in the considered descriptor. Also, we will evaluate more instances of the framework considering several different configurations. In detail, we will evaluate the performance of other meta-heuristics and other techniques, such as those based on auto-encoders, in the feature selection stage. Finally, we will extend the proposed material theory to make it possible to fusion more than one texture descriptor into the framework.

Acknowledgments. This study was financed in part by the São Paulo Research Foundation (FAPESP), process #15/14358-0, by the Brazilian National Council for Scientific and Technological Development (CNPq), process #381991/2020-2, and by the "*Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil*" (CAPES) - Finance Code 001.

References

1. Afandi, F., Sarno, R.: Android application for advanced security system based on voice recognition, biometric authentication, and internet of things. In: 2020 International Conference on Smart Technology and Applications (ICoSTA), pp. 1–6. IEEE (2020)
2. Agarwal, R., Jalal, A., Arya, K.: A review on presentation attack detection system for fake fingerprint. Mod. Phys. Lett. B **34**(05), 2030001 (2020)
3. Ali, S.S., Baghel, V.S., Ganapathi, I.I., Prakash, S.: Robust biometric authentication system with a secure user template. Image Vis. Comput. **104**, 104004 (2020)
4. Alshdadi, A., Mehboob, R., Dawood, H., Alassafi, M.O., Alghamdi, R., Dawood, H.: Exploiting level 1 and level 3 features of fingerprints for liveness detection. Biomed. Sig. Process. Control **61**, 102039 (2020)
5. Annapurani, K., Sadiq, M., Malathy, C.: Fusion of shape of the ear and tragus-a unique feature extraction method for ear authentication system. Expert Syst. Appl. **42**(1), 649–656 (2015)
6. Bosch, A., Zisserman, A., Munoz, X.: Image classification using random forests and ferns. In: 2007 IEEE 11th International Conference on Computer Vision, pp. 1–8. IEEE (2007)
7. Cappelli, R., Maio, D., Maltoni, D.: Synthetic fingerprint-database generation. In: Object Recognition Supported by User Interaction for Service Robots, vol. 3, pp. 744–747. IEEE (2002)
8. Chang, Y., Jung, C., Ke, P., Song, H., Hwang, J.: Automatic contrast-limited adaptive histogram equalization with dual gamma correction. IEEE Access **6**, 11782–11792 (2018)
9. Chugh, T., Cao, K., Jain, A.K.: Fingerprint spoof buster: use of minutiae-centered patches. IEEE Trans. Inf. Forensics Secur. **13**(9), 2190–2202 (2018)
10. Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In: 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005), vol. 1, pp. 886–893. IEEE (2005)
11. Dinca, L.M., Hancke, G.P.: The fall of one, the rise of many: a survey on multi-biometric fusion methods. IEEE Access **5**, 6247–6289 (2017)
12. Djebbar, F., Ayad, B.: Energy and entropy based features for wav audio steganalysis. J. Inf. Hiding Multimedia Sig. Process. **8**(1), 168–181 (2017)
13. Erpenbeck, D., et al.: Basic statistics of SIFT features for texture analysis. In: Tolxdorff, T., Deserno, T.M., Handels, H., Meinzer, H.-P. (eds.) Bildverarbeitung für die Medizin 2016. I, pp. 98–103. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49465-3_19
14. Ghiani, L., et al.: LivDet 2013 fingerprint liveness detection competition 2013. In: 2013 International Conference on Biometrics (ICB), pp. 1–6. IEEE (2013)

15. Ghiani, L., Yambay, D.A., Mura, V., Marcialis, G.L., Roli, F., Schuckers, S.A.: Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015. Image Vis. Comput. **58**, 110–128 (2017)
16. Gragnaniello, D., Poggi, G., Sansone, C., Verdoliva, L.: An investigation of local descriptors for biometric spoofing detection. IEEE Trans. Inf. Forensics Secur. **10**(4), 849–863 (2015)
17. Jain, A., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recogn. **38**(12), 2270–2285 (2005)
18. Jain, A.K., Flynn, P., Ross, A.A.: Handbook of Biometrics. Springer, Cham (2007). https://doi.org/10.1007/978-0-387-71041-9
19. Jain, A.K., Nandakumar, K., Ross, A.: 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recogn. Lett. **79**, 80–105 (2016)
20. Kiefer, R., Stevens, J., Patel, A., Patel, M.: A survey on spoofing detection systems for fake fingerprint presentation attacks. In: Senjyu, T., Mahalle, P.N., Perumal, T., Joshi, A. (eds.) ICTIS 2020. SIST, vol. 195, pp. 315–334. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-7078-0_30
21. Leng, C., Zhang, H., Li, B., Cai, G., Pei, Z., He, L.: Local feature descriptor for image matching: a survey. IEEE Access **7**, 6424–6434 (2018)
22. Liu, C., Yuen, J., Torralba, A.: SIFT flow: dense correspondence across scenes and its applications. IEEE Trans. Pattern Anal. Mach. Intell. **33**(5), 978–994 (2010)
23. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vis. **60**(2), 91–110 (2004)
24. Marcel, S., Nixon, M.S., Fierrez, J., Evans, N.: Handbook of Biometric Anti-Spoofing: Presentation Attack Detection. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-92627-8
25. Marcialis, G.L., et al.: First international fingerprint liveness detection competition—LivDet 2009. In: Foggia, P., Sansone, C., Vento, M. (eds.) ICIAP 2009. LNCS, vol. 5716, pp. 12–23. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04146-4_4
26. Medikonda, J., Madasu, H., Panigrahi, B.K.: Information set based gait authentication system. Neurocomputing **207**, 1–14 (2016)
27. Nanni, L., Ghidoni, S., Brahnam, S.: Handcrafted vs. non-handcrafted features for computer vision classification. Pattern Recogn. **71**, 158–172 (2017)
28. Patil, M.S., Patil, S.S.: Wet and dry fingerprint enhancement by using multi resolution technique. In: 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), pp. 188–193. IEEE (2016)
29. Prasad, P.S., Sunitha Devi, B., Janga Reddy, M., Gunjan, V.K.: A survey of fingerprint recognition systems and their applications. In: Kumar, A., Mozar, S. (eds.) ICCCE 2018. LNEE, vol. 500, pp. 513–520. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-0212-1_53
30. Raja, K.B., Raghavendra, R., Venkatesh, S., Gomez-Barrero, M., Rathgeb, C., Busch, C.: A study of hand-crafted and naturally learned features for fingerprint presentation attack detection. In: Marcel, S., Nixon, M.S., Fierrez, J., Evans, N. (eds.) Handbook of Biometric Anti-Spoofing. ACVPR, pp. 33–48. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-92627-8_2
31. Samma, H., Suandi, S.A.: Transfer learning of pre-trained CNN models for fingerprint liveness detection. In: Biometric Systems. IntechOpen (2020)
32. Sharma, R.P., Dey, S.: Fingerprint liveness detection using local quality features. Vis. Comput. **35**(10), 1393–1410 (2018). https://doi.org/10.1007/s00371-018-01618-x
33. Silva, E., Boaventura, M., Boaventura, I., Contreras, R.: Face recognition using local mapped pattern and genetic algorithms. In: Proceedings of the International Conference on Pattern Recognition and Artificial Intelligence, pp. 11–17 (2018)

34. Susan, S., Hanmandlu, M.: Difference theoretic feature set for scale-, illumination-and rotation-invariant texture classification. IET Image Process. **7**(8), 725–732 (2013)
35. Tan, G., Zhang, Q., Hu, H., Zhu, X., Wu, X.: Fingerprint liveness detection based on guided filtering and hybrid image analysis. IET Image Process. **14**(9), 1710–1715 (2020)
36. Too, J., Abdullah, A.R.: A new and fast rival genetic algorithm for feature selection. J. Supercomput., 1–31 (2020). https://doi.org/10.1007/s11227-020-03378-9
37. Toosi, A., Bottino, A., Cumani, S., Negri, P., Sottile, P.L.: Feature fusion for fingerprint liveness detection: a comparative study. IEEE Access **5**, 23695–23709 (2017)
38. Tripathi, K.: A comparative study of biometric technologies with reference to human interface. Int. J. Comput. Appl. **14**(5), 10–15 (2011)
39. Vedaldi, A., Fulkerson, B.: VLFeat: an open and portable library of computer vision algorithms (2008). http://www.vlfeat.org/
40. Veerashetty, S., Patil, N.B.: Novel LBP based texture descriptor for rotation, illumination and scale invariance for image texture analysis and classification using multi-kernel SVM. Multimedia Tools Appl. **79**(15), 9935–9955 (2020). https://doi.org/10.1007/s11042-019-7345-6
41. Velapure, A., Talware, R.: Performance analysis of fingerprint recognition using machine learning algorithms. In: Proceedings of the Third International Conference on Computational Intelligence and Informatics, pp. 227–236 (2020)
42. Yambay, D., Ghiani, L., Marcialis, G.L., Roli, F., Schuckers, S.: Review of fingerprint presentation attack detection competitions. In: Marcel, S., Nixon, M.S., Fierrez, J., Evans, N. (eds.) Handbook of Biometric Anti-Spoofing. ACVPR, pp. 109–131. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-92627-8_5
43. Yuan, C., Xia, Z., Sun, X., Wu, Q.J.: Deep residual network with adaptive learning framework for fingerprint liveness detection. IEEE Trans. Cogn. Dev. Syst. **12**(3), 461–473 (2019)
44. Zafar, M.R., Shah, M.A.: Fingerprint authentication and security risks in smart devices. In: 2016 22nd International Conference on Automation and Computing (ICAC), pp. 548–553. IEEE (2016)
45. Zhang, Y., Zhou, B., Wu, H., Wen, C.: 2D fake fingerprint detection based on improved CNN and local descriptors for smart phone. In: You, Z., et al. (eds.) CCBR 2016. LNCS, vol. 9967, pp. 655–662. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-46654-5_72
46. Zheng, T.F., Li, L.: Robustness-Related Issues in Speaker Recognition. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-3238-7