IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 October 2022, accepted 26 October 2022, date of publication 31 October 2022, date of current version 11 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3218335

RESEARCH ARTICLE

A New Multi-Filter Framework for Texture Image Representation Improvement Using Set of Pattern Descriptors to Fingerprint Liveness Detection

RODRIGO COLNAGO CONTRERAS[1,2], LUIS GUSTAVO NONATO[1], (Member, IEEE), MAURÍLIO BOAVENTURA[2], INÊS APARECIDA GASPAROTTO BOAVENTURA[2], FRANCISCO LLEDO DOS SANTOS[3], RODRIGO BRUNO ZANIN[3], AND MONIQUE SIMPLICIO VIANA[4]

[1]Institute of Mathematical and Computer Sciences, University of São Paulo, São Carlos, São Paulo 13566-590, Brazil
[2]Institute of Biosciences, Letters and Exact Sciences, São Paulo State University, São José do Rio Preto, São Paulo 15054-000, Brazil
[3]Faculty of Architecture and Engineering, Mato Grosso State University, Cáceres, Mato Grosso 78217-900, Brazil
[4]Computing Department, Federal University of São Carlos, São Carlos, São Paulo 13565-905, Brazil

Corresponding author: Rodrigo Colnago Contreras (rodrigo.contreras@unesp.br)

This work was supported in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 381991/2020-2; and in part by the São Paulo Research Foundation (FAPESP) under Grant 2022/05186-4, Grant 2021/15165-1, Grant 2015/14358-0, and Grant 2013/07375-0.

ABSTRACT The use of user recognition and authentication systems has become very common and is part of everyday routines for many people, guaranteeing access to the automatic teller machines, entrance to the gym or even to smartphones. Among all the biometrics that can be analyzed in this type of system, the fingerprint is the most considered due to the ease of collection, the uniqueness of each user, and the large amount of solid theories and computational libraries available in the scientific literature. However, in recent years, the falsification of these biometrics with synthetic materials, known as spoofing, has become a real threat to these systems. To circumvent these effects without the addition of hardware devices, techniques based on the analysis of texture pattern descriptors were developed. In this work, we propose a new framework based on steps of data augmentation, image processing and replication, and feature fusion and reduction. The method has as main objective to improve the ability of classifiers, or sets of classifiers, to recognize life in fingerprints. Furthermore, it is proposed a generalization of vector representation of patterns described in matrix form from the systematic use of sets of mapping functions. All the proposed material was analyzed on the well-established benchmark of the Liveness Detection competition of the 2009, 2011, 2013 and 2015 editions, presenting an average accuracy of 97.77% and being a competitive strategy in relation to the other techniques that make up the state of the art of specialized literature.

INDEX TERMS Fingerprint liveness detection, spoofing detection, pattern recognition, texture analysis, computer vision.

I. INTRODUCTION

Biometrics [1] is defined as a physiological or behavioral attribute that can be used to uniquely characterize an individual. As examples, we can cite fingerprints [2], faces [3], iris [4], ears [5], voice [6], palmprint [7], body silhouette [8], walking way [9], among others. Based on these characteristics, user recognition systems can be defined, being this known as Biometric Authentication Systems (BASs) [10]. In this case, BASs have numerous advantages in user recognition processes compared to other authentication techniques such as those based on password, since the user can forget their code or have it stolen, and those based on card presentation, as the user may lose the material and/or someone else may present it instead. Therefore, we can note that BASs do not have such a deficiency, as there is no possibility of a user forgetting or losing a biometric, except in the rare cases in which the user suffers an amputation or deformation.

The associate editor coordinating the review of this manuscript and approving it for publication was Mehul S. Raval.

Among all biometrics, the most used in BASs is the fingerprints [11]. With pickup devices becoming cheaper, even smatphones and personal computers with this feature are becoming popular, increasing the use of fingerprint-based BASs and boosting the level of security in user recognition for performing tasks, such as access to restricted locations or personal devices [12]. The preference for fingerprint biometrics is due to the following factors [13]: a considerable amount of academic research conducted on it, since this is the most explored biometrics and, consequently, more techniques and computational libraries are available; ease of collection, as the user touches a sensor for a few seconds to have their biometrics collected and authenticated in the system; quality of biometrics, since the fingerprint has all the good properties that an authentication feature should have, such as universality, as the vast majority of users have at least one finger, uniqueness, as there is no record current of two different people with the same fingerprints, and permanence, because fingerprints do not change over the user life.

Even though the use of fingerprints in BASs becomes widespread nowadays, the security of these systems can be compromised by frauds known as spoofing attacks, which consist in the presentation of a synthetic finger, or made by an imposter, which may be incorrectly recognized as authentic by the model adopted in the system [14]. In fact, we can find records in the literature of real systems that have suffered attacks of this type [15].

To overcome these adversities, advances were made in terms of hardware, this being a development that demands greater monetary investment, and software [16]. In the case of the latter [17], it is not necessary to carry out updates on the devices used by the BAS, but new routines must be attached to the user recognition model, which are dedicated to detecting life in the biometrics presented to the system. In detail, software-level detection techniques are divided into two main categories [18]: those based on neural networks, more specifically convolutional neural networks [19], whether deep or not; and those based on handcrafted features [20] that must be used in some classifier, so that the most common features are those produced by texture descriptors, by statistical measurements or by analysis of the region of interest. Regarding this second category, some researchers propose the use of some processes that favor the detection of fraud in biometrics, such as [21] and [22]: the use of a pre-processing step in the fingerprint images before the construction of features; the use of elaborate techniques for detecting regions of interest; conducting feature reduction to increase the classifier's accuracy; between others. In these cases, it is said that the technique composes a framework based on handcrafted features for spoofing detection in BASs, since the steps of the proposed technique are the same, differing only by the construction of the features that must represent the biometrics.

This work is an extended version of our preliminary work [22]. In this work, we propose a new framework based on handcrafted features to detect fingerprint spoofing. The main idea behind this work is to present an image representation enrichment method through simple pre-processing techniques in order to obtain competitive results to the methods that make up the current state of the art on the subject. In detail, the developed technique has steps of data augmentation, pre-processing, feature fusion and dimensionality reduction. The method described here in detail was, in a very preliminary version, runner-up in a challenge of the Liveness Detection (LivDet) competition of 2021. In this case, the method described here is a generalization of the preliminary version of our work. Thus, we present a more flexible and powerful method, described in greater detail, and conduct more complete experiments with more comparisons and test situations. Furthermore, we propose in this work a new representation category for texture descriptors evaluated directly in the fingerprint spoofing detection problem. In this way, the scientific advances contained in this text can be summarized in:

- A new framework for detecting life in fingerprint images;
- A new representation category of matrix based pattern descriptors;
- New experimental results of texture descriptors in the fingerprint spoofing detection problem,
- Competitive results compared to benchmarks and methods that represent the state of the art in the specialized literature.

The paper is organized into 7 sections: in the Section II, a review of related works on the topic of spoofing detection with software-level techniques is carried out; in Section III, a generalization is proposed for the representation of matrix-based texture descriptors through mappings; in Section IV, we propose a multi-step framework specialized in improving the representation of fingerprint images for the problem; in Section V, practical instances of the proposed generalizations are determined; the results that demonstrate the effectiveness of the proposed material are presented in Section VI; and the work finishes with conclusions and considerations for future developments in Section VII.

II. RELATED WORKS

One of the most used texture pattern descriptors in the literature is the Local Binary Pattern (LBP) [23], which was one of the first descriptors to be analyzed in official benchmarks for fingerprint spoofing detection competition [24]. To solve the technique's vulnerability to noise and, consequently, increase the accuracy of the classification routine, Jia et al. [25] considered two multi-scalar versions of the LBP: one obtained directly from the generalization of the LBP [26] and the other consisting of the LBP extraction from smoothed images by Gaussian filtering [27]. Furthermore, variations of this pattern descriptor, as the Uniform LBP (ULBP) [28], were proposed to solve the same problem. We can see that other well-known texture pattern descriptors have also been successfully used in the task of detecting life in fingerprints, namely the Scale Invariant Feature Transform (SIFT) [29], the Local Phase Quantization (LPQ) [30] and

its multi-scalar version [31], the Weber Local Descriptor (WLD) [32] and variations [33]. In this sense, Gragnaniello et al. [29] made a deep investigation to compare several texture descriptors in the problem. Also, it is worth mentioning that new texture pattern descriptors were developed in order to enhance the detection of spoofings. Examples include: the Quantized Fundamental Fingerprint Features (Q-FFF) [34], which proposes the joint analysis of known first-level features, which describe the orientation of the ridges of a fingerprint, with known third-level features level, which describe the contours of the ridges of a fingerprint, these being extracted, respectively, by a weighted linear combination based on Weber's law [35] and by the analysis of the two-dimensional short-time Fourier Transform [36]; the Weber Local Binary Descriptor (WLBD) [33], which considers all directions in its definition and not just the horizontal and vertical directions, in addition to conducting the computation of WLD components using LBP; the combined Shepard Magnitude and Orientation (SMOc) [37], which, as the name suggests, is based on the calculation of the phase information in the frequency domain and the spatial stimulus calculated by the Shepard magnitude [38]; the Distinctively Encoded Histogram of Fingerprint Features (DEHFF) [39], which is made from the analysis of the fingerprint ridge map, calculated from Gabor filters and response to spatial stimuli, and the analysis of the orientation of the fingerprint ridges, calculated from a variation of the LPQ; and the Comprehensive Edge Direction Descriptor (CEDD) [40], which is a descriptor made from the analysis of the implicit and explicit information of the Log-Gabor transform responses [41].

Techniques based on handcrafted features with elaborate formulations and various processes involving spoofing detection have been proposed in recent years. According to Sharma and Dey [42], this category of techniques has a clear superiority in real-world presentation attack situations, as they define simpler and faster approaches that should increase the security level of real-world BASs. Furthermore, Agarwal et al. [43] claim that the pure use of handcrafted features presents better results than its deep counterpart in most test situations involving open benchmarks on the theme. An example is a method presented by Jonathan Wu [44] and extended by Li et al. [45], in which the features are extracted by the pattern descriptors LBP, SIFT, and Histograms of Oriented Gradients (HOG) [45] and, before being used in the classification stage, they are merged by five different strategies: concatenation, sum, average, maximum and minimum between coordinates. In the same sense, Toosi et al. [47] propose a framework with three main processes: extraction of features from fingerprint images by groups of pattern descriptors; feature fusion; and classifier training. In the work, several combinations of specialized techniques were considered in each of the processes, being evaluated several known texture descriptors and, in the case of classifiers, four techniques, considering a proposal of a deep neural network, were evaluated. Tan et al. [48] proposed a framework with a pre-processing step based on guided filtering [47] and adaptive histogram equalization [48] and a dimensionality reduction step based on t -Distributed Stochastic Neighbor Embedding (tSNE) [49]. Jian et al. [52] proposed to improve the accuracy of five different texture descriptors by weighting the classifications obtained by a support vector machine (SVM) of their respective features and training another SVM with such weights. Similarly, in the work of Sharma and Selwal [53], in addition to proposing a new pattern descriptor based on an adaptive version of LBP, the authors present a new strategy based on radial SMVs and AdaBoosts ensembles [52] to improve the accuracy of pattern descriptors in the problem. The authors present a modified version of the mentioned framework [53], in which the features extracted by the descriptor Binarized Statistical Image Features (BSIF) are used for training a deep sequential neural network and such results are also considered in the AdaBoost committee.

Another category of techniques widely used in the detection of fingerprint fraud is those based on artificial neural networks, mainly convolutional neural networks (CNN). In detail, the first work to use a neural network to detect fingerprint spoofings was the CNN of Nogueira et al. [56] which, in this case, is used together with filtering steps, detection of the region of interest, histogram equalization, and data augmentation. The authors extended the work [55] with the use of transfer learning techniques considering the well-known AlexNet [56] and VGG [57] CNNs, originally trained for object detection and adjusted to discriminate images of legitimate fingerprints from fraudulent ones. Similarly, Samma and Suandi [60] investigated the learning transfer of the VGG network at three different depth levels, and the shallower network, containing only the two initial blocks of layers of the original network, had better performance in the spoofing detection. Further developments were conducted using CNNs to detect liveness fingerprints. As an example, Yuan et al. [59] proposed a new CNN with a spatial and pyramidal clustering layer, or pooling, whose initial parameterization was configured from a pre-training stage in the ''ImageNet 2012 database'' [60]. CNNs may require that the images used for their configuration are of the same dimensions, which generally entails the need to reduce their dimensions and, consequently, the loss of the original information present in the image. To overcome this difficulty and keep the information at the texture level, Yuan et al. [61] proposed a CNN with an image-scale equalization step and with adaptive learning. A densely connected variation of a CNN was proposed by Jian et al. [62], with the parameters of this network optimized by a Genetic Algorithm [63], which improved the quality of operation of the method in spoofing detection. Yuan et al. [64] highlight that CNNs comprise a category of neural networks whose parameter optimization tends to stagnate in local optima, especially in the backpropagation stage, which can compromise the results. To circumvent this adversity, the authors propose the use of a deep residual neural network (DRNN), with optimization driven by adaptive learning, and prove that the tool is more robust in the problem compared to other neural networks.

TABLE 1. Summarization of some of the main techniques for fingerprint spoofing detection. In this case, if the technique is based on handcrafted features, then the HF code is associated with it. Likewise, techniques based on artificial neural networks or deep learning are associated with ANN/DL code and techniques based on framework is associated with the FW code. In addition, ACC and ACE refer, respectively, to the average accuracy and to the average classification error of each technique.

Method	Year	Type of technique	LivDet edition	Average performance
Proposed method	2022	FW	2009 to 2015	ACC = 97.77% and ACE = 2.26%
DEHFF [39]	2022	HF	2011 to 2015	ACC = 96.56% and ACE = 3.43%
CEDD [40]	2022	HF	2011 to 2015	ACE = 4.95%
IFPAD [51]	2022	FW	2009 to 2013	ACC = 95.10% and ACE = 3.63%
HyFiPAD [53]	2022	FW	2009 to 2015	ACC = 96.45% and ACE = 3.34%
Linear SN6400 [50]	2021	FW	2009 to 2015	ACE = 4.23%
PCNN [59]	2021	ANN/DL	2011 to 2015	ACE = 3.43%
DCNNGA [62]	2020	ANN/DL	2009 to 2015	ACE = 5.72%
FLDNet (DCNNGA) [62, 65]	2020	ANN/DL	2009 to 2015	ACE = 6.10%
DRN (DCNNGA) [62, 64]	2020	ANN/DL	2009 to 2015	ACE = 11.83%
FGFF [44]	2020	FW	2011 to 2015	ACC = 96.74% and ACE = 3.75%
Q-FFF [34]	2020	HF	2011 to 2015	ACC = 95.38% and ACE = 3.64%
coALBP+GF [66]	2020	FW	2011 to 2015	ACC = 95.89% and ACE = 3.34%
DRNN [64]	2019	ANN/DL	2011 to 2015	ACC = 95,36% and ACE = 3.96%
WLBD [33]	2018	HF	2011 to 2015	ACE = 5.84%
ULBP [28]	2018	HF	2013	ACE = 12.91%
CNN [55]	2016	ANN/DL	2009 to 2013	ACE = 2.71%

Zhang et al. [65] start their work by highlighting that CNNs, in general, tend to need large amounts of parameters in their configuration and, because of the popularization of BASs in devices with less computational capacity, the authors propose a dense neural network that works with smaller amounts of parameters.

In summary, Table 1 presents some of the main methods discussed here, highlighting their differences and similarities. Specifically, the following are presented: the acronym of the method; the year of publication of the work; the category of techniques it is included in, that is, whether it is a technique based on handcrafted features, framework or neural networks; which editions of the Fingerprint Liveness Detection Competition (LivDet), that defines the benchmark of the theme, are considered in the experiments; and the average performance in terms of accuracy and/or average classification error. We emphasize that all the methods listed are used to compare the proposed material.

In this way, we can see that much has been done to circumvent the problem of fingerprint spoofing detection in BASs. However, this problem still remains open, since none of the existing methods has 100% accuracy in fingerprint liveness detection considering the benchmarks of the area. Thus, further developments on this topic are still needed. In this work, two main advances are made: the first consists of a new framework characterized by steps of data augmentation, multi-filtering, feature extraction and fusion, and dimensionality reduction, which is responsible for improving the accuracy of a given pattern descriptor or groups of pattern descriptors in discriminating fraudulent fingerprints; and the second being the proposal of a new generalization for representing texture descriptors based on mapping its matrix features.

III. MAPPING DESCRIPTORS AS A HANDCRAFTED FEATURE

Pattern descriptors such as LBP and its variations have the ability to represent an image as a feature vector in the form of a histogram that belongs to $\mathbb{R}^{n_H}$. In these cases, it becomes natural to use classifiers of simple definition and high performance such as SVMs. However, there is a category of descriptors that represent images by matrices. As an example, we can cite the pattern descriptor SIFT [66]. This descriptor represents the image as a set, or a matrix, of gradient histograms present in the neighborhood of some keypoints. In other words, for each keypoint in the image, which can reach thousands in the case of fingerprints, a histogram is calculated and stored in a matrix. In this way, the image is represented by a matrix in the $\mathbb{R}^{n_P \times n_H}$, where n_P is the number of keypoints — and therefore the number of histograms — a value possibly big. Consequently, representation strategies of this feature matrix must be adopted to make its use in classifiers feasible and efficient. In this case, one of the best known techniques and with the greatest number of variations is the one based on bag of visual words (BOVW). To represent an image using these techniques, it is necessary, previously, to define a dictionary of words, which consists of representatives of the histograms, commonly centroids obtained by some clustering algorithm, calculated from the histograms of the pattern descriptor with respect to various images that represent the classes on which to conduct the classification. Once the dictionary is determined, each image

is represented as a histogram that describes the amount by which each ''word'' appears in the set of histograms calculated by the pattern descriptor over the image. A very common problem in this type of technique is that the clustering algorithm needs to be executed on a large number of histograms, both previously, on an exemplary set of images that represent the problem to define the dictionary, and later, to represent the word pattern of the images in cases where the matrices represent many histograms. To mitigate this information, a part of the histograms of each image can be disregarded, which represents loss of information.

We can note that many pattern descriptors that represent the image by a matrix have been proposed in recent years. The best known are Binary robust invariant scalable keypoints (BRISK) [67], Speeded-up robust features (SURF) [68], KAZE [69], among other affine and scale-invariant descriptors [70]. In general, all these descriptors associate a given image I with a feature matrix D_I, in which the features are represented in the rows of this matrix, as shown in Equation 1. In the case of SIFT, for example, the matrix D_I is formed by the histograms $d_i \in \mathbb{R}^{n_H}, \forall i$, calculated for each of the n_P keypoints.

$$D_I = \begin{bmatrix} —d_1— \\ —d_2— \\ \vdots \\ —d_{n_P}— \end{bmatrix}_{n_P \times n_H} . \tag{1}$$

In this work, we propose an alternative and simplified way to represent the matrix D_I of the Equation 1. The representation is defined through a set of mapping functions that must be applied to the features, or histograms in the case of SIFT, extracted from the image I, and considered together to configure a feature vector that must represent the image. Mathematically, the set in question is $\mathcal{M}$, defined by $n_{\mathcal{M}}$ functions, as shown in Equation 2:

$$\mathcal{M} = \left\{m_1, m_2, \ldots, m_{n_{\mathcal{M}}}\right\}, \tag{2}$$

in which, each mapping function $m_i, i \in \{1, 2, \ldots, m_{n_{\mathcal{M}}}\}$, is a function that associates a vector with a matrix and, therefore, is given as follows:

$$\begin{aligned} m_i : \mathbb{R}^{n_P \times n_H} &\rightarrow \mathbb{R}^{n_H} \\ D_I &\mapsto m_i\left(D_I\right). \end{aligned} \tag{3}$$

Finally, it is defined as a manufactured characteristic of the image I obtained by the pattern descriptor Φ and represented by the set of mappings $\mathcal{M}$ to the measure $\mathcal{P}_{\Phi,\mathcal{M}}(I)$ of the Equation 4:

$$\mathcal{P}_{\Phi,\mathcal{M}}(I) := \mathcal{F}\left(m_1(D_I), m_2(D_I), \ldots, m_{n_{\mathcal{M}}}(D_I)\right), \tag{4}$$

in which D_I is the matrix generated by the pattern descriptor Φ and $\mathcal{F}(\cdot)$ is a function that represents an information fusion strategy, such as vector concatenation.

In Figure 1, the script for representing fingerprint images is schematized according to the proposed method. Since, in the example, the pattern descriptor considered is SIFT, the feature fusion strategy $\mathcal{F}$ is the concatenation of vectors, and a set of five mappings is used, namely: the average, the standard deviation, entropy, skewness and kurtosis of the features in D_I. The example fingerprint is the image I belonging to the training portion of the database ''Hi Scan'', from LivDet 2015, corresponding to the code user ''002_4_0'' and originally classified as a real image.

There are preliminary versions of specific cases of this proposed strategy in the literature. For example, in the work by Erpenbeck et al. [71], the authors considered the mean and standard deviation of histograms extracted by the SIFT descriptor as image representation. The strategy was successfully used in texture analysis to classify malaria parasites and was able to improve the accuracy of classifiers compared to BOVW-based representation techniques. Furthermore, in the preliminary version of this work [22], a specific variant, restricted to the dense version of SIFT descriptor was used in the fingerprint spoofing detection problem. However, to the best of our knowledge, no generalization of this representation of matrix-based pattern descriptors has been proposed and, consequently, little experimentation has been conducted on the problem of detecting fingerprint spoofings.

IV. A NEW FRAMEWORK BASED ON MULTI-FILTERING, DATA AUGMENTATION, FEATURE FUSION AND DIMENSIONALITY REDUCTION

The use of additional steps for pattern extraction and classification has become common in the specialized literature on fingerprint liveness detection. For example, a filtering step can mitigate the presence of noise in the images and, consequently, its counter-effect on the operation of classifiers. In this section, we present a generalization of techniques using this type of additional steps. Specifically, a framework specialized in detecting life in fingerprints based on handcrafted features is proposed, which is composed of four main strategies: data augmentation; image processing; image representation; and definition of the fingerprint liveness detection model. So all these steps are detailed below.

A. DATA AUGMENTATION

The idea of increasing the number of samples in the problem training databases is common in computer vision and pattern recognition tasks, given that this strategy has the potential to decrease the overfitting of classifiers and improve their accuracy [72]. To increase samples, perturbed and/or combined versions of the samples are usually made from simple transformations such as rotation or noise addition. In this case, this type of strategy has been successfully used in liveness detection techniques in biometrics such as faces [73], iris [74] and even fingerprints [75].

Thus, the first step that defines the proposed framework is increase the number of fingerprint samples originally defined by the training bases of the benchmarks. Mathematically, this increasing is considered to be done according to the $n_{\mathcal{T}}$

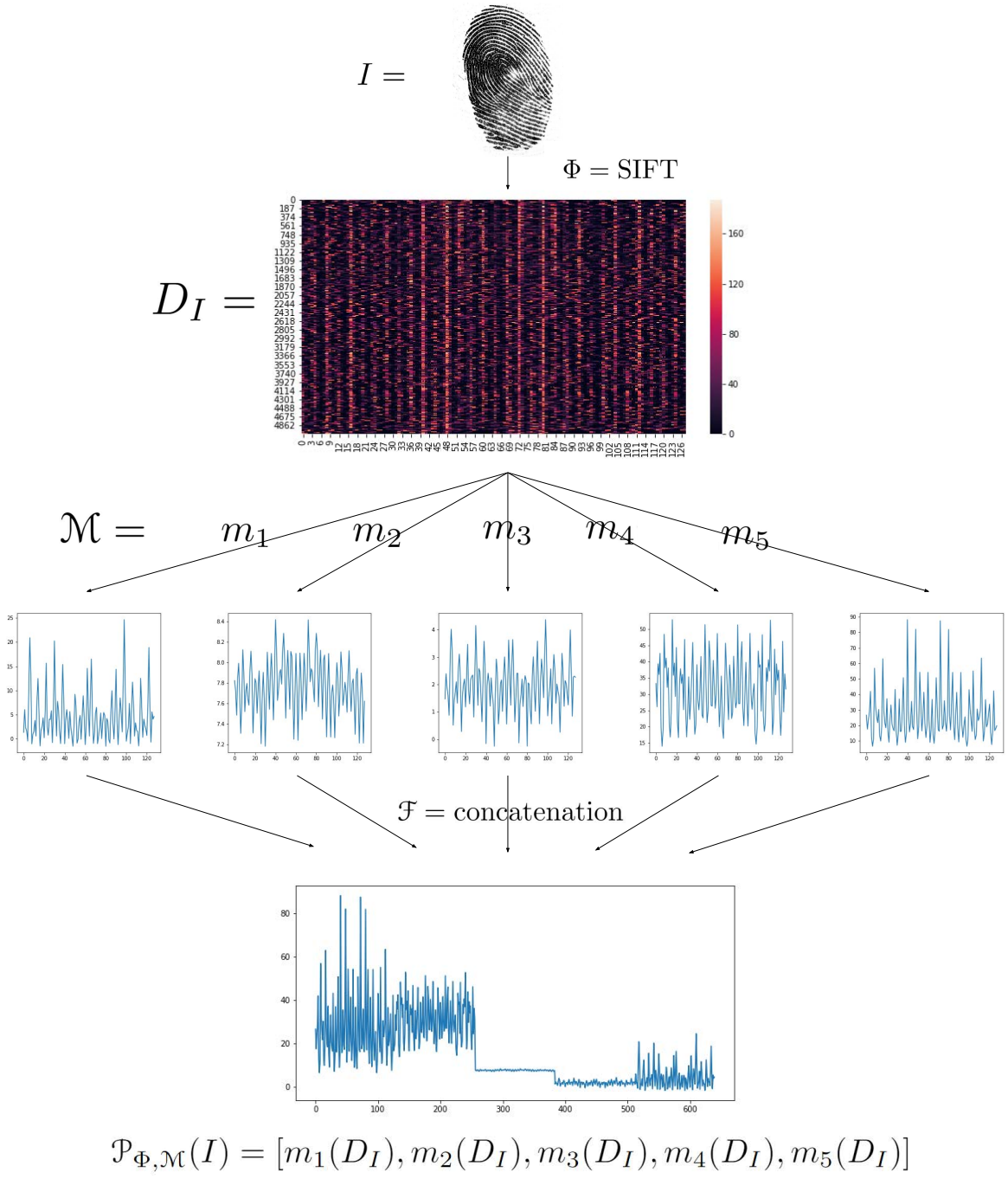


FIGURE 1. Fingerprint coding scheme by the proposed representation of matrix pattern descriptors using set of mapping functions. In the example, we are considering five mapping functions m_i responsible for determining statistical magnitudes of the columns of the matrix D_I, calculated through the descriptor Φ = SIFT. Finally,, the measurements are merged using the $\mathcal{F}$ function which, in the example, is defined by concatenation of vectors and are used to compose the mapped pattern of I: $\mathcal{P}_{\Phi,\mathcal{M}}(I)$.

transformations of the set $\mathcal{T}$:

$$\mathcal{T} = \{T_1, T_2, \ldots, T_{n_\mathcal{T}}\}, \tag{5}$$

in which, T_i are functions of matrix transformations that must be performed on fingerprint images. Thus, for each image I from a training database, more $n_\mathcal{T}$ images will be made: $T_1(I), T_2(I), \ldots, T_{n_\mathcal{T}}(I)$.

B. IMAGE PROCESSING

In this section, the generalization of one of the most common steps in fingerprint liveness detection systems is presented, which concerns image enhancement strategies to highlight important details present in biometrics. Specifically, for this framework step, we propose that the image goes through a region of interest (ROI) detection process,

followed by a multi-filtering routine and, finally, its histogram is equalized.

In detail, the ROI detection is important, since most of the sensors used do not only capture the fingerprint during the collection of biometrics, but a fixed area. For example, in the case of the sensor responsible for composing the ''Italdata'' database from the LivDet 2011 competition, many images have an extensive light-colored background and some regions with noticeable dirt, which can define a noisy texture and, consequently, compromise the proper pattern extraction according to the considered descriptor. Thus, we propose that a ROI detection strategy be employed in order to improve the biometrics representation without image background interference. For this, the function ROI$(\cdot)$ is defined, which must be applied to an image containing a fingerprint in order to obtain an image containing only the biometrics: the I_{ROI} .

In the analysis of fingerprint images, there may be some natural phenomena associated with the human finger that end up compromising the image capture by the sensor [76]. As example, we can mention the cases where the fingers are too wet or too dry, are dirty, have excess oiliness, among others. Thus, the characterization of the collected fingerprint is impaired in these situations and the use of a smoothing filter may be convenient to alleviate these difficulties. However, the use of this type of technique can make it difficult to detect important features in the fingerprint, which can be crucial for the classification step, since they are dissolved in the image with the use of these filters. Mainly in cases where the image captured by the sensor does not fit into any of the aforementioned problem situations 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. In addition, in many situations, it can be beneficial to use a sharpening filter so that the blurred features can be highlighted in the image and be used in the task of representing the image together with the features extracted from the original image and from the smoothed image.

Also in this sense, in the special case of the synthetic fingerprint detection problem, the presence of special classes of noise and imperfections in biometric images is known in the literature [77], since many details are lost in the manufacturing process. In addition, also as a result of this process, it is common for the appearance of ''artifacts'' in biometrics, in the form of holes or gaps between the fingerprint ridges, in the form of loss of continuity between these ridges or, still, in the creation of almost homogeneous regions and, consequently, without well-defined ridges. In this sense, smoothing filters may prove to be more efficient in fake fingerprints, since regions with the presence of an artifact are regions with abrupt variations in gray levels and, consequently, defined by high frequencies. Likewise, sharpening filters should be more effective in synthetic images, as defects present in biometrics, which should be more recurrent in spoofings, are highlighted by this procedure. As an example, in Figure 2, we can see that some of these artifacts were created on the fingerprint of code ''002_4_0'', in the training database ''Hi_Scan'' of the LivDet 2015 competition.

Given the raised propositions, we propose that modified versions of the fingerprint image be created using sets of filters with different behaviors. In detail, we consider the set $\mathbf{F}$ of the Equation 6 defined by $n_{\mathbf{F}}$ filtering processes, which must correspond to filters of varying characteristics. That is, $\mathbf{F}$ must be composed of low-pass filtering, high-pass filtering, mixed filtering, etc.

$$\mathbf{F} = \left\{F_1, F_2, \ldots, F_{n_{\mathbf{F}}}\right\}, \tag{6}$$

such that F_i are filters that must be applied to an image containing a fingerprint ROI I_{ROI}, giving rise to its filtered versions I_i.

Pattern descriptors, especially those that are dedicated to representing textures, can be dependent on lighting conditions [78]. In this way, a correction step conducted by histogram equalization strategies must also be incorporated in this step to enhance the descriptor representation capacity. Thus, for each image I_i generated by the filtering processes, a version I_i^{HE} with a histogram equalized by the function h must be additionally generated.

In summary, the steps for generating corrected versions of the input image described in this image processing step are presented in Algorithm 1.

Algorithm 1 Image Processing Step in the Proposed Framework

Input:		
	I	Fingerprint image.
	ROI	ROI detection routine.
	$\mathbf{F}$	Set of filters with $n_{\mathbf{F}}$ elements.
	h	Histogram equalization function.

1: $I_{\text{ROI}} := \text{ROI}(I)$ ▷ ROI detection in I.
2: **for** $F_i \in \mathbf{F}$ **do**
3: $I_i := F_i(I_{\text{ROI}})$ ▷ Calculate the filtered version of I_{ROI} using F_i.
4: $I_i^{\text{HE}} := h(I_i)$ ▷ Define a histogram equalized version of I_i using h.
5: **end for**

Saída: $\left\{I_1, I_1^{\text{HE}}, I_2, I_2^{\text{HE}}, \ldots, I_{n_{\mathbf{F}}}, I_{n_{\mathbf{F}}}^{\text{HE}}\right\}$	Versions of I as the result of this step.

C. IMAGE REPRESENTATION

As a result of the previous image processing step, we have a set $\mathcal{I}$, presented in Equation 7, which is formed by the original image I, by its $n_{\mathbf{F}}$ filtered versions I_i and its $n_{\mathbf{F}}$ filtered and histogram-equalized versions I_1^{HE}, with $i \in \{1, 2, \ldots, n_{\mathbf{F}}\}$.

$$\mathcal{I} = \left\{I, I_1, I_1^{\text{HE}}, I_2, I_2^{\text{HE}}, \ldots, I_{n_{\mathbf{F}}}, I_{n_{\mathbf{F}}}^{\text{HE}}\right\}. \tag{7}$$

We can see that each of the images in $\mathcal{I}$ may contain a feature intrinsic to the spoofing detection problem. In addition, these features must be highlighted according to the adopted filters and lighting corrections. Thus, all these images must be considered in the feature extraction process.

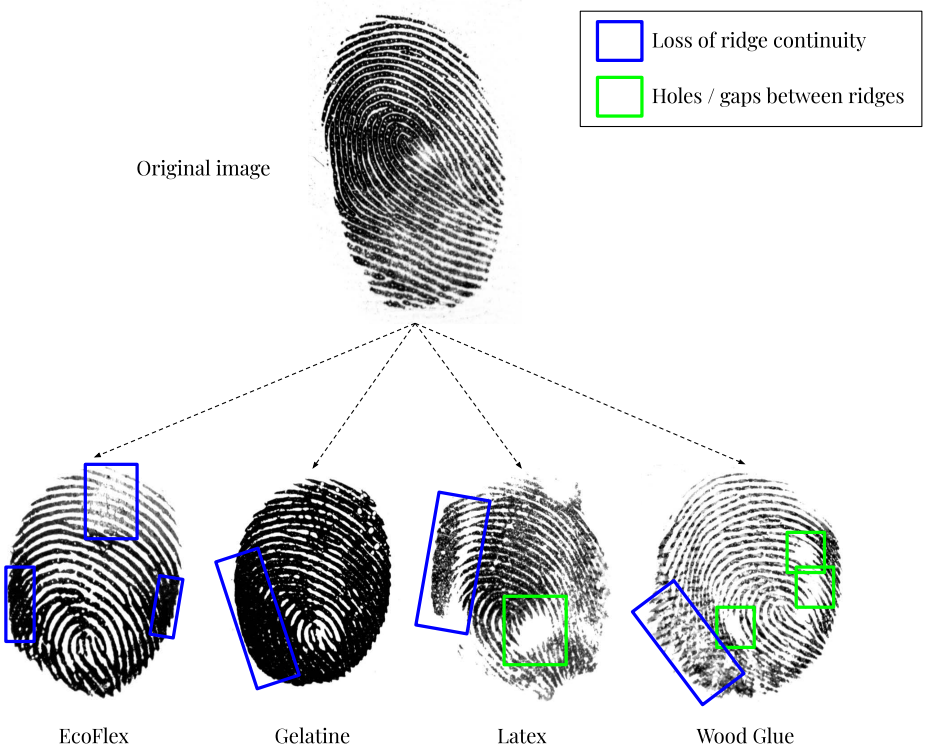


FIGURE 2. Artifacts in fake fingerprints concerning four different synthetic materials from the same individual, whose code is "002_4_0" in the database LivDet 2015. In the example, it is possible to detect in the artificial fingerprints homogeneous regions, highlighted in blue, or with discontinuities, highlighted in green.

Each pattern descriptor in the literature has a specialized representation ability that can be limited or enhanced according to the considered task or texture. Consequently, in many image recognition problems, sets of descriptors are used to represent the image in feature space. Furthermore, this approach has already been used in the detection of spoofing in fingerprints [43], [44] and in other biometrics [29]. Thus, in this work, we propose that the image representation step be composed by the extraction and aggregation of the features in all images from $\mathcal{I}$ that must be extracted using a set $\mathbf{P}$ of $n_{\mathbf{P}}$ pattern descriptors, as shown in Equation 8.

$$\mathbf{P} = \left\{\Phi_1, \Phi_2, \ldots, \Phi_{n_{\mathbf{P}}}\right\}. \tag{8}$$

In other words, each pattern in Φ_j must be extracted from the original image I, giving rise to the feature vectors $\vec{v}_{0,j}$ of Equation 9. The same must occur for the filtered versions and for the histogram equalized filtered versions, which must generate, respectively, the feature vectors of the Equations 10 and 11.

$$\vec{v}_{0,j} := \Phi_j(I), \forall j \in \{1, 2, \ldots, n_{\mathbf{P}}\}, \tag{9}$$

$$\vec{v}_{i,j} := \Phi_j(I_i), \forall i \in \{1, 2, \ldots, n_{\mathbf{F}}\}, j \in \{1, 2, \ldots, n_{\mathbf{P}}\}, \tag{10}$$

$$\vec{v}^{\,\mathrm{HE}}_{i,j} := \Phi_j(I^{\mathrm{HE}}_i), \forall i \in \{1, 2, \ldots, n_{\mathbf{F}}\}, j \in \{1, 2, \ldots, n_{\mathbf{P}}\}. \tag{11}$$

Finally, each image I will be represented by the aggregation — or fusion —, defined by the function $\mathcal{A}(\cdot)$, of all the features generated in this step. Thus, for each image I, the proposed framework associates a feature vector $\vec{v}_I$ given by the Equation 12.

$$\vec{v}_I := \mathcal{A}\left(\vec{v}_{0,1}, \vec{v}_{0,2}, \ldots, \vec{v}_{0,n_{\mathbf{P}}}, \vec{v}_{1,1}, \vec{v}^{\,\mathrm{HE}}_{1,1}, \vec{v}_{1,2}, \vec{v}^{\,\mathrm{HE}}_{1,2}, \ldots, \vec{v}_{1,n_{\mathbf{P}}}, \vec{v}^{\,\mathrm{HE}}_{1,n_{\mathbf{P}}}, \ldots, \vec{v}_{n_{\mathbf{F}},n_{\mathbf{P}}}, \vec{v}^{\,\mathrm{HE}}_{n_{\mathbf{F}},n_{\mathbf{P}}}\right). \tag{12}$$

D. FINGERPRINT LIVENESS DETECTION MODEL DEFINITION

Each vector $\vec{v}_I$ is composed of $(2n_{\mathbf{F}} + 1)n_{\mathbf{P}}$ feature vectors. Since each $\mathbf{P}$ descriptor must represent each of the images in $\mathcal{I}$. Thus, it is expected that, in many configurations of the proposed framework, the vector $\vec{v}_I$ will be of high dimension, which brings to this representation the problem of high dimensionality. To get around this situation, we propose the use of some data projection technique, represented by the transformation PROJ$(\cdot)$ that describes the data from a space $\mathbb{R}^{n_{\text{high}}}$ to a space $\mathbb{R}^{n_{\text{low}}}$, where $n_{\text{low}} \ll n_{\text{high}}$.

Finally, it is necessary to define a spoofing detection model using a classifier. In this case, a base of features extracted from images referring to the training B_{Train} of the Equation 13 must be used to adjust a classification algorithm. In addition, together with such algorithm, it is common to use some

normalization, or scaling, strategy on the feature vectors. For this, we consider that the used normalization strategy is NORM(·).

$$B_{\text{Train}} := \left\{ \vec{v}_{I_1}, \vec{v}_{I_2}, \ldots, \vec{v}_{I_{n_{\text{Train}}}} \right\}, \tag{13}$$

where n_{Train} is the number of images from the considered training image base.

In summary, in the Algorithm 2, the process of defining the spoofing detection model in fingerprint-based BASs is described according to a feature vector base.

Algorithm 2 Classifier Training Stage and Definition of the Fingerprint Liveness Detection Model in the Proposed Framework

Entrada:	B_{Train}	Training database with n_{Train} feature vectors.
	PROJ(·)	Dimensionality reduction strategy.
	NORM(·)	Normalization function.

1: **for** $i \in \{1, 2, 3, \ldots, n_{\text{Train}}\}$ **do**
2: $\hat{v}_{I_i} := \text{NORM}\left(\text{PROJ}\left(\vec{v}_{I_i}\right)\right)$ ▷ Reduce the dimension of feature vectors and normalize them.
3: **end for**
4: $\hat{B}_{\text{Train}} := \left\{ \hat{v}_{I_1}, \hat{v}_{I_2}, \ldots, \hat{v}_{I_{n_{\text{Train}}}} \right\}$ ▷ Define a training base normalized with feature vectors with smaller dimensions.
5: Train a classifier with the base $\hat{B}_{\text{Train}}$.

Output: A fingerprint liveness detection model.

E. PROPOSED ALGORITHM

The proposed framework consists of the composite and sequential use of all the steps mentioned in the previous subsections. Specifically, it is established that the following processes are executed:

1) Define the necessary parameters for the execution of the framework. These are, for example, data augmentation routines, sets of filtering techniques, etc.
2) Increase the number of samples in training database.
3) Create different versions of each image I through ROI detection routines, filtering and histogram equalization.
4) Use a set of pattern descriptors to represent the images generated in item 3. At the same time, the same is done with the original image, which was not the result of any type of image treatment.
5) Combine all the characteristics generated in item 4.
6) Reduce the dimension of feature vectors.
7) Normalize feature vectors with reduced dimension.
8) Train a classifier with the reduced dimension normalized feature vectors of all the images of the considered training database.
9) Define a fingerprint liveness detection model.

Finally, all the steps of the proposed framework are outlined in the flowchart of the Figure 3.

We can notice that, according to the proposed algorithm configuration, it is possible to define existing techniques in the literature, which corresponds to the generalizing character of the proposed material. For example, we can obtain an instance of the Tan et al. [21]'s algorithm by from the following configuration:

- Non-use of data augmentation strategy: $\mathcal{T} = \{\}$.
- Use as a technique to ROI detection, a modified Otsu segmentation method [79].
- Use the original image and its guided filtered [47] version with ROI detection. For this, the set $\mathbf{F}$ must be formed by the identity function and the guided filtering procedure.
- Use contrast limited adaptive histogram equalization [48].
- Using the co-occurrence of adjacent local binary patterns (coALBP) [80] pattern descriptor: $\mathbf{P} = \{\text{coALBP}\}$.
- Use as an information aggregation function the strategy that consists of concatenation and that disregards the feature vectors associated with the original image and with the versions of the image that do not have equalized histogram.
- Use the t-SNE technique as dimensionality reduction [49].
- Use an RBF - SVM as a classifier.

V. PARAMETERS FOR THE PROPOSED METHOD AND PRACTICAL INSTANCES

All proposed contributions, both the representation of matrix descriptors and the framework, were presented in the form of generalizations. That is, the proposed representation is dependent on a matrix descriptor Φ, a set of mappings $\mathcal{M}$, and a fusion strategy $\mathcal{F}(\cdot)$. Similarly, the framework is dependent on filtering sets, routines specialized in detecting ROI and in equalizing image histograms, among other parameters. Thus, we had to establish a specific configuration for both contributions so that a functional instance is defined. To conduct the experiments, the objective is to define the simplest possible parameterization for each case and to evaluate the improvement that the proposed strategies can obtain through elementary methodological additions.

Besides, in the preliminary content of this work [22], three different versions of the developed tool were evaluated. In this work, ten usable instances are considered to solve the problem of detecting life in fingerprints, which are detailed below.

A. MAPPING REPRESENTATION PARAMETERS

The mapping set considered is formed by statistical measurements of the features of the matrix pattern extracted from an image I by a descriptor Φ. In this case, the following mapping measures are considered [81]: mean (m_1), standard deviation (m_2), entropy (m_3), skewness (m_4) and kurtosis (m_5). In addition, the concatenation of vectors generated by all mappings will be considered as the fusion strategy $\mathcal{F}(\cdot)$. Thus, the feature vector calculated by the proposed representation will be the vector $(m_1(D_I), m_2(D_I), m_3(D_I), m_4(D_I), m_5(D_I))$.

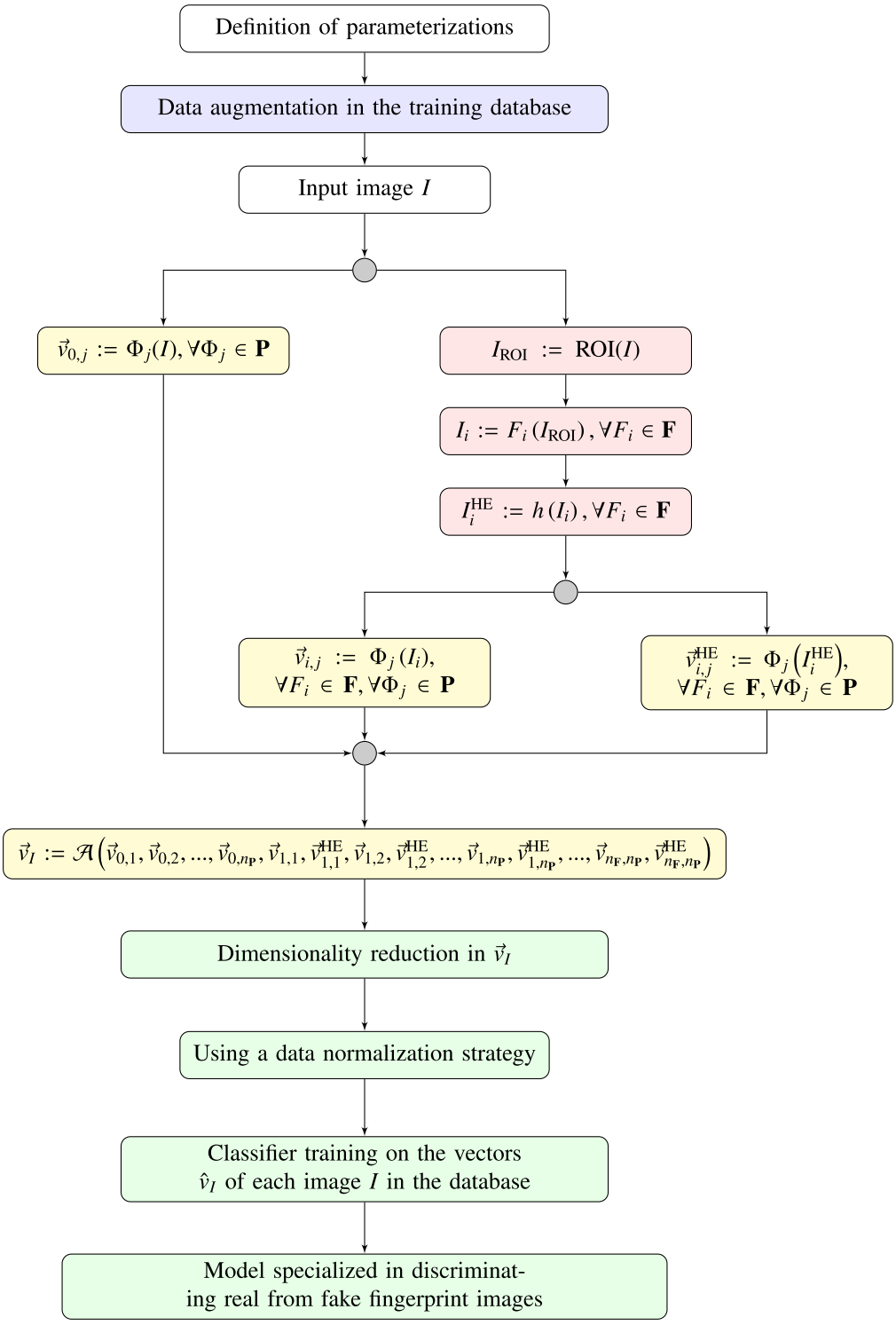


FIGURE 3. Flowchart of the proposed framework. The colors represent the steps of the method. Specifically, the blue color represents the data augmentation step, the red color represents the image processing step, the yellow color represents the image representation step, and the red color represents the fingerprint liveness detection model definition step.

We can see that in the preliminary version of this work [22], only the SIFT descriptor in its dense version (DenseSIFT) was considered for this configuration. In this work, the proposed representation method will be evaluated on the matrix patterns collected using three different descriptors: SIFT, DenseSIFT, and BRISK. These are three of the most

used pattern descriptors to solve the life detection problem in fingerprints. However, as already mentioned, any pattern descriptor that represents the image in matrix features can be represented by the proposed strategy. In this case, as $\mathcal{M}$ is formed by statistical measures, these descriptors will be referred to, respectively, by the abbreviations sSIFT, sDenseSIFT, and sBRISK.

B. FRAMEWORK PARAMETERS

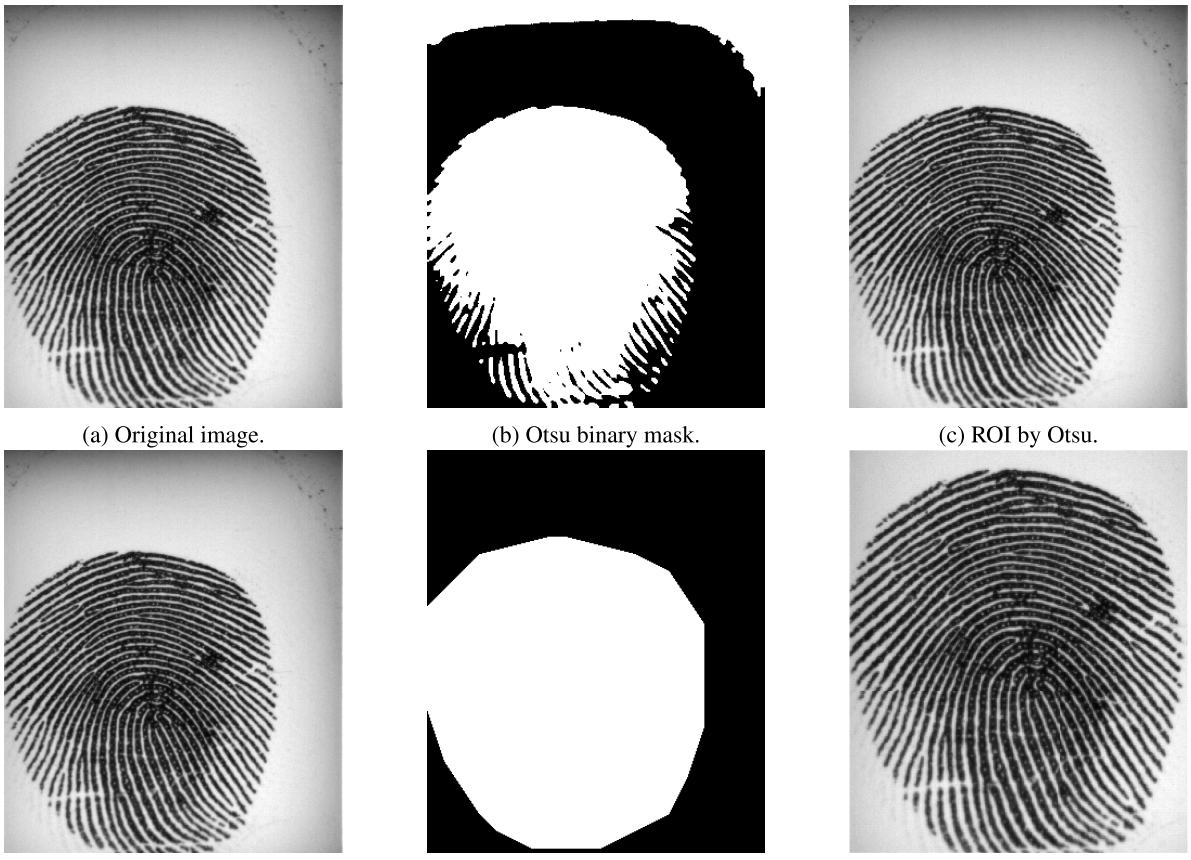
The framework demands a more extensive and elaborate parameterization than the proposed representation, since, for each step, several components must be defined. In fact, in some framework steps, more than one parameterization will be considered for analysis and, consequently, will be highlighted in this section. Thus, in the sequence, the proposed parameterization for each component of the framework is presented:

- **Data augmentation**: To increase the number of example images of the training base, five simple strategies that should compose the set $\mathcal{T}$ will be considered:
  1) Horizontal flip (T_1): the original image is reflected along the abscissa axis.
  2) Vertical flip (T_2): the original image is reflected along the ordinate axis.
  3) Double flip (T_3): the original image is modified by the two previous processes.
  4) Resizing (T_4): the original image undergoes a downsampling process so that it assumes half of its original dimensions and, subsequently, it undergoes an upsampling process via cubic spline to reassume its original dimensions.
  5) Noise addition (T_5): random Gaussian noise is added to the original image.
- **ROI detection**: Considering that traditional fingerprint segmentation techniques such as the Otsu threshold method [79] are not efficient for some fingerprints of the LivDet competition sensors, a more robust technique based on the Fisher measure [82] and active contours, described by Zheng et al. [83], is used. In Figure 4, an example of a real fingerprint image of the Biometrika sensor, code "031TamRrngBmk", from the LivDet 2013 train database is shown. Note that Otsu's segmentation is not capable of detecting the fingerprint properly, since the background of the image is not completely discarded by the binary mask, while the used technique can segment the fingerprint adequately.
- **Filters**: To preserve the original intent of the proposal, four different filtering strategies will be considered to compose the set **F**:
  1) Smoothing (F_1): this procedure is defined by a Gaussian filter of kernel with standard deviation equal to 1.
  2) Sharpening (F_2): this process is defined by a Laplace filter, whose mask is a matrix 5×5 with central coordinate are equal to 24 and the others are equal to -1.
  3) Guided filter (F_3): this routine is defined by the guided filtering of He et al. [49].
  4) ROI of non-filtered image (F_4): to define this strategy, the identity function is adopted for F_4.

TABLE 2. Versions of the proposed framework according to the set of descriptors.

Version code	**P**
$\mathbf{V}_1$	{sBRISK}
$\mathbf{V}_2$	{LPQ}
$\mathbf{V}_3$	{sSIFT}
$\mathbf{V}_4$	{sDenseSIFT}
$\mathbf{V}_5$	{coALBP}
$\mathbf{V}_6$	{LPQ, coALBP)}
$\mathbf{V}_7$	{sBRISK, coALBP}
$\mathbf{V}_8$	{sBRISK, sSIFT, sDenseSIFT}
$\mathbf{V}_9$	{sBRISK, sSIFT, sDenseSIFT, LPQ}
$\mathbf{V}_{10}$	{sBRISK, sSIFT, sDenseSIFT, LPQ, coALBP}

- **Histogram equalization**: The used lighting correction strategy (h) is one of the most used histogram equalization strategies in the literature, which consists of the limited contrast-based adaptive histogram equalization technique of Zuiderveld [48].
- **Set of descriptors**: All parameterization to this part of the text is common to all evaluated versions of the proposed framework. In fact, what should define a specific version is the **P** set of pattern descriptors. This being formed by combinations of the descriptors sSIFT, sDenseSIFT, sBRISK, LPQ, and coALBP. In detail, we will consider 10 different versions referenced by $\mathbf{V}_1, \mathbf{V}_2, \ldots, \mathbf{V}_{10}$ and defined respectively by variations of **P** as shown in Table 2. The idea is to evaluate the execution of the proposed descriptors sSIFT, sDenseSIFT, and sBRISK together with the framework. In addition, two descriptors widely used to detect life in fingerprints, LPQ and coALBP, are considered.
  Not all possible combinations among these five descriptors were considered for reasons of text space, but the most important combinations to analyze the developed material, which are the versions from $\mathbf{V}_1$ to $\mathbf{V}_5$, in which we have representations of **P** with only one element, which makes it possible to evaluate how and how much the framework is enhancing the descriptor's ability to detect life in fingerprint. Still, the other versions should confirm the framework's ability to represent different texture features in the fingerprint image and, consequently, improve its ability to detect life in these images and make the method competitive with the others present in the state-of-the-art.
- **Information aggregation**: In this work, the information aggregation strategy $\mathcal{A}(\cdot)$ will be considered the simplest possible feature fusion routine, which is the concatenation of vectors.



(a) Original image. (b) Otsu binary mask. (c) ROI by Otsu.

(d) Original image. (e) Fisher binary mask. (f) ROI by Fisher.

FIGURE 4. ROI detection of a real fingerprint by Otsu's segmentation techniques, on the top images, and segmentation via Fisher measure analysis and active contour, on the bottom images.

- **Dimensionality reduction**: As it is one of the simplest and most representative techniques in the class of projection methods, the Singular Value Decomposition (SVD) [84] will be used as a function PROJ(·). Specifically, in each version $\mathbf{V}_i$, four dimensions will be evaluated to compose the reduced feature space: 100, 200, 400, and 800.
- **Normalization**: To normalize the feature vectors, four different strategies were used, these being the most common in the problem. Specifically, four different scales were considered for each $\mathbf{V}_i$ version: the Min-Max scale (NORM_1); the standard scale (NORM_2); robust scale (NORM_3); and the non-use of normalization function. Mathematically, considering $\hat{B}_{\text{Train}} := \left\{\hat{v}_{I_1}, \hat{v}_{I_2}, \ldots, \hat{v}_{I_{n_{\text{Train}}}}\right\}$ the basis for training feature vectors in reduced space $\mathbb{R}^m$ and each $\hat{v}_{I_j} = \left(\hat{v}_{I_j,1}, \hat{v}_{I_j,2}, \ldots, \hat{v}_{I_j,m}\right)$, then the four normalization functions are:
  1) Min-Max scale (MM):

$$\text{NORM}_1(x) := \left(\frac{x_1 - \min_j\{\hat{v}_{I_j,1}\}}{\max_j\{\hat{v}_{I_j,1}\} - \min_j\{\hat{v}_{I_j,1}\}}, \ldots, \frac{x_m - \min_j\{\hat{v}_{I_j,m}\}}{\max_j\{\hat{v}_{I_j,m}\} - \min_j\{\hat{v}_{I_j,m}\}}\right);$$

  2) Standard scale:

$$\text{NORM}_2(x) := \left(\frac{x_1 - \mu_1}{\sigma_1}, \ldots, \frac{x_m - \mu_m}{\sigma_m}\right),$$

  where,

$$\mu_i = \sum_{j=1}^{n_{\text{Train}}} \frac{\hat{v}_{I_j,i}}{n_{\text{Train}}},$$

$$\sigma_i = \frac{1}{\sqrt{n_{\text{Train}}}} \sqrt{\sum_{k=1}^{n_{\text{Train}}} \left(\hat{v}_{I_k,i} - \mu_i\right)^2};$$

  3) Robust scale (NORM_3): it is a modification of the standard scale that is robust to outliers. For this, the mean (μ_i) is replaced by the median and the standard deviation (σ_i) by the distance between the first and third quartile of the distribution.
  4) No scale: it is the strategy represented by the identity function. That is, $\text{NORM}_4(x) = x$.
- **Classifier**: To discriminate the feature vectors of each image, a binary classifier of the SVM type with linear kernel was used. It is worth noting that this is one of the most used classification models in the topic addressed.

VI. RESULTS AND EXPERIMENTS

In this section, the necessary experiments must be carried out to evaluate the performance of the proposed advances. For this, a well established benchmark is defined and detailed in Section VI-A. In this case, two situations must be analysed: one involving an internal analysis of the proposed content and another involving an external analysis of it. The first, described in Section VI-B, aims to evaluate the proposed representation for matrix descriptors and for each step of the framework. The second situation, detailed in Section VI-C, was designed to allow the comparison of the proposed material performance to existing techniques in the literature and that make up the state of the art on the topic.

To make possible the comparisons, it is necessary to specify some performance metrics that represent the amounts of error and success of the method with respect to the images of the test bases. In this work, the official metrics of LivDet competitions were used, which are the following [85]:

- *FerrLive* (FL): which represents the rate of real fingerprints classified as fakes.
- *FerrFake* (FF): which represents the percentage of fake fingerprints classified as real.
- *Average Classification Error* (ACE): which is the average between the false positive and false negative rates of the method. Mathematically, $\text{ACE} = \frac{\text{FL} + \text{FF}}{2}$.
- *Accuracy* (ACC): is the rate of correctly classified fingerprints.

All implementations presented in this work were built in Python[1] programming language, more specifically with the use of scikit-learn[2] and OpenCV,[3] on a personal microcomputer equipped with 8 GB of RAM and an Intel (R) Core (TM) i5-4460 of 3.20GHz frequency.

A. BENCHMARK

Having its first edition held in 2009 [86] and organized to take place in odd years, the Fingerprint Liveness Detection (LivDet) competition has been the most representative event on the topic of spoofing detection in biometrics. The main intention of the competition is to bring together solutions at the software level to alleviate the problem and, consequently, promote the development of new methods with greater robustness and greater accuracy in fingerprint spoofing detection.

In each edition of the competition, a group of sensors is used to build pairs of training and testing bases from examples of real and fake fingers. Specifically, each sensor is used to collect fingerprints from a group of users and to conduct the reading of synthetic fingerprints. In this case, the algorithms evaluated in the competition must use only the training portion to define and adjust their method. After the competition, both databases are made available for research and experimentation.

[1] https://www.python.org/
[2] https://scikit-learn.org/
[3] https://opencv.org/

TABLE 3. Details about the real and fake fingerprint image databases of the benchmark formed by the bases presented in the LivDet competitions. DPIs represents the number of dots per inch.

Year	Sensor	Size	DPIs	Train		Test	
				Real	Fake	Real	Fake
2009	Biometrika	312 × 372	569	520	520	1473	1480
	CrossMatch	640 × 780	500	1000	1000	3000	3000
	Identix	720 × 720	686	750	750	2250	2250
2011	Biometrika	312 × 372	500	1000	1000	1000	1000
	Digital	355 × 391	500	1004	1000	1000	1000
	Italdata	640 × 480	500	1000	1000	1000	1000
	Sagem	352 × 384	500	1008	1008	1000	1036
2013	Biometrika	312 × 372	569	1000	1000	1000	1000
	Italdata	640 × 480	500	1000	1000	1000	1000
	Swipe	208 × 1500	96	1221	979	1153	1000
2015	HiScan	1000 × 1000	1000	1000	1000	1000	1500
	CrossMatch	640 × 480	500	1510	1473	1500	1448
	DigitalPersona	252 × 324	500	1000	1000	1000	1500
	GreenBit	500 × 500	500	1000	1000	1000	1500

TABLE 4. Materials used for spoofing construction in the LivDet benchmark for each year of the competition.

2009	2011	2013	2015	
			Train	Test
Play-Doh	Body Double	Body Double	Body Double	Body Double
Silicone	Ecoflex	Ecoflex	Ecoflex	Ecoflex
Gelatine	Silicone	Modasil	Play-Doh	OOMOO
	Latex	Play-Doh	Latex	Play-Doh
	Gelatine	Latex	Woodglue	RTV
	Woodglue	Gelatine		Latex
		Woodglue		Gelatine
				Liquid Ecoflex
				Woodglue

For the experiments carried out in this work, the most recurrent databases in the literature are considered, which are presented in the LivDet editions referring to the years 2009 [86], 2011 [87], 2013 [88] and 2015 [89]. In the Table 3, some details of these databases and the images that compose them are presented. Specifically, the sensors used in each year of edition, the dimensions of the images, and the amounts of real and fake images reserved for training and testing are presented. It is also worth noting that, in the case of the 2013 edition, the CrossMatch sensor was not considered, as it is known that a problem in the acquisition may have affected the quality of the data in this database [21], [88].

For each edition of the LivDet competition, a set of synthetic materials is used to manufacture fake fingerprints. In the first three editions of LivDet, the same materials were used both for the definition of the training set and for the definition of the test set. However, for the 2015 edition, a set of five materials was used for training and a set of nine materials was used for testing. In this case, the intention is to evaluate the generalization capacity of the methods in detecting spoofing of materials different from those used to define your model. In detail, in Table 4, the materials used in each edition of LivDet are listed.

B. PERFORMANCE ANALYSIS BY CONFIGURATION

All the considered versions of the proposed framework configurations, including its 16 variations depending on the 4 normalization strategies and the 4 possible amounts of feature vector coordinates obtained by the projection technique,

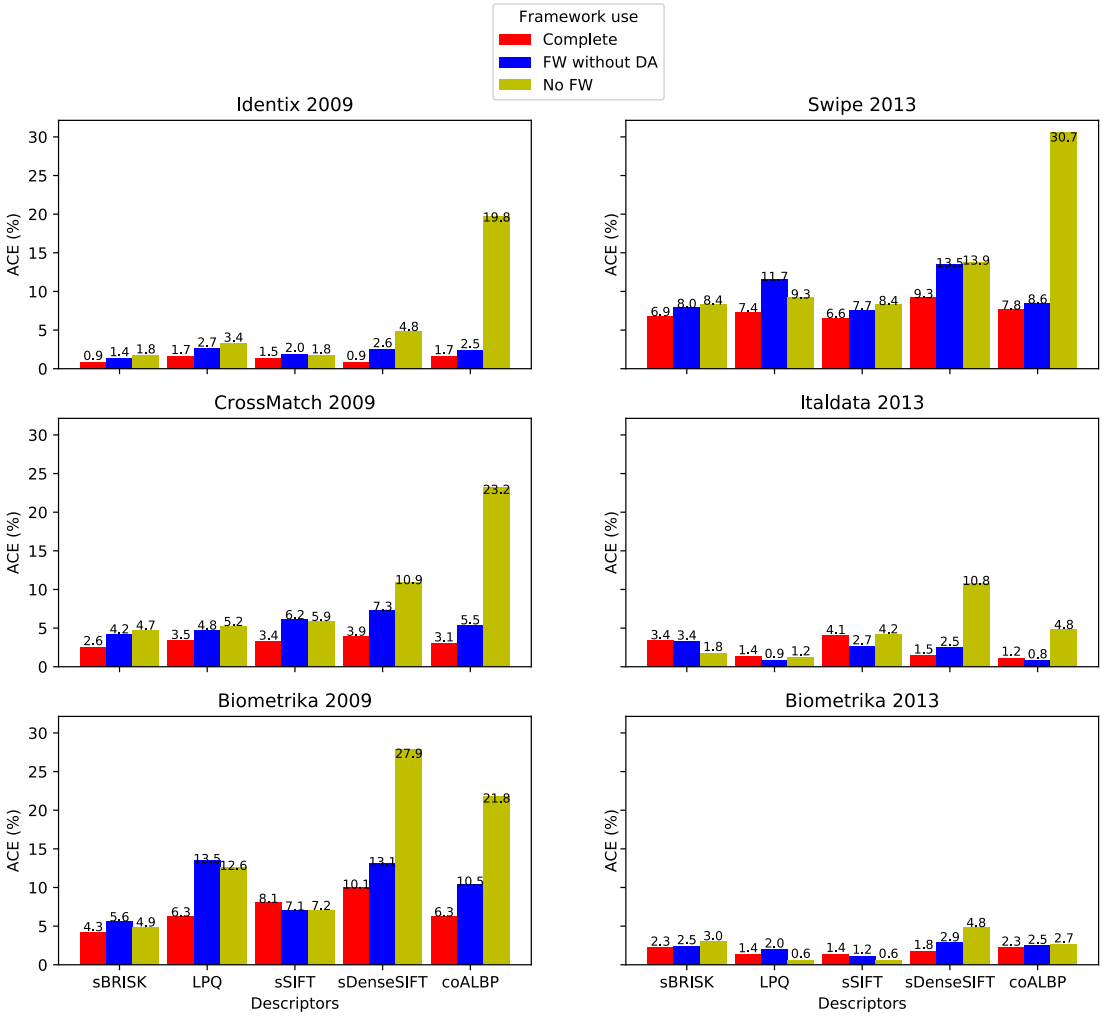


FIGURE 5. Comparison between ACE, in percentage, for the sensors of the LivDet competitions of the 2009 editions, on the left, and 2013, on the right. The descriptor used by each technique is highlighted on the lower axis of each graph. To create the results represented by the blue and red bars, only the best accuracy values were considered among the variations of each version for normalization and projection functions.

were evaluated on the 14 sensors of the used benchmark. This resulted in the creation of 140 tables with detailed information on all FL, FF, ACE, and ACC metrics regarding each sensor and each version of the framework. Since all these tables are presented in the supplementary material to this work and, in the following paragraphs, some analyzes are conducted based on clippings of these results.

To start the experiments, the impact of using the proposed framework on the considered descriptors will be analyzed. Thus, it will be possible to verify the influence of the main steps of the framework in improving the image representation capacity in each of the evaluated descriptors. For this, in each of the versions $\mathbf{V}_1$ to $\mathbf{V}_5$, three variations of the framework are analyzed: one containing all the steps described and configured according to the V; one that does not have the data augmentation step; and one that does not have any step of the proposed framework, consisting only of the pattern extracted by the descriptor and whose classification model is based on the training of a linear SVM. In Figures 5 and 6, a bar chart is presented with the ACE measurements, in percentage, of each of the evaluated methods, with the red bars referring to the techniques that use all the steps of the framework, the blue bars refer to techniques that do not only use the data augmentation step, and the yellow bars refer to the original techniques without using the proposed framework. In the case of the first two variations of techniques, as several projection dimensions and normalization functions are analyzed in the framework configuration, the best result presented by the technique is evaluated.

Observing the results presented in Figures 5 and 6, some interesting facts can be noticed. In detail, the following stand out:

- In most cases, the ACE is higher when no step of the framework is used. Thus, it is clear that the framework enhances the ability to represent the fingerprint image to facilitate the detection of life. As an example, the representation of coALBP stands out, which became competitive with the use of the framework. Furthermore,

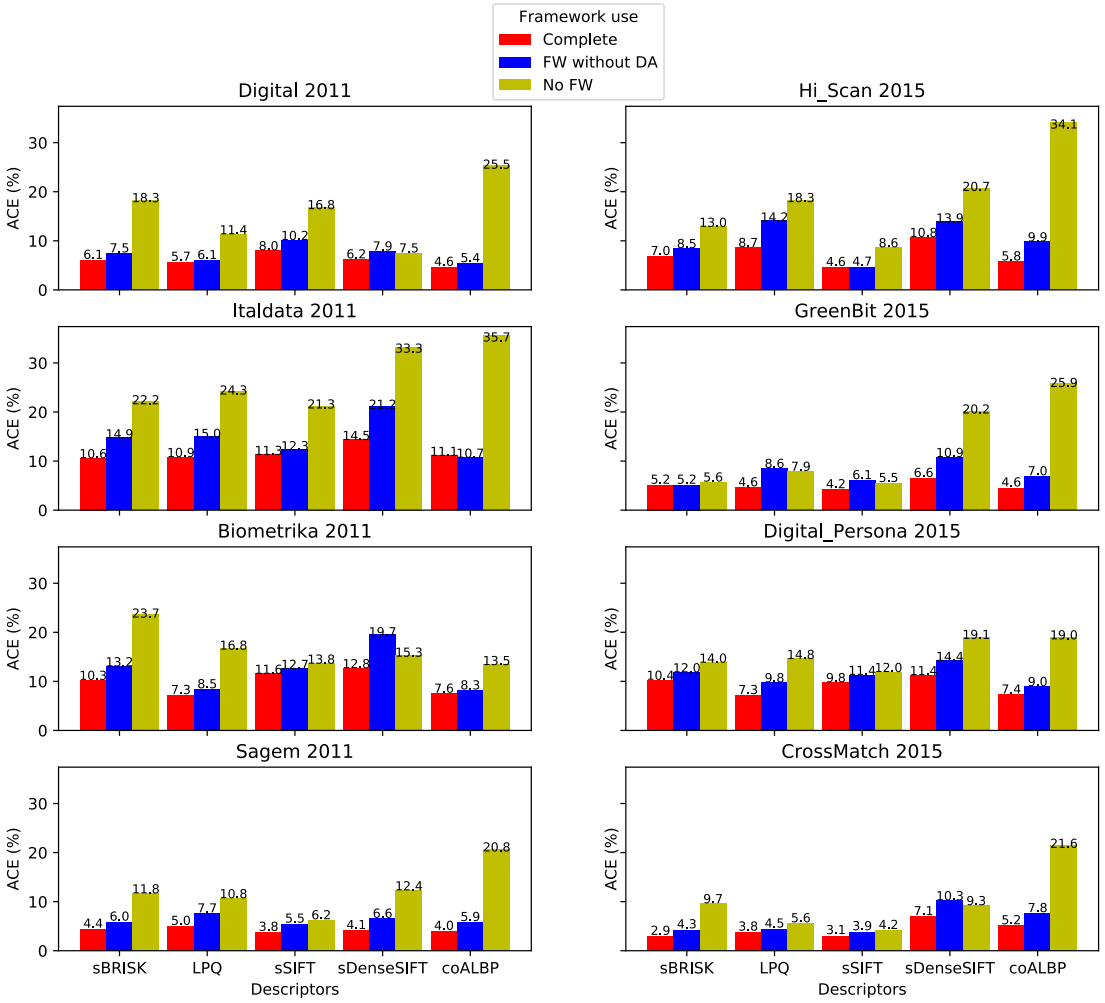


FIGURE 6. Comparison between ACE, in percentage, for the sensors of the LivDet competitions of the 2011 editions, on the left, and 2015, on the right. The descriptor used by each technique is highlighted on the lower axis of each graph. To create the results represented by the blue and red bars, only the best accuracy values were considered among the variations of each version for normalization and projection functions.

as can be seen in the case of LivDet 2009's Identix sensor, the ACE of the coALBP, which originally corresponds to 19.8%, now corresponds to 1.7%, which is less than 10% of the original value.

- The use of the framework improved the classification accuracy for most cases. Only in four situations out of the 70 evaluated, the framework did the classification result worst: in the case of the sSIFT descriptor in the representation of Biometrika images from the LivDet 2009 and 2013; and in the case of the LPQ descriptor for the images of the Italdata and Biometrika sensors from the LivDet 2013. However, in all these cases, the addition of ACE corresponds to values below 1%. A similar analysis can be obtained regarding the use of the framework without the data augmentation step whose results are represented by the blue bars in the images.
- The data augmentation step proved to be very efficient in most of the considered cases, since there is a tendency that the red bars represent lower ACE values than those represented by the blue bars, which, in turn, represent lower values of the ACE than the values of the yellow bars. In other words, there is a tendency that all stages of the framework should be used for the greatest performance gain. In addition, we can see that the data augmentation step is effective in improving the accuracy in detecting life in fingerprints. This indicates that there may be a sampling deficiency in most of the image bases of the benchmark.
- The use of representation by mappings as proposed in Section III proved to be competitive in the cases of SIFT and DenseSIFT descriptors for its original representation investigated by Gragnaniello et al. [29]. The results obtained with the use of the proposed framework were, on average, superior to those obtained with the visual vocabulary representation of words. This indicates that the use of the proposed steps, even if configured by simple strategies, can considerably enhance the ability to represent images by pattern descriptors and,

TABLE 5. Results for the sensors referring to LivDet 2009. The used normalization is represented by: "Rob" for robust, "Std" for standard, "MM" for max-min and "UnS" when no normalization is used. The average accuracy and the average error considering all sensors are represented respectively by μ (ACC) and μ (ACE). In bold, the best accuracy value is represented with respect to all analyzed versions for the case of a particular sensor or for the average case.

Sensor	Measure	$\mathbf{V}_1$	$\mathbf{V}_2$	$\mathbf{V}_3$	$\mathbf{V}_4$	$\mathbf{V}_5$	$\mathbf{V}_6$	$\mathbf{V}_7$	$\mathbf{V}_8$	$\mathbf{V}_9$	$\mathbf{V}_{10}$
Identix	ACC	99.16	98.36	98.60	99.16	98.38	99.18	99.76	99.69	**99.83**	99.74
	ACE	0.85	1.65	1.41	0.85	1.63	0.83	0.25	0.32	0.18	0.27
	Dimension	800	800	400	800	800	100	200	800	400	800
	Normalization	Rob	Rob	Rob	Rob	Rob	MM	UnS	Rob	UnS	Rob
CrossMatch	ACC	97.42	96.57	96.67	96.12	96.90	98.82	98.82	98.85	98.92	**99.10**
	ACE	2.59	3.44	3.34	3.89	3.10	1.19	1.19	1.16	1.09	0.91
	Dimension	800	800	800	800	800	800	800	800	800	400
	Normalization	Rob	Rob	UnS	UnS	Rob	Rob	Rob	Rob	Rob	Rob
Biometrika	ACC	95.77	93.77	91.91	89.98	93.77	91.34	92.11	96.38	97.87	**99.60**
	ACE	4.24	6.24	8.09	10.02	6.25	8.69	7.91	3.62	2.13	0.41
	Dimension	400	200	100	800	800	200	200	800	400	400
	Normalization	UnS	Rob	Std	Rob	Rob	Rob	Rob	Rob	Rob	Rob
μ (ACC)		97.45	96.24	95.73	95.09	96.35	96.45	96.90	98.31	98.87	**99.48**
μ (ACE)		2.56	3.78	4.28	4.92	3.66	3.57	3.12	1.70	1.14	0.53

TABLE 6. Results for the sensors referring to LivDet 2011. The used normalization is represented by: "Rob" for robust, "Std" for standard, "MM" for max-min and "UnS" when no normalization is used. The average accuracy and the average error considering all sensors are represented respectively by μ (ACC) and μ (ACE). In bold, the best accuracy value is represented with respect to all analyzed versions for the case of a particular sensor or for the average case.

Sensor	Measure	$\mathbf{V}_1$	$\mathbf{V}_2$	$\mathbf{V}_3$	$\mathbf{V}_4$	$\mathbf{V}_5$	$\mathbf{V}_6$	$\mathbf{V}_7$	$\mathbf{V}_8$	$\mathbf{V}_9$	$\mathbf{V}_{10}$
Digital	ACC	93.90	94.30	92.05	93.80	95.40	95.65	95.65	**97.50**	97.20	97.40
	ACE	6.10	5.70	7.95	6.20	4.60	4.35	4.35	2.50	2.80	2.60
	Dimension	800	800	800	800	800	800	800	800	800	800
	Normalization	UnS	Rob	UnS	UnS	Rob	Rob	Rob	Rob	Rob	Rob
Italdata	ACC	89.40	89.15	88.70	85.50	88.90	88.80	91.30	91.95	92.35	**93.50**
	ACE	10.60	10.85	11.30	14.50	11.10	11.20	8.70	8.06	7.65	6.50
	Dimension	800	800	800	800	800	800	400	800	800	200
	Normalization	UnS	Rob	MM	Rob	MM	MM	Rob	MM	Rob	MM
Biometrika	ACC	89.70	92.75	88.40	87.20	92.45	88.50	**93.20**	92.60	93.00	91.65
	ACE	10.30	7.25	11.60	12.80	7.55	11.50	6.80	7.40	7.00	8.35
	Dimension	800	800	800	800	400	400	800	800	800	800
	Normalization	Rob	Rob	Rob	UnS	Rob	MM	UnS	Rob	Rob	Rob
Sagem	ACC	95.63	95.04	96.32	95.88	96.08	96.22	97.06	**98.24**	97.75	97.50
	ACE	4.40	5.00	3.71	4.10	3.93	3.80	2.95	1.78	2.28	2.51
	Dimension	800	400	800	800	800	800	400	800	400	400
	Normalization	Rob	Rob	UnS	Rob	Rob	Rob	MM	Rob	UnS	MM
μ (ACC)		92.16	92.81	91.37	90.60	93.21	92.30	94.31	**95.08**	**95.08**	95.02
μ (ACE)		7.85	7.20	8.64	9.40	6.80	7.72	5.70	4.94	4.94	4.99

consequently, make these descriptors competitive for the problem.

Next, the performances of the proposed framework versions are compared. Thus, in the Tables 5, 6, 7 and 8, the performance of each version with respect to the sensors of the LivDet 2009, LivDet 2011, LivDet 2013 and LivDet 2015. In each table, each version is presented: in "ACC", the best ACC obtained value by the version for each sensor; in "ACE", the best ACE obtained value by the version for each sensor; in "Dimension", the feature vector dimension in which the analyzed version reached the best ACC value; and, in "Normalization", the normalization strategy used in which the analyzed version reached the best ACC value.

We can see that all evaluated versions have an average accuracy of over 90% in all editions of LivDet. Furthermore, the ACE of all versions is below 15% for any specific sensor, as can be seen in the summary illustrated in Figures 7 and 8. In these, it is possible to detect a trend of performance improvement in versions that are defined by sets **P** with more elements. Visually, note that the bars referring to the ACEs of versions $\mathbf{V}_7$, $\mathbf{V}_8$, $\mathbf{V}_9$ and $\mathbf{V}_{10}$ are smaller than those presented by the other versions in most of the bases. Specifically, $\mathbf{V}_7$ has the best accuracy value in 1 sensor; $\mathbf{V}_8$ presents the best accuracy value in 3 sensors; $\mathbf{V}_9$ presents the best accuracy value in 4 sensors; and $\mathbf{V}_{10}$ presents the best accuracy value in 6 sensors. This fact helps to confirm the veracity of the framework's foundation in the sense that the more pattern descriptors used in **P**, the greater the image representation capacity, since each descriptor has a certain ability to represent information. However, the difference in

TABLE 7. Results for the sensors referring to LivDet 2013. The used normalization is represented by: "Rob" for robust, "Std" for standard, "MM" for max-min and "UnS" when no normalization is used. The average accuracy and the average error considering all sensors are represented respectively by μ (ACC) and μ (ACE). In bold, the best accuracy value is represented with respect to all analyzed versions for the case of a particular sensor or for the average case.

Sensor	Measure	$\mathbf{V}_1$	$\mathbf{V}_2$	$\mathbf{V}_3$	$\mathbf{V}_4$	$\mathbf{V}_5$	$\mathbf{V}_6$	$\mathbf{V}_7$	$\mathbf{V}_8$	$\mathbf{V}_9$	$\mathbf{V}_{10}$
Swipe	ACC	93.12	92.95	93.67	91.04	92.67	92.53	93.22	94.07	**94.81**	93.43
	ACE	6.83	7.35	6.58	9.27	7.71	7.98	6.69	5.88	5.14	6.49
	Dimension	800	800	800	800	400	800	400	400	400	400
	Normalization	UnS	Rob	UnS	UnS	MM	Rob	MM	Rob	UnS	MM
Italdata	ACC	96.60	98.65	95.90	98.55	98.85	99.80	99.75	99.20	99.25	**99.85**
	ACE	3.40	1.35	4.10	1.45	1.15	0.20	0.25	0.80	0.75	0.16
	Dimension	100	400	200	800	400	100	100	100	800	800
	Normalization	UnS	Std	UnS	UnS	Std	MM	MM	UnS	Rob	Rob
Biometrika	ACC	97.75	98.65	98.60	98.20	97.75	98.85	99.05	99.30	**99.65**	99.25
	ACE	2.25	1.35	1.40	1.80	2.25	1.15	0.95	0.70	0.35	0.75
	Dimension	400	800	200	800	200	100	200	400	100	400
	Normalization	UnS	Rob	Rob	Rob	Rob	MM	Rob	Rob	UnS	Rob
μ (ACC)		95.83	96.75	96.06	95.93	96.43	97.06	97.34	97.53	**97.91**	97.51
μ (ACE)		4.16	3.35	4.03	4.18	3.71	3.11	2.63	2.46	2.08	2.47

TABLE 8. Results for the sensors referring to LivDet 2015. The used normalization is represented by: "Rob" for robust, "Std" for standard, "MM" for max-min and "UnS" when no normalization is used. The average accuracy and the average error considering all sensors are represented respectively by μ (ACC) and μ (ACE). In bold, the best accuracy value is represented with respect to all analyzed versions for the case of a particular sensor or for the average case.

Sensor	Measure	$\mathbf{V}_1$	$\mathbf{V}_2$	$\mathbf{V}_3$	$\mathbf{V}_4$	$\mathbf{V}_5$	$\mathbf{V}_6$	$\mathbf{V}_7$	$\mathbf{V}_8$	$\mathbf{V}_9$	$\mathbf{V}_{10}$
HiScan	ACC	93.52	92.24	96.20	89.92	94.64	96.84	97.96	97.12	97.16	**97.88**
	ACE	6.92	8.65	4.57	10.80	5.79	3.10	2.07	2.97	3.02	2.07
	Dimension	800	800	800	800	800	400	800	400	800	400
	Normalization	UnS	UnS	Rob	Rob	Rob	Rob	Rob	Rob	Rob	Rob
GreenBit	ACC	94.88	95.52	96.04	93.72	95.48	98.36	98.00	97.44	98.60	**99.04**
	ACE	5.12	4.57	4.16	6.57	4.54	1.70	1.92	2.47	1.37	0.92
	Dimension	800	400	800	800	800	200	200	800	800	400
	Normalization	MM	MM	UnS	Rob	Rob	Rob	MM	UnS	UnS	UnS
DigitalPersona	ACC	89.96	92.92	90.72	88.52	92.96	91.04	89.61	93.60	**95.04**	94.24
	ACE	10.32	7.25	9.81	11.32	7.37	9.17	10.75	6.77	5.35	6.10
	Dimension	800	800	800	800	400	400	800	400	800	800
	Normalization	Rob	Rob	Rob	Rob	Rob	Rob	Rob	Rob	Rob	Rob
CrossMatch	ACC	97.19	96.24	97.02	93.02	94.95	96.88	98.78	**99.33**	99.22	99.06
	ACE	2.86	3.77	3.02	7.07	5.13	3.16	1.24	0.69	0.80	0.97
	Dimension	800	800	800	800	800	100	400	800	800	800
	Normalization	UnS	UnS	Rob	Rob	Rob	MM	MM	Rob	UnS	Rob
μ (ACC)		93.89	94.23	95.00	91.30	94.51	95.78	96.09	96.88	97.51	**97.56**
μ (ACE)		6.31	6.06	5.39	8.94	5.71	4.28	4.00	3.23	2.64	2.52

average accuracy obtained by these versions is not very significant, since, for the sensors of the LivDet 2009, 2011, 2013, and 2015, this difference is, respectively, 2.58%, 0.77%, 0.57%, and 1.47%. Furthermore, we can note that the versions from $\mathbf{V}_1$ to $\mathbf{V}_5$, which are defined by only one descriptor, presented competitive results with each other for most of the evaluated bases. In particular, the proposed sBRISK, sSIFT, and sDenseSIFT, used to compose the versions $\mathbf{V}_1$, $\mathbf{V}_3$ and $\mathbf{V}_4$, respectively, presented similar performance to the $\mathbf{V}_2$ and $\mathbf{V}_5$, defined, respectively, by the well-established LPQ and coALBP, which proves their effectiveness in representing textures for the problem.

Regarding the normalization and dimensionality reduction strategies, we can also notice a trend in the results. In this case, we can see that the robust normalization strategy, or NORM_3, is the most efficient in most bases. In fact, according to Figure 9a, this scaling strategy is what helps most versions to reach the best accuracy value considering the bases of all years of the LivDet competition. This indicates that most image bases have examples that are represented in a discrepant way from the others, which configures the presence of outliers, and that, therefore, need a normalization that is little influenced by these examples. Similarly, the use of 800 dimensions for the latent representation of the feature vector proved to be more efficient for most versions considered in most bases. In this case, as shown in Figure 9b, the greater the number of used coordinates, the greater the chance that the version will assume the best accuracy value.

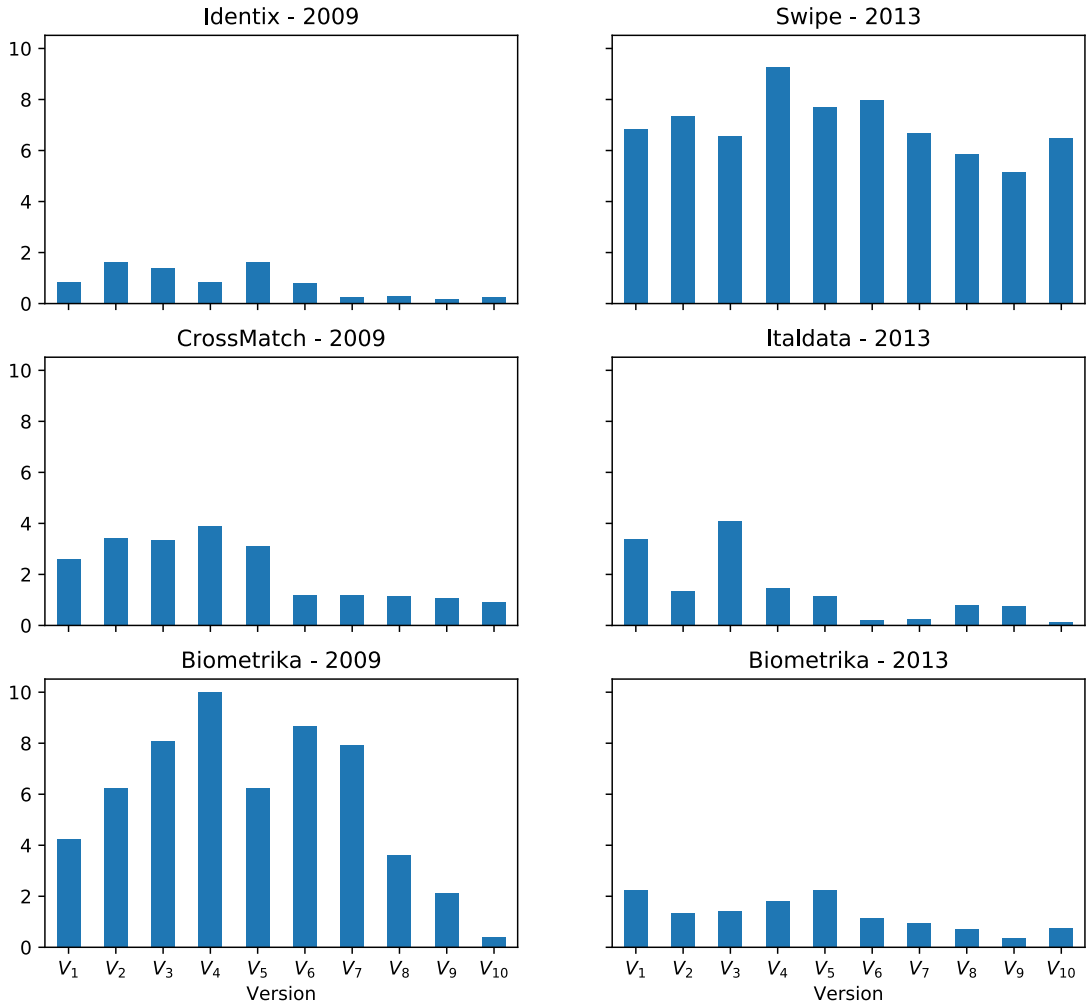


FIGURE 7. Illustration in bar-chart of the ACE measure, in percentage, presented by the considered versions of the proposed material, specified in Table 2, with respect to LivDet from the years 2009 and 2013. In the representation, it is possible to observe that the versions that consider a greater number of descriptors are those that present a lower error value.

Thus, projections in latent spaces with very small dimensions can compromise the representation of the feature vector in this problem.

Evaluations were also carried out considering situations in which the sensors used to collect the images that make up the training base are different from the sensor used to collect the images from the test base. This test situation seeks to demonstrate the generalizability of a fingerprint liveness detection method since the training is done with respect to one sensor and the test is done with respect to another. In addition, according to Table 4, this situation also evaluates the performance of the method on different sets of synthetic materials used to make the spoofings. Specifically, the sensors used to build the ''Biometrika'' and ''Italdata'' bases for the LivDet 2011 and LivDet 2013 were considered, totaling four base pairs. It is known [88] that the fingerprint spoofing images from the 2011 databases have better quality than the same category images from 2013. Thus, three main test scenarios are defined: the worst scenario, in which the versions are trained using the 2013 bases and evaluated on the 2011 bases; the medium scenario, in which the versions are trained using the 2013 bases and are evaluated on the 2011 bases; and the best scenario, in which the training and testing bases are from the same edition of the competition. In Table 9, the performance of all considered versions of the proposed framework is summarized.

We can see that the worst ACC of considered versions occurs in the worst scenario. For example, the version $\mathbf{V}_3$, even analyzing all its variations for the normalization and dimensionality reduction functions, was able to correctly classify only 49.95% of the images from the Italdata 2011 database when trained by the Italdata 2013 database. Something similar occurs when we consider the different editions of Biometrika. In these two situations, all the analyzed versions have an accuracy close to 50%, which corresponds to poor performance and which serves as evidence for the fact that the proposed method needs good-quality images to correctly represent spoofings. At the same time, in the

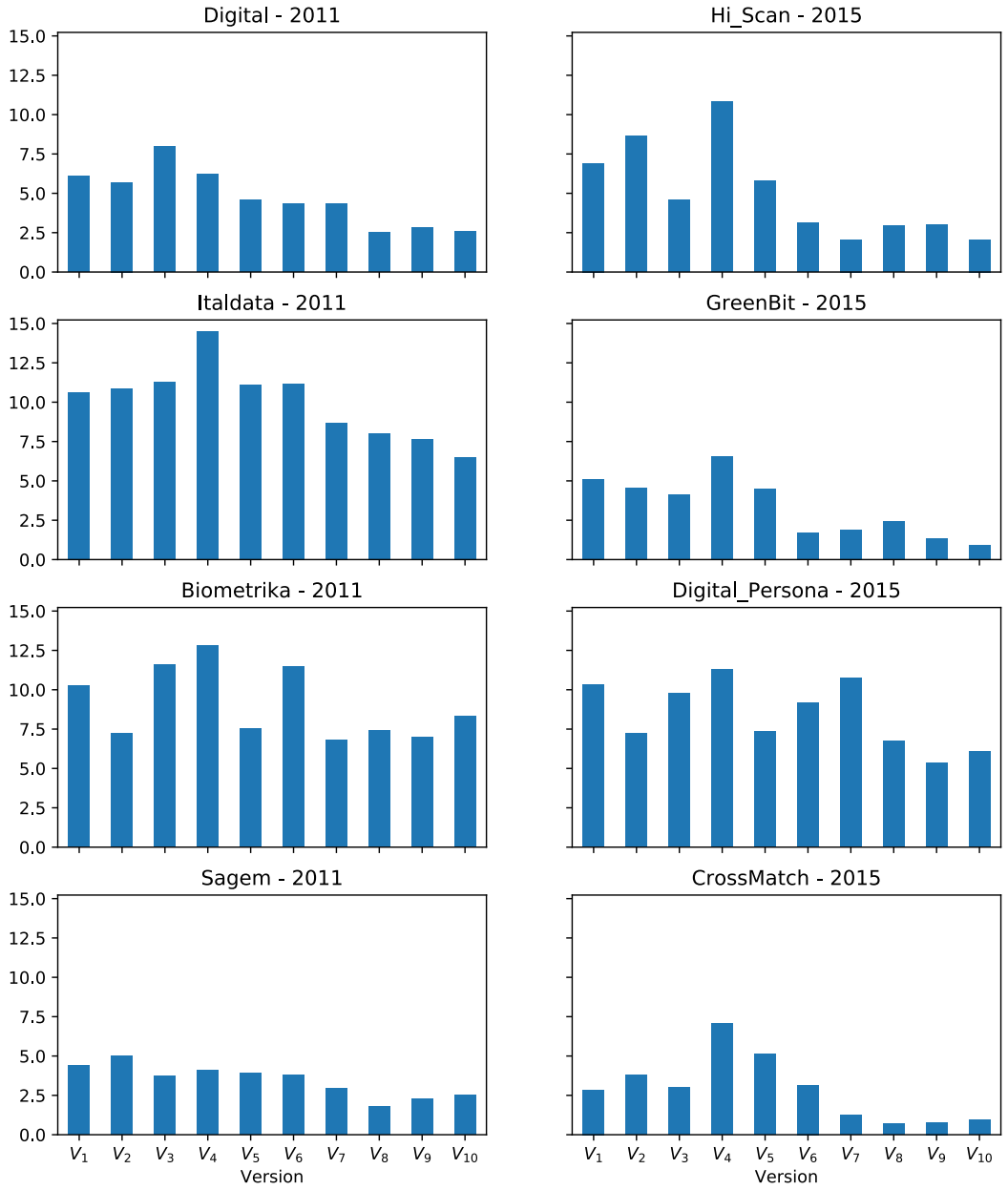


FIGURE 8. Illustration in bar-chart of the ACE measure, in percentage, presented by the considered versions of the proposed material, specified in Table 2, with respect to LivDet from the years 2011 and 2015. In the representation, it is possible to observe that the versions that consider a greater number of descriptors are those that present a lower error value.

medium-difficulty scenario, the proposed material worked reasonably well. In detail, in the case where the base used for training was the Biometrika 2011 and the base used for testing was the Biometrika 2013, all versions presented ACC greater than 70%. Half of the analyzed versions had ACC greater than 90%. Similar results can be detected when the Italdata 2011 is used for training and the Italdata 2013 is used for testing. This suggests that the proposed method can generalize well when training is performed on a base of good quality images and using the same sensor. In fact, in cases where the images used for training and testing are of good quality, belonging to the 2011 edition, but are collected by different sensors, most of the analyzed versions of the proposed method also have difficulty in correctly classifying the images. However, some versions present reasonable performance in this situation, as is the case of the $\mathbf{V}_5$ and $\mathbf{V}_7$, which have an accuracy greater than 80% when trained with the Biometrika base and evaluated on the Italdata base, both from 2011, and $\mathbf{V}_6$ and $\mathbf{V}_7$ which also present an accuracy greater than 80% when trained with the Italdata and evaluated on the Biometrika. Finally, all the considered versions presented satisfactory performance, with ACC between

TABLE 9. Classification results for cross sensors, following the notation "Training sensor × Test sensor". The used normalization is represented by: "Rob" for the robust, "Std" for the standard, "MM" for the max-min and "UnS" when no normalization is used. The average ACC and the average ACE considering all sensors are represented respectively by μ (ACC) and μ (ACE).

Sensors	Measure	$\mathbf{V}_1$	$\mathbf{V}_2$	$\mathbf{V}_3$	$\mathbf{V}_4$	$\mathbf{V}_5$	$\mathbf{V}_6$	$\mathbf{V}_7$	$\mathbf{V}_8$	$\mathbf{V}_9$	$\mathbf{V}_{10}$
Bio 11 x Bio 13	ACC	71.20	87.50	90.45	75.85	91.60	90.45	74.80	90.75	88.90	90.50
	ACE	28.80	12.50	9.56	24.15	8.40	9.56	25.20	9.25	11.10	9.50
	Dimension	200	800	800	800	400	400	100	100	400	200
	Normalization	MM	UnS	Rob	UnS	Std	Std	Std	MM	Std	Std
Bio 13 x Bio 11	ACC	54.20	53.70	54.05	52.20	52.75	51.05	51.30	51.55	51.70	50.85
	ACE	45.80	46.30	45.95	47.80	47.25	48.95	48.70	48.45	48.30	49.15
	Dimension	400	400	100	100	200	100	400	100	100	100
	Normalization	Rob	Std	MM	MM	Rob	Rob	Rob	Rob	Rob	MM
Ita 11 x Ita 13	ACC	84.25	85.30	82.75	82.60	93.35	90.10	83.65	82.15	82.65	90.30
	ACE	15.75	14.70	17.25	17.40	6.65	9.90	16.36	17.86	17.36	9.70
	Dimension	100	800	800	400	100	100	100	800	800	200
	Normalization	Std	UnS	UnS	Rob	Rob	Std	Rob	Rob	UnS	Std
Ita 13 x Ita 11	ACC	54.30	56.45	49.95	51.05	54.30	55.01	53.30	53.45	51.50	52.10
	ACE	45.70	43.55	50.05	48.95	45.70	45.00	46.70	46.55	48.50	47.90
	Dimension	100	400	100	100	200	100	100	100	100	100
	Normalization	Std	Std	MM	Std	MM	MM	Std	Std	Std	MM
Bio 11 x Ita 11	ACC	57.25	59.55	78.55	53.41	82.20	78.61	86.45	58.85	75.00	75.60
	ACE	42.75	40.46	21.46	46.60	17.80	21.40	13.55	41.15	25.00	24.40
	Dimension	800	400	100	400	100	800	800	100	400	200
	Normalization	Rob	Rob	Rob	UnS	UnS	UnS	UnS	UnS	UnS	Rob
Ita 11 x Bio 11	ACC	65.65	69.16	76.35	51.95	74.91	85.55	82.90	72.66	64.41	81.20
	ACE	34.35	30.85	23.65	48.05	25.10	14.45	17.11	27.35	35.60	18.80
	Dimension	800	400	100	100	200	100	200	800	100	100
	Normalization	UnS	Rob	Std	MM	UnS	UnS	Std	Std	Std	Std
Bio 13 x Ita 13	ACC	89.00	88.15	98.15	85.55	91.75	96.95	98.30	94.25	89.61	98.70
	ACE	11.00	11.85	1.85	14.45	8.25	3.05	1.70	5.75	10.40	1.30
	Dimension	800	800	400	100	800	100	200	100	100	400
	Normalization	Rob	Rob	UnS	Std	Rob	Rob	Rob	Std	Std	MM
Ita 13 x Bio 13	ACC	94.40	97.35	97.90	93.45	96.90	97.55	98.65	99.15	99.10	99.15
	ACE	5.60	2.65	2.10	6.55	3.10	2.46	1.35	0.85	0.90	0.85
	Dimension	100	100	400	100	100	100	200	400	200	100
	Normalization	Std	Std	Rob	Std	Std	Std	Std	Rob	Rob	Std
μ (ACC)		71.29	74.65	78.52	68.26	79.72	80.66	78.67	75.36	75.36	79.80
μ (ACE)		28.72	25.36	21.49	31.75	20.29	19.35	21.34	24.65	24.65	20.21

89% and 99.15%, in cases where the training and test bases are composed of spoofing images of poor quality with different sensors, which demonstrates the generalization capacity of the proposed method when the spoofing strategy is the same, even if different sensors are used.

C. COMPARISON WITH THE STATE OF THE ART

In order to validate the scientific advance in the problem, comparisons are made between the results obtained by the proposed material and by methods that make up the state of the art of fingerprint liveness detection solutions. Specifically, the best values of the ACC and ACE are presented considering all versions of the proposed framework that were addressed in Section VI-B and these values are compared with the results presented by the methods gathered in Table 1. Thus, in the Tables 10, 11, 12 and 13 these results are summarized according to the sensors of LivDet competitions from the years 2009, 2011, 2013 and 2015, respectively. These tables contain information on the ACC and/or ACE, when existing in the original works for each technique. The best value of these metrics regarding the techniques submitted for evaluation in each year of the competition is also presented. Such values are represented by the ''Best on LivDet'' indicator.

According to the values in Table 10, we can see that most current techniques present a satisfactory performance on all 2009 bases, since they classify more than 90% of the images correctly and/or rate less than 10% of images wrongly. Even so, the results of the proposed material stand out, corresponding to accuracies greater than 99% in all cases. In fact, only the CNN-VGG technique presents an ACE value of 0.31% lower than that presented by the proposal in the case of the CrossMatch sensor. However, the proposal presents the lowest average ACE, equivalent to 0.5%, which is less than 1/3 of the average ACE presented by CNN-VGG.

The proposal also presents high ACC, above 90%, for the bases of the LivDet 2011, which corresponds to a competitive performance. In this case, among the thirteen considered techniques, only two presented a higher average ACC and only four presented an average ACE lower than the same

TABLE 10. Comparison with the state of the art for the LivDet 2009 database. ACC and ACE values are given in percentage. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen in the column.

Method	Sensor						Average	
	Identix		CrossMatch		Biometrika			
	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE
Proposed	***99.83***	***0.18***	***99.10***	0.91	***99.60***	***0.41***	***99.51***	***0.50***
IFPAD	96.80	1.60	95.20	4.86	90.30	6.24	94.10	4.23
HyFiPAD	96.90	-	97.20	-	95.30	-	96.44	4.11
Linear SN6400	-	1.71	-	3.35	-	6.53	-	3.86
DCNNGA	-	8.91	-	2.98	-	2.67	-	4.85
FLDNet	-	3.36	-	2.95	-	11.99	-	6.10
DRN	-	5.71	-	4.43	-	25.34	-	11.83
CNN-VGG	-	0.20	-	***0.60***	-	4.10	-	1.63
CNN-AlexNet	-	0.40	-	1.10	-	5.60	-	2.37
CNN-Random	-	0.80	-	1.70	-	9.20	-	3.90
Best on LivDet	-	2.75	-	9.40	-	18.15	-	10.10

TABLE 11. Comparison with the state of the art for the LivDet 2011 database. ACC and ACE values are given in percentage. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen in the column.

Method	Sensor								Average	
	Digital		Italdata		Biometrika		Sagem			
	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE
Proposed	97.50	2.50	93.50	6.50	93.20	6.80	98.24	1.78	95.61	4.40
DEHFF	-	**2.10**	-	8.70	-	**3.35**	-	1.87	**95.99**	**4.01**
CEDD	-	3.71	-	10.93	-	**4.78**	-	2.15	-	5.39
IFPAD	96.10	***1.81***	**95.01**	**5.77**	92.40	**4.85**	96.81	2.92	95.08	**3.84**
HyFiPAD	97.30	-	***97.18***	**-**	***94.18***	-	96.90	-	***96.39***	***3.19***
Linear SN6400	-	2.95	-	**5.85**	**-**	***3.05***	-	3.87	-	**3.93**
PCNN	-	**2.10**	-	11.00	-	7.60	-	2.50	-	5.65
FGFF	97.40	2.60	**95.30**	**4.70**	89.00	11.00	***99.90***	***0.10***	95.40	4.60
DRNN	***97.80***	**1.90**	85.05	11.00	90.30	7.60	95.33	**1.72**	94.35	5.56
WLBD	-	4.10	-	11.85	-	**5.65**	-	2.25	-	5.96
Q-FFF	-	4.00	-	11.15	-	**4.50**	-	**1.47**	-	5.28
coALBP+GF	96.35	-	91.10	-	95.15	**-**	94.70	**-**	94.33	-
DCNNGA	-	5.95	-	12.25	-	7.70	-	5.12	-	7.76
Best on LivDet	-	8.90	-	***2.80***	-	20.00	-	13.45	-	11.29

TABLE 12. Comparison with the state of the art for the LivDet 2013 database. ACC and ACE values are given in percentage. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen in the column.

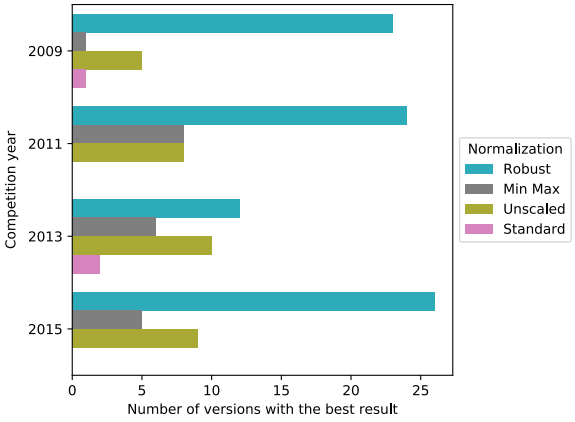
Method	Sensor						Average	
	Swipe		Italdata		Biometrika			
	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE
Proposed	94.81	5.14	***99.85***	***0.16***	99.65	0.35	98.10	1.88
DEHFF	-	**3.95**	-	0.60	-	0.60	***98.28***	**1.72**
CEDD	-	**3.56**	-	0.77	-	0.38	-	**1.57**
IFPAD	**97.81**	**4.85**	95.90	1.18	94.62	2.46	96.11	2.83
HyFiPAD	**97.20**	-	97.10	-	96.25	-	96.85	2.88
Linear SN6400	-	**4.62**	-	3.50	-	2.50	-	3.54
PCNN	-	***0.74***	-	0.85	-	2.00	-	**1.20**
WLBD	-	**4.31**	-	0.95	-	0.40	-	1.89
Q-FFF	-	**3.50**	-	1.20	-	1.30	-	2.00
coALBP+GF	**96.30**	**-**	***99.85***	-	98.10	-	98.08	-
DCNNGA	-	10.74	-	2.00	-	2.70	-	5.15
FGFF	***97.90***	**2.70**	96.60	5.10	***99.90***	***0.10***	98.13	2.63
DRNN	94.57	***0.74***	97.35	1.35	92.60	1.45	97.04	***1.18***
ULBP	-	14.35	-	13.70	-	10.68	-	12.91
Best on LivDet	**96.47**	-	99.40	-	98.30	-	98.06	-

values presented by the proposed material. Furthermore, the average ACC of the proposed technique, which is 95.61%, is 0.78% less than the best observed, which is 96.39%.

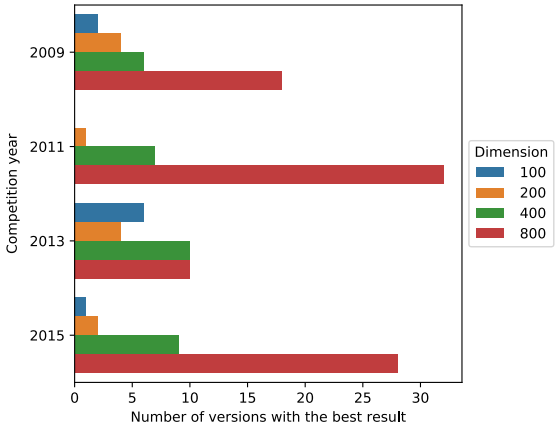
Analyzing the results for the LivDet 2013, we note that the proposal presents a lower performance compared to most other techniques for the Swipe. In detail, the technique's ACC differs by 3.09% from the best observed ACC and the technique's ACE differs by 4.40% from the best observed ACE value. However, the proposed material achieves the best ACC and ACE for the Italdata sensor and the second best value for

TABLE 13. Comparison with the state of the art for the LivDet 2015 database. ACC and ACE values are given in percentage. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen in the column.

Method	Sensor								Average	
	HiScan		GreenBit		DigitalPersona		CrossMatch			
	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE	ACC	ACE
Proposed	97.96	2.07	***99.04***	***0.92***	95.04	***5.35***	99.33	0.69	***97.84***	***2.26***
DEHFF	-	2.61	-	3.43	-	8.82	-	3.45	95.42	4.58
CEDD	-	7.61	-	4.78	-	9.60	-	9.55	-	7.89
HyFiPAD	95.50	-	96.70	-	***97.20***	-	95.00	-	96.10	3.19
Linear SN6400	-	8.48	-	4.87	-	5.62	-	3.34	-	5.58
FGFF	***99.20***	***1.60***	95.30	6.20	92.40	8.20	***99.90***	***0.10***	96.70	4.03
DRNN	93.04	5.56	91.10	4.77	91.96	6.80	96.47	3.46	94.68	5.15
WLBD	-	9.64	-	4.53	-	13.72	-	10.82	-	9.68
DCNNGA	-	6.15	-	2.32	-	7.20	-	4.71	-	5.10
Q-FFF	96.40	-	97.37	-	91.00	-	96.73	-	95.38	-
coALBP+GF	93.36	-	94.83	-	94.08	-	98.77	-	95.26	-
Best on LivDet	95.20	-	95.80	-	93.72	-	98.10	-	95.71	-



(a)



(b)

FIGURE 9. Number of versions of the proposed framework that achieved the best ACC with respect to all sensors per year of the LivDet competition according to the normalization strategy used, in (a), and according to the number of dimensions used by the feature vector, in (b).

the Biometrika. In addition, the proposal obtained the second highest average ACC of 98.10%, being only 0.18% below the highest observed one. We can also see that the average ACE of the technique, which corresponds to 1.88%, is higher than the five average ACE presented by the other fourteen techniques, with 1.18% being the smallest of these values.

Regarding the sensors of LivDet 2015, the proposed material also presented satisfactory performance compared to the other techniques. In detail, for the GreenBit, the proposal obtained the best ACC and ACE. At the same time, for the other bases of this edition, the proposal presented the second highest ACC and the second lowest ACE. In this case, the proposal is the technique that most correctly classified fingerprint images, since it presented the highest average ACC and the lowest average ACE.

Thus, as summarized in Table 14, the proposed material presents competitive values for ACC and ACE. In fact, with respect to the considered techniques and their respective average values of ACC and ACE obtained on their respective evaluated benchmarks, the proposed material is the method with the highest average ACC and the lowest average ACE among such techniques.

The proposed method was also compared with other techniques on the challenge of using cross sensors in the training and testing of the classifier. This evaluation, which aims to analyze the method's ability to generalize, is not as common in the literature as the previous ones, since only a portion of the considered studies addresses this situation. Even so, the results obtained by the proposal are compared with the results of six other techniques, as shown in Table 15.

We can notice that the proposed material presents performance comparable to the other techniques when an image base is used for training and another is used for tests. In detail, the technique obtained the lowest ACE in three cases, the most significant being the case in which the classifier was trained on the Biometrika base of the year 2011 and was evaluated on the Italdata base of the year 2011. In this situation, the method presented an ACE equal to 17.80%, which corresponds to less than 60% of the ACE of the coALBP+GF technique, which is equal to 29.75% and corresponds to the second lowest ACE for this same situation. In addition, the proposed method obtained the best ACE value for situations in which the model is trained on 2011 bases and tested on 2013 bases, specifically the cases I11 $\times$ I13 and B11 $\times$ B13, which also proves the generalization ability of the method

TABLE 14. Average performance of all techniques considered for comparison. ACC and ACE values are given in percentage. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen on the line.

	LivDet 2009		LivDet 2011		LivDet 2013		LivDet 2015		Average	
Method	**ACC**	**ACE**	**ACC**	**ACE**	**ACC**	**ACE**	**ACC**	**ACE**	**ACC**	**ACE**
Proposed	***99,51***	***0,50***	95,61	4,40	98,10	1,88	***97,84***	***2,25***	***97,77***	***2,26***
DEHFF	-	-	**95,99**	**4,01**	***98,28***	**1,72**	95,42	4,58	96,56	3,43
CEDD	-	-	-	5,39	-	**1,57**	-	7,89	-	4,95
IFPAD	94,10	4,23	95,08	**3,84**	96,11	2,83	-	-	95,10	3,63
HyFiPAD	96,44	4,11	***96,39***	***3,19***	96,85	2,88	96,10	3,19	96,45	3,34
Linear SN6400	-	3,86	-	**3,93**	-	3,54	-	5,58	-	4,23
PCNN	-	-	-	5,65	-	**1,20**	-	-	-	3,43
DCNNGA	-	4,85	-	7,76	-	5,15	-	5,10	-	5,72
FLDNet	-	6,10	-	8,13	-	6,42	-	5,32	-	6,49
DRNN	-	11,83	-	12,07	-	9,11	-	13,12	-	11,53
FGFF	-	-	95,40	4,60	**98,13**	2,63	96,70	4,03	96,74	3,75
Q-FFF	-	-	-	5,28	-	2,00	95,38	-	95,38	3,64
coALBP+GF	-	-	94,33	-	98,08	-	95,26	-	95,89	-
DRNN	-	-	94,35	5,56	97,04	***1,18***	94,68	5,15	95,36	3,96
WLBD	-	-	-	5,96	-	1,89	-	9,68	-	5,84
ULBP	-	-	-	-	-	12,91	-	-	-	12,91
CNN	-	1,63	-	4,53	-	1,96	-	-	-	2,71

TABLE 15. State-of-the-art comparison for cross-based training and testing with respect to ACE (%). Four sensors are considered in this case: Biometrika, from the 2011 (B11) and 2013 (B13) editions, and Italdata, from the 2011 (I11) and 2013 (I13) editions. The symbol "-" means that the information is not available in the cited work. If the value is highlighted in bold, then this value is better than the one presented by the proposed technique. If the value is in bold, but is also italicized and underlined, then the value is the best seen on the row.

Train × Test	**Proposed**	**coALBP+GF**	**QFFF**	**CNN-VGG**	**CNN-AlexNet**	**SMOc**	**DEHFF**
B11 × B13	***8.40***	8.45	18.45	15.50	15.90	23.20	22.20
B13 × B11	45.80	**35.45**	***29.40***	46.80	47.00	46.60	50
I11 × I13	***6.65***	7.50	11.80	14.60	15.80	10.80	14
I13 × I11	43.55	***32.35***	47.55	46.00	79.10	46.55	-
B11 × I11	***17.80***	29.75	-	37.20	39.80	-	39.95
I11 × B11	14.45	28.32	***14.15***	31.00	33.90	15.95	19.55
B13 × I13	1.30	3.05	17.95	8.80	9.50	22.85	***0.60***
I13 × B13	0.85	10.75	7.05	2.30	3.90	5.15	***0.60***
Average	***17.35***	19.45	20.91	25.28	30.61	24.44	17.83

regarding cross-materials, since the materials used to make spoofings in the 2011 edition are different from those used in the 2013 edition. The proposal was also able to present the second lowest ACE in four situations and the third lowest ACE in one situation. Finally, we note that the proposed technique presented the lowest average ACE among all the analyzed techniques.

D. LIMITATIONS

For the execution of the proposed method, many parameters need to be configured, since it is defined in a generalized way. Thus, as we could see in this section, many variations of the method can be configured, but they must be analyzed together, which can make the stages of experimentation necessarily extensive.

The proposed framework demands that a series of processes be carried out to increase classification accuracy. Among these, it is possible to mention image replication, multiple filtering routines, histogram equalization, ROI detection, and pattern extraction by sets of descriptors. All these processes require processing time and therefore must be configured in a way that does not slow down the material.

VII. CONCLUSION

In this work, two advances on the topic of fingerprint spoofing detection were proposed for the purpose of improving the security offered in BASs. The first advance consists in the proposal of generalizing the vector representation of texture descriptors based on matrices through the use of mapping sets. The second advance is given in the form of a multi-step framework that allows the definition of filtering sets and texture pattern descriptors to increase the image representation capacity and, consequently, improve the accuracy of the classifiers.

The contributions of the work were given in a generalized way and, therefore, it was necessary to define practical instances, or versions, of the material in order to conduct the appropriate evaluations of its execution. In detail, three pattern descriptors — sBRISK, sSIFT and sDenseSIFT — were defined using the proposed mapping representation strategy, which were used to establish ten different versions of the proposed framework. Experimentally, all these practical instances were evaluated in two situations. Since, in the first situation, the instances were compared with each other according to their results on the basis of LivDet competitions and the influence of specific steps of the proposed

framework, such as data augmentation and multi-filtering processes, could have been found and their effectiveness has been proven. Furthermore, in the second situation, the best results presented by the proposed material could be compared with the results available in the specialized literature on the topic. In this case, it was possible to observe that the proposal presents numerical results, at least, competitive with the state of the art with respect to the ACC and ACE metrics considered.

As future experiments, more elaborate strategies should be used to compose the steps of the proposed framework. It is worth mentioning the fact that the simplest possible strategies were considered in the practical versions evaluated and the results obtained were satisfactory. Furthermore, it is believed that the proposed material should present equally acceptable results in problems of spoofing detection on other image-based biometrics, such as faces, iris and ears. Finally, the proposal must also be evaluated on other computer vision problems that demand texture analysis and recognition.

ACKNOWLEDGMENT

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of CNPq and Fapesp.

REFERENCES

[1] M. Sharif, M. Raza, J. H. Shah, M. Yasmin, and S. L. Fernandes, "An overview of biometrics methods," in *Handbook of Multimedia Information Security: Techniques and Applications*. Cham, Switzerland: Springer, 2019, pp. 15–35.

[2] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.

[3] M. Khan, S. Chakraborty, R. Astya, and S. Khepra, "Face detection and recognition using OpenCV," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Oct. 2019, pp. 116–119.

[4] M. Dua, R. Gupta, M. Khari, and R. G. Crespo, "Biometric iris recognition using radial basis function neural network," *Soft Comput.*, vol. 23, no. 22, pp. 11801–11815, Nov. 2019.

[5] Z. Wang, J. Yang, and Y. Zhu, "Review of ear biometrics," *Arch. Comput. Methods Eng.*, vol. 28, no. 1, pp. 149–180, 2021.

[6] O. Yudin, R. Ziubina, S. Buchyk, O. Bohuslavska, and V. Teliushchenko, "Speaker's voice recognition methods in high-level interference conditions," in *Proc. IEEE 2nd Ukraine Conf. Electr. Comput. Eng. (UKRCON)*, Jul. 2019, pp. 851–854.

[7] L. Fei, G. Lu, W. Jia, S. Teng, and D. Zhang, "Feature extraction methods for palmprint recognition: A survey and evaluation," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 2, pp. 346–363, Feb. 2018.

[8] K. Gościewska and D. Frejlichowski, "Silhouette-based action recognition using simple shape descriptors," in *Proc. Int. Conf. Comput. Vis. Graph.* Cham, Switzerland: Springer, 2018, pp. 413–424.

[9] A. Sepas-Moghaddam and A. Etemad, "Deep gait recognition: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, early access, Feb. 15, 2022, doi: 10.1109/TPAMI.2022.3151865.

[10] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 27721–27776, Oct. 2020.

[11] S. Hemalatha, "A systematic review on fingerprint based biometric authentication system," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE)*, Feb. 2020, pp. 1–4.

[12] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, "Fingerprint recognition on mobile devices: Widely deployed, rarely understood," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–9.

[13] A. Hindi, M. O. Dwairi, and Z. Alqadi, "Analysis of procedures used to build an optimal fingerprint recognition system," *Int. J. Comput. Sci. Mobile Comput.*, vol. 9, no. 2, pp. 21–37, 2020.

[14] R. Agarwal, A. S. Jalal, and K. V. Arya, "A review on presentation attack detection system for fake fingerprint," *Modern Phys. Lett. B*, vol. 34, no. 5, Feb. 2020, Art. no. 2030001.

[15] (2013). *Doctor 'Used Silicone Fingers' to Sign in for Colleagues*. Accessed: Jul. 25, 2022. [Online]. Available: https://www.bbc.com/news/world-latin-america-21756709

[16] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–36, Jan. 2014.

[17] R. Ramachandra, "A survey on unknown presentation attack detection for fingerprint," in *Proc. Intell. Technol. Appl., 3rd Int. Conf. (INTAP)*, vol. 1382. Grimstad, Norway: Springer, Sep. 2021, p. 189.

[18] S. Agarwal, A. Rattani, and C. R. Chowdary, "A comparative study on handcrafted features v/s deep features for open-set fingerprint liveness detection," *Pattern Recognit. Lett.*, vol. 147, pp. 34–40, Jul. 2021.

[19] T. K. A. Kumar, R. Vinayakumar, V. V. S. Variyar, V. Sowmya, and K. P. Soman, "Convolutional neural networks for fingerprint liveness detection system," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 243–246.

[20] K. B. Raja, R. Raghavendra, S. Venkatesh, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "A study of hand-crafted and naturally learned features for fingerprint presentation attack detection," in *Handbook Biometric Anti-Spoofing*. Cham, Switzerland: Springer, 2019, pp. 33–48.

[21] G. Tan, Q. Zhang, H. Hu, X. Zhu, and X. Wu, "Fingerprint liveness detection based on guided filtering and hybrid image analysis," *IET Image Process.*, vol. 14, no. 9, pp. 1710–1715, Jul. 2020.

[22] R. C. Contreras, L. G. Nonato, M. Boaventura, I. A. G. Boaventura, B. G. Coelho, and M. S. Viana, "A new multi-filter framework with statistical dense sift descriptor for spoofing detection in fingerprint authentication systems," in *Proc. Int. Conf. Artif. Intell. Soft Comput.* Cham, Switzerland: Springer, 2021, pp. 442–455.

[23] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 971–987, Aug. 2002.

[24] L. Ghiani, P. Denti, and G. L. Marcialis, "Experimental results on fingerprint liveness detection," in *Proc. Int. Conf. Articulated Motion Deformable Objects*. Berlin, Germany: Springer, 2012, pp. 210–218.

[25] X. Jia, X. Yang, K. Cao, Y. Zang, N. Zhang, R. Dai, X. Zhu, and J. Tian, "Multi-scale local binary pattern with filters for spoof fingerprint detection," *Inf. Sci.*, vol. 268, pp. 91–102, Jun. 2014.

[26] T. Maenpaa, "The local binary pattern approach to texture analysis: Extensions and applications," Ph.D. thesis, Dept. Elect. Inf. Eng., Infotech Oulu, Univ. Oulu, Oulu, Finland, 2004.

[27] S. Liao, X. Zhu, Z. Lei, L. Zhang, and S. Z. Li, "Learning multi-scale block local binary patterns for face recognition," in *Proc. Int. Conf. Biometrics*. Berlin, Germany: Springer, 2007, pp. 828–837.

[28] Y. Jiang and X. Liu, "Uniform local binary pattern for fingerprint liveness detection in the Gaussian pyramid," *J. Electr. Comput. Eng.*, vol. 2018, pp. 1–9, Jan. 2018.

[29] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "An investigation of local descriptors for biometric spoofing detection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 4, pp. 849–863, Apr. 2015.

[30] L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in *Proc. 21st Int. Conf. Pattern Recognit. (ICPR)*, 2012, pp. 537–540.

[31] C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale LPQ and PCA," *China Commun.*, vol. 13, no. 7, pp. 60–65, Jul. 2016.

[32] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on Weber local image descriptor," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl.*, Sep. 2013, pp. 46–50.

[33] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y.-Q. Shi, "A novel Weber local binary descriptor for fingerprint liveness detection," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 4, pp. 1526–1536, Apr. 2018.

[34] A. A. Alshdadi, R. Mehboob, H. Dawood, M. O. Alassafi, R. Alghamdi, and H. Dawood, "Exploiting level 1 and level 3 features of fingerprints for liveness detection," *Biomed. Signal Process. Control*, vol. 61, Aug. 2020, Art. no. 102039.

[35] S. Dehaene, "The neural basis of the weber–fechner law: A logarithmic mental number line," *Trends Cognit. Sci.*, vol. 7, no. 4, pp. 145–147, Apr. 2003.

[36] F. Owens and M. Murphy, "A short-time Fourier transform," *Signal Process.*, vol. 14, no. 1, pp. 3–10, 1988.

[37] R. Mehboob, H. Dawood, H. Dawood, M. U. Ilyas, P. Guo, and A. Banjar, "Live fingerprint detection using magnitude of perceived spatial stimuli and local phase information," *J. Electron. Imag.*, vol. 27, no. 5, 2018, Art. no. 053038.

[38] J. J. Mathew and A. P. James, "Spatial stimuli gradient sketch model," *IEEE Signal Process. Lett.*, vol. 22, no. 9, pp. 1336–1339, Sep. 2015.

[39] R. Mehboob and H. Dawood, "DEHFF—A hybrid approach based on distinctively encoded fingerprint features for live fingerprint detection," *Biomed. Signal Process. Control*, vol. 75, May 2022, Art. no. 103572.

[40] J. Li, Y. Chen, and E. Zhang, "Comprehensive edge direction descriptor for fingerprint liveness detection," *Signal Process., Image Commun.*, vol. 102, Mar. 2022, Art. no. 116603.

[41] D. J. Field, "Relations between the statistics of natural images and the response properties of cortical cells," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 4, no. 12, pp. 2379–2394, 1987.

[42] R. P. Sharma and S. Dey, "A comparative study of handcrafted local texture descriptors for fingerprint liveness detection under real world scenarios," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 9993–10012, Mar. 2021.

[43] C. Yuan and Q. M. Jonathan Wu, "Fingerprint liveness detection based on multi-modal fine-grained feature fusion," in *Smart Multimedia*, T. McDaniel, S. Berretti, I. D. D. Curcio, and A. Basu, Eds. Cham, Switzerland: Springer, 2020, pp. 417–428.

[44] X. Li, W. Cheng, C. Yuan, W. Gu, B. Yang, and Q. Cui, "Fingerprint liveness detection based on fine-grained feature fusion for intelligent devices," *Mathematics*, vol. 8, no. 4, p. 517, Apr. 2020.

[45] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2005, vol. 1, no. 1, pp. 886–893.

[46] A. Toosi, A. Bottino, S. Cumani, P. Negri, and P. L. Sottile, "Feature fusion for fingerprint liveness detection: A comparative study," *IEEE Access*, vol. 5, pp. 23695–23709, 2017.

[47] K. He, J. Sun, and X. Tang, "Guided image filtering," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 6, pp. 1397–1409, Jun. 2013.

[48] K. Zuiderveld, "Contrast limited adaptive histogram equalization," in *Graphics Gems*. New York, NY, USA: Academic, Aug. 1994, pp. 474–485.

[49] L. Van der Maaten and G. Hinton, "Visualizing data using t-SNE," *J. Mach. Learn. Res.*, vol. 9, no. 11, Nov. 2008.

[50] W. Jian, Y. Zhou, and H. Liu, "2-layer parallel SVM network based on aggregated local descriptors for fingerprint liveness detection," in *Proc. 13th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jun. 2021, pp. 296–304.

[51] D. Sharma and A. Selwal, "An intelligent approach for fingerprint presentation attack detection using ensemble learning with improved local image features," *Multimedia Tools Appl.*, vol. 81, pp. 1–33, Jul. 2022.

[52] Y. Freund and R. E. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," *J. Comput. Syst. Sci.*, vol. 55, no. 1, pp. 119–139, Aug. 1995.

[53] D. Sharma and A. Selwal, "HyFiPAD: A hybrid approach for fingerprint presentation attack detection using local and adaptive image features," *Vis. Comput.*, vol. 38, pp. 1–27, Aug. 2022.

[54] R. Frassetto Nogueira, R. de Alencar Lotufo, and R. Campos Machado, "Evaluating software-based fingerprint liveness detection using convolutional networks and local binary patterns," in *Proc. IEEE Workshop Biometric Meas. Syst. Secur. Med. Appl. (BIOMS)*, Oct. 2014, pp. 22–29.

[55] R. F. Nogueira, R. De Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1206–1213, Jun. 2016.

[56] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 25, 2012, pp. 84–90.

[57] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.

[58] H. Samma and S. A. Suandi, "Transfer learning of pre-trained CNN models for fingerprint liveness detection," in *Biometric Systems*. Aug. 2020, p. 85.

[59] C. Yuan, Q. Cui, X. Sun, Q. J. Wu, and S. Wu, "Fingerprint liveness detection using an improved CNN with the spatial pyramid pooling structure," in *Advances in Computers*, vol. 120. Amsterdam, The Netherlands: Elsevier, 2021, pp. 157–193.

[60] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg, and L. Fei-Fei, "ImageNet large scale visual recognition challenge," *Int. J. Comput. Vis. (IJCV)*, vol. 115, no. 3, pp. 211–252, 2015.

[61] C. Yuan, Z. Xia, L. Jiang, Y. Cao, Q. M. J. Wu, and X. Sun, "Fingerprint liveness detection using an improved CNN with image scale equalization," *IEEE Access*, vol. 7, pp. 26953–26966, 2019.

[62] W. Jian, Y. Zhou, and H. Liu, "Densely connected convolutional network optimized by genetic algorithm for fingerprint liveness detection," *IEEE Access*, vol. 9, pp. 2229–2243, 2020.

[63] L. B. Booker, D. E. Goldberg, and J. H. Holland, "Classifier systems and genetic algorithms," *Artif. Intell.*, vol. 40, nos. 1–3, pp. 235–282, Sep. 1989.

[64] C. Yuan, Z. Xia, X. Sun, and Q. M. J. Wu, "Deep residual network with adaptive learning framework for fingerprint liveness detection," *IEEE Trans. Cognit. Develop. Syst.*, vol. 12, no. 3, pp. 461–473, Sep. 2020.

[65] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao, and C. Gao, "FLDNet: Light dense CNN for fingerprint liveness detection," *IEEE Access*, vol. 8, pp. 84141–84152, 2020.

[66] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, 2004.

[67] S. Leutenegger, M. Chli, and R. Y. Siegwart, "BRISK: Binary robust invariant scalable keypoints," in *Proc. Int. Conf. Comput. Vis.*, Nov. 2011, pp. 2548–2555.

[68] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," *Comput. Vis. Image Understand.*, vol. 110, no. 3, pp. 346–359, Jun. 2008.

[69] P. F. Alcantarilla, A. Bartoli, and A. J. Davison, "KAZE features," in *Proc. Eur. Conf. Comput. Vis.* Berlin, Germany: Springer, 2012, pp. 214–227.

[70] S. A. K. Tareen and Z. Saleem, "A comparative analysis of SIFT, SURF, KAZE, AKAZE, ORB, and BRISK," in *Proc. Int. Conf. Comput., Math. Eng. Technol. (iCoMET)*, Mar. 2018, pp. 1–10.

[71] D. Erpenbeck, T. Bergen, T. Wittenberg, E. Tannich, C. Wegner, C. Münzenmayer, and M. Benz, "Basic statistics of sift features for texture analysis," in *Bildverarbeitung für die Medizin*, T. Tolxdorff, T. M. Deserno, H. Handels, and H.-P. Meinzer, Eds. Berlin, Germany: Springer, 2016, pp. 98–103.

[72] B. Zoph, E. D. Cubuk, G. Ghiasi, T.-Y. Lin, J. Shlens, and Q. V. Le, "Learning data augmentation strategies for object detection," in *Proc. Eur. Conf. Comput. Vis.* Cham, Switzerland: Springer, 2020, pp. 566–583.

[73] S. Purnapatra, N. Smalt, K. Bahmani, P. Das, D. Yambay, A. Mohammadi, A. George, T. Bourlai, S. Marcel, S. Schuckers, and M. Fang, "Face liveness detection competition (LivDet-Face)-2021," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, 2021, pp. 1–10.

[74] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner, and A. Kuijper, "The overlapping effect and fusion protocols of data augmentation techniques in iris PAD," *Mach. Vis. Appl.*, vol. 33, no. 1, pp. 1–21, Jan. 2022.

[75] D. Ametefe, S. Sarnin, D. Ali, and M. Zaheer, "Fingerprint liveness detection schemes: A review on presentation attack," *Comput. Methods Biomech. Biomed. Eng., Imag. Visualizat.*, vol. 10, no. 2, pp. 1–24, 2022.

[76] M. S. Patil and S. S. Patil, "Wet and dry fingerprint enhancement by using multi resolution technique," in *Proc. Int. Conf. Global Trends Signal Process., Inf. Comput. Commun. (ICGTSPICC)*, Dec. 2016, pp. 188–193.

[77] R. P. Sharma and S. Dey, "Fingerprint liveness detection using local quality features," *Vis. Comput.*, vol. 35, no. 10, pp. 1393–1410, Oct. 2019.

[78] S. Veerashetty and N. B. Patil, "Novel LBP based texture descriptor for rotation, illumination and scale invariance for image texture analysis and classification using multi-kernel SVM," *Multimedia Tools Appl.*, vol. 79, nos. 15–16, pp. 9935–9955, Apr. 2020.

[79] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-9, no. 1, pp. 62–66, Jan. 1979.

[80] R. Nosaka, Y. Ohkawa, and K. Fukui, "Feature extraction based on co-occurrence of adjacent local binary patterns," in *Proc. Pacific-Rim Symp. Image Video Technol.* Berlin, Germany: Springer, 2011, pp. 82–91.

[81] S. Kokoska and D. Zwillinger, *CRC Standard Probability and Statistics Tables and Formulae*. Boca Raton, FL, USA: CRC Press, 2000.

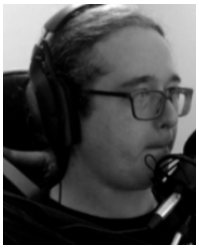
[82] K. Fukunaga, *Introduction to Statistical Pattern Recognition*. Amsterdam, The Netherlands: Elsevier, 2013.

[83] X. Zheng, Y. Wang, and X. Zhao, "Fingerprint image segmentation using active contour model," in *Proc. 4th Int. Conf. Image Graph. (ICIG)*, Aug. 2007, pp. 437–441.

[84] G. W. Stewart, "On the early history of the singular value decomposition," *SIAM Rev.*, vol. 35, no. 4, pp. 551–566, 1993.

[85] D. Yambay, L. Ghiani, G. L. Marcialis, F. Roli, and S. Schuckers, "Review of fingerprint presentation attack detection competitions," in *Handbook Biometric Anti-Spoofing*. Cham, Switzerland: Springer, 2019, pp. 109–131.

[86] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers, "First international fingerprint liveness detection competition—LivDet 2009," in *Proc. Int. Conf. Image Anal. Process.* Berlin, Germany: Springer, 2009, pp. 12–23.
[87] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011-fingerprint liveness detection competition 2011," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, 2012, pp. 208–215.
[88] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2013 fingerprint liveness detection competition 2013," in *Proc. Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.
[89] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," in *Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2015, pp. 1–6.



RODRIGO COLNAGO CONTRERAS received the B.Sc. and M.Sc. degrees in applied and computational mathematics from São Paulo State University (Unesp), in 2013 and 2015, respectively, and the Ph.D. degree in computer science and computational mathematics from the University of São Paulo (USP), in 2020. He completed his postdoctoral fellowship training in pattern recognition in fingerprint spoofing detection with the Geometric Processing Laboratory, USP. He is currently a Postdoctoral Fellow at the Speech Processing Laboratory, Unesp, working on voice spoofing detection. He was the author of the technique that took second place in 2021 Fingerprint Liveness Detection Competition (LivDet). He has experience in artificial intelligence and signal processing, acting on the following subjects: liveness detection in biometrics, deep learning, computational optimization, and visual and analytical pattern recognition.

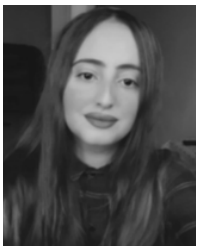
LUIS GUSTAVO NONATO (Member, IEEE) received the Ph.D. degree in applied mathematics from the Pontificia Universidade Catolica do Rio de Janeiro, Rio de Janeiro, Brazil, in 1998. He was a Visiting Professor with the Center for Data Science, New York University, New York, from 2017 to 2018. From 2008 to 2010, he was a Visiting Scholar with the Scientific Computing and Imaging Institute, University of Utah, Salt Lake City. He is currently a Full Professor with the Institute of Mathematical and Computer Sciences, University of São Paulo, São Carlos, Brazil. His research interests include visualization, visual analytics, machine learning, and data science. Besides serving in several program committees, including IEEE SciVis, IEEE InfoVis, and EuroVis, he was an Associate Editor of the *Computer Graphics Forum* and IEEE TRANSACTIONS ON VISUALIZATION AND COMPUTER GRAPHICS. He was also the Editor-in-Chief of *International Journal of Applied Mathematics and Computational Sciences* (SBMAC SpringerBriefs).

MAURÍLIO BOAVENTURA received the degree in mathematics from São Paulo State University, in 1984, the master's degree in computer science and computational mathematics from the University of São Paulo, in 1989, the Ph.D. degree in applied mathematics from the State University of Campinas, in 1998, and a Postdoctoral degree from Michigan State University, in 2012. He is currently an Adjunct Professor at São Paulo State University, a member of the Editorial Board of the *Scientific Initiation Journal* (PETMAT), and a member of the Editorial Board of C.Q.D. *São Paulo Journal of Mathematics Sciences* (electronic). He has experience in the field of mathematics, with an emphasis on applied mathematics. Acting mainly on the following topics: elimination of noise, partial differential equations, image processing, digital retouching, finite differences, and numerical methods.

INÊS APARECIDA GASPAROTTO BOAVENTURA received the bachelor's degree in mathematics from São Paulo State University, in 1986, and the master's degree in computer science and computational mathematics and the Ph.D. degree in electrical engineering from the University of São Paulo, in 1992 and 2010, respectively. She completed her postdoctoral internship training at Michigan State University, in 2012, in the area of biometrics. She has experience in computer science, with emphasis on image processing, working mainly on the following topics: image processing, computer vision, intelligent systems, and biometrics.

FRANCISCO LLEDO DOS SANTOS received the Graduate and master's degrees in civil engineering from São Paulo State University, in 2000 and 2003, respectively, and the joint Ph.D. degree in electrical engineering from São Paulo State University, in 2013, with Sandwich at LNEC—Portugal, in 2013. He was an Occupational Safety Engineer. He is currently a Professor at the Faculty of Architecture and Engineering, Mato Grosso State University (Unemat). He has experience in free surface hydraulics, with emphasis on rheology and waves, working mainly on the following subjects: fluid mechanics, rheology, and open channels and recently application of neural networks in free surface flows and flood control. He was a Coordinator of the Civil Engineering Course—Unemat/Sinop (2006–2008) and the Director of the Faculty of Exact Sciences, Mato Grosso State University (2008–2010). He was the Pro-Rector of Student Affairs at Unemat (2011) and the Pro-Rector of Planning and Institutional Development (2011). He was the Pro-Rector of Planning and Information Technology at Unemat, from 2013 to 2018. He works as an External Affairs Advisor at the Rector's Office and a Permanent Professor of the Professional Master Program Management and Regulation of Water Resources—ProfÁgua.

RODRIGO BRUNO ZANIN received the Graduate degree in mathematics and the master's and Ph.D. degrees in cartographic sciences in computing images from São Paulo State University (Unesp), in 1996, 2004, and 2012, respectively. He is currently an Adjunct Professor and a Rector at the Faculty of Sciences and Technology—FACET, Mato Grosso State University (Unemat), and University Sinop. He has experience in the area of mathematics, with emphasis on applied mathematics, acting on the following subjects: differential equations applied to Image analysis in the computational vision and digital image processing, with applications in geoprocessing and geotechnologies.



MONIQUE SIMPLICIO VIANA received the degree in informatics for business from the Faculty of Technology of São Paulo (FATEC), in 2013, the master's degree in computer science from the Federal University of São Carlos (UFSCar), in 2016, the degree in mathematics from the Integrated Colleges of Ariquemes (FIAR), in 2018, the Doctorate degree in computer science from UFSCar, in 2021, and the M.B.A. degree in project management from the University of São Paulo. She has experience in the area of computational optimization, with an emphasis on bio-inspired meta-heuristics, working mainly on the topics: genetic algorithms and production scheduling, having published articles in traditional events and in journals in the area, and being reviewer in the journals *International Journal of Production Research*, *International Journal of Computer Integrated Manufacturing*, and *Journal of Cloud Computing: Advances, Systems and Applications*. Currently, she is a Supervisor for Course Completion Work of the M.B.A. degree in data science and analytics.