A comprehensive survey of fingerprint presentation attack detection

Konstantinos Karampidis, Minas Rousouliotis, Euangelos Linardos, Ergina Kavallieratou

Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi 83200, Samos, Greece.

Correspondence to: Dr. Konstantinos Karampidis, Department of Information and Communication Systems Engineering, University of the Aegean, Palama 2 & Gorgyras Str., Karlovassi 83200, Samos, Greece. E-mail: karampidis@aegean.gr

How to cite this article: Karampidis K, Rousouliotis M, Linardos E, Kavallieratou E. A comprehensive survey of fingerprint presentation attack detection. J Surveill Secur Saf 2021;2:117-61. https://dx.doi.org/10.20517/jsss.2021.07

Received: 1 Jul 2021 First Decision: 3 Aug 2021 Revised: 28 Aug 2021 Accepted: 30 Sep 2021 Published: 27 Oct 2021

Academic Editors: Jie Yang, Ding Wang Copy Editor: Xi-Jun Chen Production Editor: Xi-Jun Chen

Abstract

Nowadays, the number of people that utilize either digital applications or machines is increasing exponentially. Therefore, trustworthy verification schemes are required to ensure security and to authenticate the identity of an individual. Since traditional passwords have become more vulnerable to attack, the need to adopt new verification schemes is now compulsory. Biometric traits have gained significant interest in this area in recent years due to their uniqueness, ease of use and development, user convenience and security. Biometric traits cannot be borrowed, stolen or forgotten like traditional passwords or RFID cards. Fingerprints represent one of the most utilized biometric factors. In contrast to popular opinion, fingerprint recognition is not an inviolable technique. Given that biometric authentication systems are now widely employed, fingerprint presentation attack detection has become crucial. In this review, we investigate fingerprint presentation attack detection by highlighting the recent advances in this field and addressing all the disadvantages of the utilization of fingerprints as a biometric authentication factor. Both hardware- and software-based state-of-the-art methods are thoroughly presented and analyzed for identifying real fingerprints from artificial ones to help researchers to design securer biometric systems.

Keywords: Presentation attack detection, fingerprints, hardware- and software-based methods, biometrics, multimodal systems, multi-factor authentication
INTRODUCTION

As the utilization of digital devices and applications continues to grow, the need for more complex solutions to authenticate legitimate users is becoming essential. In this context, biometric-based authentication systems are being increasingly employed as they can be found almost everywhere, including in smartphones, laptops and so on. Fingerprint recognition is based on the Galton points [Figure 1], named after Sir Francis Galton, who in the late nineteenth century used the so-called Galton points to categorize the attributes of a finger that are utilized to identify a person. Later on, in the late 1960s, with the mechanization of fingerprint matching and the advancement of computer science, these points were renamed to minutiae points and became the standard in the feature extraction stage of fingerprint systems. \[1\]

Fingerprint recognition has some of the lowest false rejection rates (FRRs) and false acceptance rates (FARs) compared to other biometric authentication systems. In 2015, it held 58% of the global market share of biometric authentication systems. Although fingerprints are one of the most utilized biometric factors, security weaknesses still arise. To enhance security, multi-fingerprint systems have been proposed. These systems use more than one finger to produce the biometric identity of a user.

As more biometric systems are utilized, presentation attacks (PAs) are also increasing. PAs can be defined as “presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.” Artificial fingerprints can be created using low-cost hardware and software, meaning that a skilled person who wants to compromise the security of a system is very likely to succeed.

Security attacks on fingerprint authentication systems can be classified into three categories: (1) attacks with the use of PA instruments at the sensor; (2) attacks on a module of the system; and (3) attacks on the communication channel between the modules of the system. Many types of security violations on fingerprint scanners occur during the communication between the modules of the authentication scheme. Attackers try to modify the data on the communication channel between the sensor and the feature extraction module. Data modification also happens when they circumvent the channel amongst the feature extraction module database and the matching module or between the database and the matching module. In this kind of attack, the attackers modify the data of the channel and manipulate the routines of the various modules of the system. Moreover, perpetrators can insert fake data that the system recognizes as genuine. This attack takes place directly at the modules of the authentication system, i.e., the data storage, the signal processing and the comparison decision [Figure 2], by modifying the data. The aforementioned vulnerabilities can be countered with the use of software- or hardware-based encoding and decoding techniques on the communication channels between the modules of the fingerprint authentication system. \[5\]

Liveness detection refers to the analysis of the features of a finger to determine whether the input finger is live or not. Presentation attack detection (PAD) is the automated determination of a PA, while liveness detection is a sub-category of PAD. The term PAD will be utilized throughout this survey, although authors in the presented state-of-the-art research may use the previous term, i.e., liveness detection or “anti-spoofing attacks”. A taxonomy of the state-of-the-art methods is shown in Figure 3. To detect whether a fingerprint is artificial, additional hardware is used to detect the heartbeat, blood pressure, skin impedance and other biometrics of the fingerprint like odor. Nevertheless, these approaches are usually expensive. To tackle this, researchers are using software-based methods to extract PAD features directly from the acquired sample from the main sensor. These approaches are based on the fact that certain characteristics of live fingerprints cannot be duplicated. These distinct features can be extracted and selected with the use of further analysis of the acquired sample. There are two kinds of methods that are employed, i.e., “dynamic” methods that perform feature extraction by investigating multiple frames of the acquired sample and
“static” methods that use a single image of the impression of the fingertip[4].

This survey presents a comprehensive literature review of PAD methods. The performance and quantitative analysis of the methods presented in the following sections have also been given by the utilized metrics in the discussed studies, such as the accuracy, fake error rate and so on.

Kundargi et al.[7] refer only to textural feature-based fingerprint PAD methods, while we make an overall presentation. Comprehensive surveys are given in Refs.[8,9] but these are now outdated. The detailed surveys in Refs.[10-12] only provide the PAD methods proposed for LivDet competitions[13]. This work (1) provides a detailed literature review of state-of-the-art fingerprint PAD methods; (2) is focused on, but not limited, the last decade; (3) refers to all PAD categories (i.e., both software- and hardware-based approaches) and not only to specific ones (e.g., only texture- or hardware-based approaches); and (4) is up to date, including current research trends, such as deep learning techniques.
Figure 3. Presentation attack detection methods, inspired by [8,9].

All discussed studies were retrieved by Google Scholar. Initially, the search terms “fingerprint presentation attack detection” and “fingerprint liveness detection” were given and this resulted in the retrieval of 17,200 and 6830 records, respectively. To lessen the number of retrieved studies, a new search was performed under the limitation that the search term should be part of the title of the publication, thereby making them relevant to the subject of interest. The search queries were: (1) allintitle: “fingerprint liveness detection”, which resulted in 199 publications; (2) fingerprint “presentation attack”, which retrieved 51 publications; and (3) allintitle: “fingerprint spoof detection”, which resulted in 31 publications.

A thorough search was also made regarding the LivDet competitions from 2009 to 2019 [13], as the most relevant events for PAD. Furthermore, a recent survey [14] (included in Ref. [15]) was considered and taken into account. By combining the aforementioned search results and by reading the abstract of each publication to determine whether it was relevant to our research, we eventually reached a total of more than 190 publications, which are discussed in the following sections.

The main contributions of this article can be summarized as follows:

1. A comprehensive review is performed regarding state-of-the-art methods for fingerprint PAD.
2. The literature review presents both hardware- and software-based methods, thereby updating other similar works [8,9] and those where only one category was examined [7].
3. The software-based methods include the latest trends, such as deep learning approaches.
4. A quantitative and qualitative analysis of the datasets that were utilized in the relevant literature is presented.
5. In addition to the presentation of the methods according to the taxonomy in Figure 3, tables are given for each category that summarize the most important features of each method.
(6) The research challenges and potential research directions are outlined.

The rest of the review is organized as follows. In TERMS, DEFINITIONS AND EVALUATION METRICS, the terms, definitions and evaluation metrics are presented, while DATASETS refers to the most utilized and publicly available datasets. HARDWARE-BASED PRESENTATION ATTACK DETECTION presents the hardware-based methods, while the software-based methods are given in SOFTWARE-BASED PRESENTATION ATTACK DETECTION. A discussion along with potential research directions is presented in DISCUSSION. Finally CONCLUSIONS outlines the derived conclusions from this review.

TERMS, DEFINITIONS AND EVALUATION METRICS

In this section, we report the terms and evaluation metrics utilized by authors in their publications. It must be noted that some of them are no longer utilized, as they no longer exist in the ISO/IEC 30107-3 standard\[^{16}\]. Nevertheless, since they were utilized in previous studies, it was deemed appropriate to report them. The most common evaluation metrics are the accuracy, maximum accuracy (ACC), equal error rate (EER), average classification error (ACE) [Equation (1)], attack presentation classification error rate (APCER) and bona fide presentation classification error rate (BPCER). These estimators were used on the ATVS\[^{17}\], the LivDet 2009-2019\[^{13}\] [Figure 4], the MSU FPAD\[^{18}\] and the Precise Biometrics Spoof-Kit dataset\[^{18}\]. The terms and evaluation metrics are defined as follows:

- Attack presentation/presentation attack: “presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system”.

- Presentation attack instrument (PAI): “biometric characteristic or object used in a presentation attack”.

- PAI species: “class of presentation attack instruments created using a common production method and based on different biometric characteristics”.

- Bona fide presentation: “interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system”.

- Bona fide presentation classification error rate: “proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario”.

- Attack presentation classification error rate: “proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario”.

The accuracy and average classification rates can be described as:

- Accuracy: rate of correctly classified genuine (live) and fake fingerprints given a threshold of 0.5.

- True detection rate (TDR): the percentage of PA samples correctly detected.

- False detection rate (FDR): the percentage of bona fide samples incorrectly classified as PA.

- False spoof acceptance (FSA): the percentage of live fingerprint samples that are misclassified as spoofs (PAs).
- False live rejection (FLR): the percentage of spoof (PA) samples that are misclassified as live.

- FerrLive: rate of misclassified live fingerprints.

- FerrFake: rate of misclassified fake (artificial) fingerprints.

- Equal error rate: rate at which FerrLive and FerrFake are equal.

- False acceptance rate: percentage of imposters accepted by the system.

- False rejection rate: percentage of genuine users rejected by the system.

- Average classification error rate (ACER): \[
ACE = \frac{BPCER + APCER}{2}
\]

- Correct classification rate (CCR): percentage of correctly classified presentations (not defined in the ISO/IEC 30107-3 standard but used in previous studies).

- Spoof, spoofing and anti-spoofing: terms used in the literature instead of PAI, PA and PAD before the adoption of the ISO/IEC 30107-3 standard.
Although APCER and BPCER are the standard metrics in ISO/IEC 30107-3\cite{16}, ACER is also mentioned due to its utilization in LivDet competitions.

**DATASETS**

Fingerprint PAD is a binary classification problem, i.e., the acquired samples are classified as bona fide or artificial. The datasets that train and test the classifiers play an important role. For this reason, it is important to refer to the structure and the characteristics of the most common and publicly available datasets. The procedure to create a dataset is to capture samples from unique individuals and afterwards to create the artificial ones. The resulting dataset is then split into a training and a test set, which are utilized to train and test the proposed classifiers, respectively.

To create the artificial fingerprint images, two different approaches are deployed, namely, the cooperative and non-cooperative methods. In the cooperative method, the subject pushes their finger into a malleable material, e.g., plastic, or wax, to create a mold, which is then filled with a material, such as gelatin, Play-Doh or silicone. In the non-cooperative method, an attacker typically enhances a latent fingerprint left on a surface, e.g., a CD, photographs it and finally prints the negative image on a transparency sheet.

A dataset needs to be both qualitatively and quantitatively good. The quantitative part concerns the number of existing bona fide and artificial samples. The more samples in the dataset, the better it should be. However, in addition to the absolute number of bona fide/artificial samples, a key factor is the distribution of samples in each one of the two categories. Ideally, datasets must be balanced. A balanced dataset is a dataset where each output class, bona fide and artificial in this case, is represented by the same number of input samples. As deep learning methods have been extensively utilized in recent years, the number of samples in the dataset, along with their distribution (number of bona fide/artificial samples), are important factors in the design of efficient classification algorithms.

Another qualitative element of a dataset is the number of subjects that were used to capture the bona fide samples and the number of visits that were needed to capture the bona fide samples. In some cases, the bona fide samples were captured during one visit, while in others in multiple visits. It is important to include a large number of unique subjects, as well as multiple visits for the training bona fide samples\cite{19}.

Moreover, the number of optical sensors (scanners), their resolution and the size of the captured images are other factors that need to be addressed. Good quality of the captured images is a prerequisite for good system performance, but it also allows for subsequent reliable processing of the data. Furthermore, the method with which the images were acquired should also be considered. Bona fide samples with wet and dry fingers and with high and low pressures should be present in the dataset.

Finally, it must be noted that an efficient algorithm should recognize artificial samples from unknown, i.e., not present in the training set, materials. Thus, the proposed algorithms are evaluated against overfitting and how well they generalize unseen data (artificial samples of unknown materials). For this reason, the test set should be adjusted accordingly.

The most common datasets that were utilized from the presented state-of-the-art methods are the ATVS, LivDet 2009-2019, MSU-FPAD and the Precise Biometrics Spoof-Kit Dataset. However, although the aforementioned datasets are considered as benchmarks, especially the ones introduced in the LivDet competitions, there are many proposed methods that utilize custom datasets\cite{20-22}. The qualitative and the quantitative elements of the most common publicly available datasets are presented in Table 1.
Table 1. Most utilized and publicly available datasets

| Dataset   | Number of capture subjects | Number of scanners used | Used PAI species                                                                 | Creation method of the artificial fingerprints | Number of samples in training set | Number of samples in test set | Total number of samples |
|-----------|---------------------------|------------------------|---------------------------------------------------------------------------------|-----------------------------------------------|---------------------------------|---------------------------|------------------------|
| LivDet 2009 | 111                       | 3                      | Gelatin, silicone, Play-Doh                                                    | Cooperative                                   | 2750                            | 8250                      | 11,000                 |
| LivDet 2011 | 206                       | 4                      | EcoFlex, Silgum, Gelatine, Latex, Wood Glue, Play-Doh, Silicone                | Cooperative                                   | 4000                            | 4000                      | 8000                   |
| LivDet 2013 | 244                       | 4                      | EcoFlex, Gelatine, Latex, Modasil, Body Double, Wood Glue, Play-Doh            | Cooperative/Non-cooperative                  | 8500                            | 8500                      | 17,000                 |
| LivDet 2015 | 51                        | 4                      | Body Double, EcoFlex, Play-Doh, Gelatine, Latex, Wood Glue                     | Cooperative                                   | 10,448                          | 10,448                    | 20,896                 |
| LivDet 2017 | 50                        | 3                      | Body Double, Ecoflex, Play-Doh, Wood Glue, Gelatin, Ecoflex w. additive, Gelatin w. additive | Cooperative/Non-cooperative                  | 6598                            | 11,186                    | 17,784                 |
| LivDet 2019 | NA                        | 3                      | Wood Glue, Ecoflex, Body Double, Latex, Gelatine, Liquid Ecoflex                | Cooperative/Non-cooperative                  | 6400                            | 6565                      | 12,965                 |
| ATVS       | 17                        | 3                      | Play-Doh                                                                        | Cooperative/Non-cooperative                  | 1530                            | 1530                      | 3060                   |
| MSU-FPAD   | NA                        | 2                      | Ecoflex, Play-Doh, 2D print (Matte Paper), 2D print (transparency)            | Cooperative                                   | 9750                            | 9750                      | 19,500                 |
| Precise biometrics | NA   | 2                      | Ecoflex, Gelatin, Latex Body paint, Ecoflex with silver colloidal ink coating, Ecoflex with bare paint coating, Ecoflex with Nanofit coating, Crayola Model Magic, Wood glue, Monster Liquid Latex, 2D fingerprint on office paper | Cooperative                                   | 950                             | 950                       | 1900                   |

PAI: Presentation attack instrument.

HARDWARE-BASED PRESENTATION ATTACK DETECTION

Hardware-based PAD methods require explicit sensors to be integrated into the fingerprint biometric system to detect whether signals, such as the fingerprint temperature\(^{[23]}\), pulse oximetry\(^{[24]}\), blood pressure\(^{[25]}\) or odor\(^{[26]}\), are real or not. Biometric systems that make use of these hardware sensors capture both the subject’s fingerprint and one or more of the signals to authenticate the user. Thus, authentication is more accurate, PAs are prevented and the FAR will be higher. However, on the contrary, the system becomes more complex and expensive.

The skin temperature is considered normal when it lies between 26 and 37 °C. However, there are people whose blood circulation is problematic and this fact finally leads to a larger deviation in skin temperature. Moreover, the environmental conditions, e.g., temperature, that exist during sample acquisition must be considered in order to make the biometric system operational under different conditions. Therefore, the temperature range must become larger, but this inevitably increases the likelihood that the system will be deceived.
Baldisserra et al. proposed an odor-based PAD system. The acquisition of the odor is made of chemical sensors that detect the characteristic pattern of an odor. The achieved EER measured during the experiments was 7.48%. The conducted experiments showed that when the odor sensors were exposed to skin or gelatin, the voltage decreased, while it increased when the sensors were exposed to silicone or latex. However, the drawback of the method was that some artificial fingers, such as gelatin, show analogous sensor responses to real fingers and therefore the biometric system can be fooled.

Pulse oximetry measures the saturation of oxygen of hemoglobin (%SpO2) by calculating the red and near infrared light absorption characteristics of oxygenated and deoxygenated hemoglobin.

Blood pressure was also proposed as a biosignal capable of discriminating between bona fide and artificial fingerprints. Normal adult blood pressure is in the range of 80 mmHg, when the heart relaxes (diastolic pressure), to 120 mmHg, when the heart beats (systolic pressure). Lower values mean that the person suffers from hypotension. Conversely, when the systolic blood pressure is equal to or above 140 mmHg and/or a diastolic blood pressure is equal to or above 90 mmHg, the person suffers from hypertension. Critical pressure values are 140 mmHg for the diastolic blood pressure and 300 mmHg for the systolic blood pressure. Therefore, diastolic and systolic blood pressure values range from 80 to 140 mmHg and from 120 to 300 mmHg, respectively. Thus, blood pressure values outside these ranges may indicate an artificial fingerprint. The limitation of this method relies on the case that if an attacker “wears” an artificial fingerprint on their finger, the measured blood pressure value may lie within the accepted range. Therefore, an attacker with hypertension could bypass this PAD method.

Another approach to detect whether or not an artificial material was utilized is the deployment of optical coherence tomography (OCT). OCT is an imaging technique that allows some of the subsurface characteristics of the skin to be imaged and extracts relevant features of multilayered tissues up to a maximum depth of 3 mm.

Cheng and Larin proposed the adoption of OCT by acquiring averaged B-scan slices to reduce speckle noise and form a one-dimensional curve that represented the distribution of light into the skin. Afterwards, they applied autocorrelation analysis to detect repeating structures. Homogeneous signals yield high absolute autocorrelation coefficients, while inhomogeneous signals yield autocorrelation coefficients close to zero. The authors assumed that real human skin exhibits inhomogeneity while artificial fingerprints do not.

Cheng and Larin extended the previous work and instead of obtaining a B-scan slice, they acquired a number of lateral scans to create a volumetric representation of the finger. Using this method, they were able to visually analyze the topography of the fake layer and the underlying real fingerprint to detect PAs.

Other similar works utilized a frequency-domain OCT system, a spectral-domain OCT system, an en face and time-domain OCT system and a swept source OCT system as PAD methods. These techniques include the ability to detect differences between fake layers placed on a finger and the real finger below, to map eccrine sweat glands on the fingertip, to detect additional layers placed on top of the skin and to extract reliable subsurface information from a real finger, which are not present in artificial fingerprints.

In addition to the aforementioned OCT-based PAD methods, other research has utilized short-wave infrared (SWIR) images, special lighting microscopes and terahertz time-domain spectroscopy (TDS).
Hussein et al.\cite{35} proposed a novel hardware-based method based on two sensing modalities, i.e., MS illumination in the SWIR spectrum (wavelength range from 1200 to 1550 nm) and laser speckle contrast imaging (LSCI). The authors evaluated the effectiveness of both modalities by developing a touchless prototype fingerprint imaging system that was designed to capture images in the visible domain for verification, and in the SWIR domain and LSCI for FPAD. The capture device was used to collect data from 778 finger samples (551 bona fide and 227 PA), covering 17 different attack species. To evaluate the effectiveness of the capture device, the authors utilized a patch-based convolutional neural network on the two sensing modalities and the results were promising.

Tolosana et al.\cite{36} proposed a novel fingerprint presentation attack detection method based on convolutional neural networks (CNNs) and SWIR multi-spectral images. Based on an analysis of the intra- and interclass variability, two SWIR wavelengths and their combination were selected as input for the network. The experimental evaluation yields a BPCER of 0% (i.e., a highly convenient system) and an APCER of 0% simultaneously (i.e., highly secure). Although the results are excellent, more experiments should be made on a larger database, comprising more PAIs and more bona fide samples, in order to further test the performance of the algorithm for both known and unknown attacks.

Gomez-Barrero et al.\cite{37} introduced another PAD scheme that utilized SWIR spectral images of the finger and the inside of it using LSCI technology. For the classification of the fingerprint as bona fide or artificial, the fusion with a weighted sum of several features and classifiers depending on the input of the scheme was used. They evaluated their method on a custom dataset whilst including unknown PA showed a less than 0.1% BPCER and an APCER of ~3%.

Tolosana et al.\cite{38}, in an extension of their work in\cite{36}, introduced a novel capture device capable of acquiring fingerprint samples in the SWIR spectrum. They experimented with three CNN architectures: (1) a residual CNN both trained from scratch and pretrained; (2) VGG19\cite{39}; and (3) MobileNet\cite{40}. The optimal performance was exhibited with the fusion of the residual CNN trained from scratch and the VGG19 architecture on a dataset comprised of 4700 samples and with the assumption that five PAI species were not used in the training and were considered as unknown PAI. This architecture achieved an APCER of ~7% for a BPCER of 0.1% if user convenience was the top priority and a BPCER of 2% for any APCER under 0.5% when security took precedence.

Goicoechea-Telleria et al.\cite{41} proposed a low-cost PAD subsystem using special lighting microscopes with only one wavelength (575 nm) with a filter (610 nm) and took only the red channel. This resulted in low APCER and BPCER values, i.e., an APCER of 1.78% and a BPCER of 1.33% at 70% training. Moreover, all iterations of classifying the 480/510 nm wavelength of the blue channel have shown a BPCER of 0.00%. Furthermore, it was discovered that Play-Doh artefacts were very easily detected with this approach. Although the aforementioned results are promising, the system has to be thoroughly tested with a larger dataset.

To facilitate the exploration of novel fingerprint PAD techniques involving both hardware and software, Engelsma et al.\cite{42} designed and prototyped a low-cost custom fingerprint reader, known as RaspiReader, with ubiquitous components. RaspiReader has two cameras for fingerprint image acquisition. One camera provides high-contrast frustrated total internal reflection (FTIR) fingerprint images and the other outputs direct images of the finger in contact with the platen. Using both of these image streams, the discriminative color local binary patterns (CLBP) from both raw images were extracted which, when fused together, matched the performance of state-of-the-art PAD methods (CNN). Moreover, fingerprint matching
experiments between images acquired from the FTIR output of RaspiReader and images acquired from a commercial off-the-shelf (COTS) reader verified the interoperability of the RaspiReader with existing COTS optical readers.

Pałka and Kowalski\[43\] used a TDS setup in a reflection configuration for the non-intrusive detection of fingerprint PAs. More specifically, the authors studied the interaction of terahertz radiation with the friction ridge skin of finger pads and with artificial samples. Moreover, five common PA materials were used and their complex refractive indices were determined. It was proved that both the reflected time signals and the reflectance spectra of the imitations differ significantly from the living fingers of 16 people. Based on the conducted analysis, two PAD methods were proposed. The first method was based on a time-frequency feature analysis and achieved a TDR of 87.9% and an FDR of 3.9%. The second method was based on a deep learning classifier applied to reflectance spectra, with a second criterion based on reflected signals in the time domain. The second method with five-fold cross validation provided excellent classification with a TDR of 98.8%. The second method was also validated using the cross-material scenario and achieved slightly lower results with a TDRs of 98.7% and 93.2% for silicone, latex and plasticine samples (Group I) and gelatin, Play-Doh and water-based samples (Group II), respectively.

Spinoulas et al.\[44\] explored the effectiveness of PAD schemes in front-illumination imaging using shortwave-infrared, near-infrared and laser illumination and back-illumination imaging using near-infrared light. Their architecture utilized a memory efficient fully convolutional neural network (FCN). The effectiveness of the FCN was first validated on the LivDet 2015 dataset. They concluded that in the case of unknown PAs, front-illuminated multi-spectral images (visible, NIR and SWIR) presented the best performance, either individually or in fusion with other modalities used in this study to capture the fingerprint image.

Other hardware-based solutions, such as the capture means of biological signals of life, like blood flow and pulse rate detection\[45\] and electrocardiogram (ECG)\[46\] or electroencephalogram (EEG) signals\[47\], are also discussed in the literature. However, all the biological signals either require expensive capture equipment or in some cases\[48\] may add a time delay to the user authentication process.

PAD methods make biometric systems securer and resistant to attacks. Nevertheless, due to their limitations and given the fact that they are not immune to PAs, software-based solutions have been proposed to enhance security and avoid any modifications to the hardware.

SOFTWARE-BASED PRESENTATION ATTACK DETECTION

Software-based PAD methods utilize algorithms to detect artificial fingerprints once the sample has been acquired by the sensor. A typical PAD follows the procedure of capturing the sample, preprocessing and decision, as shown in Figure 5.

It must be noted that in many cases, the feature extraction from the captured data and the classification can be performed from the same system, e.g., from a convolutional neural network.

The categorization of software-based PAD approaches presented here was inspired by Refs.\[8,9\]. Software-based PAD methods can be divided into two major categories: dynamic and static.
Dynamic methods

Dynamic PAD methods utilize dynamic features. These features change over time and for their extraction, a time-series sequence of images or video of the fingerprint is required. This is opposed to static methods that classify bona fide or artificial presentations according to the data acquired from a single image. Dynamic methods present the ability to detect and measure vitality signs that can distinguish between bona fide and artificial fingerprints. These signs include the perspiration phenomenon, skin elasticity deformation and the displacement of blood that occurs when a finger is under pressure. Table 2 summarizes the discussed methods.

Abhyankar and Schuckers\cite{20} proposed a PAD method based on the perspiration phenomenon and utilized two samples captured in a time series of 0 and 5 s. The coefficients of Daubechies wavelet analysis using the zoom-in property were utilized to reflect the perspiration pattern. A threshold was applied to the first difference of the information in all the sub-bands. A dataset consisting of 30 live, 30 artificial and 14 cadaver fingerprint samples was utilized, where half of the data were used for training and the other half for evaluation. The proposed method achieved an FLR of 0% and an FSA of 0% at threshold levels of 44.55, 40.75 and 31.6 for an optical scanner, a capacitive DC scanner and an opto-electrical scanner, respectively.

Antonelli et al.\cite{49} proposed a PAD method based on skin elasticity/distortion. This method requires that the user moves their finger while applying force to the scanner in order to maximize skin distortion. The proposed method was evaluated on a dataset comprising of ten image sequences of each finger (thumb and forefinger of the right hand) of 45 volunteers and ten image sequences of 40 artificial fingers, and achieved an EER of 11.24%.

Jia et al.\cite{50} introduced a novel PAD method based on skin elasticity. This method was based on two features that represent skin elasticity acquired from a two-image sequence. The utilized features were the correlation coefficient of the fingerprint area, the average image signal intensity and the standard deviation of the fingerprint area extension in the x and y axes. The classification was accomplished with Fisher’s linear discriminant analysis. This method achieved an EER of 4.78% on a dataset comprised of 770 image sequences.

Zhang et al.\cite{51} proposed a PAD method based on finger skin elasticity analysis and utilized the thin-plate spline model. This method exhibited an EER of 4.5% on a dataset of image sequences recorded from 120 artificial fingers from 20 volunteers and the corresponding real fingers.

DeCann et al.\cite{52} proposed a PAD method that quantified the perspiration phenomenon and it was based on a time-series sequence of acquired fingerprint samples with a 1 s interval. It used region labeling on the first image capture whilst the second capture was comprised of three images (absolute, positive and negative). A neural network was utilized for classification. A dataset of 1526 bona fide and 1588 artificial fingerprints from 150 volunteers was used for evaluation and the proposed method achieved an EER of 4.5%.
Table 2. Dynamic methods

| Ref. | Year | Dataset | Method | Results |
|------|------|---------|--------|---------|
| Abhyankar and Schuckers | 2004 | Own dataset | Detection of perspiration phenomenon | FLR of 0% and FSA of 0% at threshold levels of 44.55, 40.75 and 31.6 of optical, capacitive DC scanner and opto-electrical scanner, respectively |
| Antonelli et al. | 2006 | Own dataset | Skin elasticity/distortion | EER of 11.24% |
| Jia et al. | 2007 | Own dataset | Skin elasticity | EER of 4.78% |
| Zhang et al. | 2007 | Own dataset | Skin elasticity | EER of 4.5% |
| DeCann et al. | 2009 | Own dataset | Detection of perspiration phenomenon | EER of 4.5% |
| Nikam and Agarwal | 2009 | Own dataset | Detection of perspiration phenomenon | Classification accuracy of 97.92% for live and of 99.10% for artificial samples |
| Abhyankar and Schuckers | 2009 | Own dataset | Detection of perspiration phenomenon | EER of 0.03% while incorporated to verifinger scanner. Exhibited a 13.82% improvement to the scanner’s EER performance |
| Abhyankar and Schuckers | 2010 | Own dataset | Detection of perspiration phenomenon | Classification rate of 93.7% |
| Marcialis et al. | 2010 | Own dataset | Detection of sweat pores | Qualitative interpretation of the results |
| Memon et al. | 2011 | NIST4, BFBIG-DB1 | Detection of active sweat pores | Qualitative interpretation of the results |
| Husseis et al. | 2020 | Own dataset | Extraction of eight global measures that included intensity, contrast, and randomness | BPCER of 18.1% at 5% APCER for thermal sensor BPCER of 19.5% at 5% APCER for optical sensor |
| Husseis et al. | 2021 | Own dataset | Extraction of five spatiotemporal features | BPCER of 3.89% at 5% APCER for thermal sensor BPCER of 1.11% at 5% APCER for optical sensor |

FLR: False live rejection; FSA: false spoof acceptance; EER: equal error rate; BPCER: bona fide presentation classification error rate.

Nikam and Agarwal introduced a perspiration detection algorithm that relies on the processing of the ridge lines of the fingerprint in the wavelet domain by utilizing a time-series image capture sequence of 2 or 4 s. A neural network, support vector machine (SVM) and K-nearest neighbor algorithm (K-NN) were utilized as classifiers. On a dataset of sequences of image captures from 340 real, 260 gummy and 195 Fun-Doh artificial fingers, the proposed method exhibited a classification accuracy of 97.92% for bona fide samples and 99.10% for artificial samples, with the use of an SVM for classification.

Abhyankar and Schuckers proposed a PAD method that detected the perspiration changes along the fingerprint ridges from fingerprint samples captured at 0 and 2 s. The measures used to classify a fingerprint as artificial or not were the Daubechies wavelet transform, the multiresolution analysis and the wavelet packet transform, which were used to isolate the changes in perspiration based on the total energy distribution. A dataset of sequences of images of 58 live, 50 artificial and 28 cadaver fingerprints was utilized. The method exhibited an EER of 0.03% when it was incorporated into the commercially available “verifinger” matcher. The “verifinger” matcher without this incorporation achieved an EER of 13.85%.

Abhyankar and Schuckers utilized a time-series fingerprint image, captured with a 2-time interval in order to use the perspiration phenomenon to classify fingerprints as bona fide or not. This method was based on the detection of the signal changes of singularity points that were found with the use of wavelets. The method was evaluated on a dataset of 58 bona fide, 50 artificial and 28 cadaver time-series fingerprint samples and achieved a 93.7% correct classification rate.
Marcialis et al.\cite{Marcialis} proposed a PAD method based on the detection of sweat pores. This was a two-step procedure that evolved the time series capture of two samples in a 5 s interval. The authors utilized the difference in the number of pores of each region of interest (ROI) between the captured samples (four features), along with the average Euclidean distances among pores in the second sample (three features). Therefore, a seven-dimensional feature vector was formed, which was utilized to train a K-NN classifier and a multi-layer perceptron (MLP). The experimental results on their own dataset consisting of 8960 bona fide and 7760 artificial fingerprint samples showed that analyzing the location of pores for PAD is a promising technique.

Memon et al.\cite{Memon} developed a system that can detect active sweat pores to determine whether a fingerprint is bona fide or artificial. Two fingerprint images with a 2 s time interval were utilized in conjunction with an image processing algorithm that depends on high pass and correlation filtering, followed by binarization. The efficiency of this method is negatively correlated to the threshold value of binarization. Alternatively, the discrimination ability is positively correlated with the threshold. The algorithm was tested on the NIST4\cite{NIST4} and BFBIG-DB1\cite{BFBIG-DB1} databases.

Husseis et al.\cite{Husseis} used eight global measures that included intensity, contrast and randomness. These features were extracted from fingerprint videos. For the evaluation of the proposed method, 792 bona fide presentations and 2772 attack presentations were collected from thermal and optical sensors and used as a dynamic dataset. An SVM, linear discriminant analysis (LDA) and ensemble learning were used for classification. This PAD method achieved a performance of 18.1% BPCER for the thermal subset and 19.5% BPCER for the optical subset at 5% APCER when an SVM was used for classification.

Husseis et al.\cite{Husseis}, in an extension of their previous work\cite{Husseis}, utilized videos of fingerprints to extract five spatiotemporal features that allowed them to detect PAIs. An SVM with a second-degree polynomial kernel was used for classification. This method achieved a BPCER of 1.11% for an optical sensor and a BPCER of 3.89% for a thermal sensor at 5% APCER for both sensors on their own dataset.

**Static methods**

Static PAD methods rely on features extracted from a single fingerprint image. These features are unique and do not change over time. Depending on the technique or the type of features or the type of classification method used (e.g., neural networks, deep learning and so on), static methods can be further divided into those that utilize anatomical or physiological features, image quality features, textural features, neural networks, fusion of features and generalization efficient/wrapper methods. The latter category describes the methods that focus on performance against PAIs not seen in training. Some of them can be combined with the ones from the first five categories to improve the overall system performance, especially against PAI species made with unknown materials.

**Anatomical or physiological features**

This section describes state-of-the-art PAD methods, where anatomical or physiological features, such as sweat pores and perspiration, are utilized to determine if a fingerprint is real or artificial. The detection schemes are mainly focused on sweat pores [Figure 6] or perspiration. The term sweat pore describes tiny openings in the skin where sweat reaches the surface from their respective glands below. Perspiration is a phenomenon where sweat starts from the pores and scatters along ridges. Thus, regions between pores become darker. Modern PAD methods exploit this property and by observing numerous samples, they can capture a perspiration pattern that indicates whether a finger is real or not. Table 3 summarizes the presented methods.
Table 3. Anatomical features

| Ref.               | Year | Dataset         | Method                                                                 | Results                                                                 |
|--------------------|------|-----------------|------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Tan and Schuckers  | 2010 | Own dataset     | Perspiration. Ridge signal and valley noise analysis                   | EER of 0.9%                                                            |
| Espinoza and Champod | 2011 | Own dataset     | Pores of the skin                                                      | 21.2% FAR and 8.3% FRR                                                 |
| Memon et al.       | 2011 | NIST4, BFBIG-DB1 | Active sweat pores                                                     | Qualitative interpretation of the results                              |
| Marasco and Sansone| 2012 | LivDet 2009     | Feature set combined of (1) residual noise (2) first order statistics  (3) the intensity distribution and (4) individual pore spacing | Improved performance by 33.56% ACE of 4.17% for the SVM and of 4.27% for the MLP (Single attempt for acceptance scenario) |
| Pereira et al.     | 2012 | Own dataset     | Combination of features sets proposed in Refs [64,65]                | ACE of 12.5%                                                           |
| Marcialis et al.   | 2012 | LivDet 2009     | Features that are encountered in the production of artificial fingers | Promising results                                                     |
| Johnson and Schuckers | 2014 | LivDet 2011, 2013 | Perspiration based presentation attack detector                       | EER of 12% on the LivDet 2011 and of 12.7% on the LivDet 2013          |
| Lu et al.          | 2015 | LivDet 2011, ATVS | Five statistical pore distribution features                           | ACE of 7.11% on the LivDet 2011, ACE of 11.4% on the ATVS             |

EER: Equal error rate; FAR: false acceptance rate; FRR: false rejection rate; ACE: average classification error; SVM: support vector machine.

Tan and Schuckers proposed a detection scheme based on perspiration and utilized ridge signal and valley noise analysis. Gray level patterns in spatial, frequency and wavelet domains in combination with classification trees and neural networks were used for the detection. The proposed scheme achieved an EER of 0.9% on their own dataset comprised of 644 bona fide and 570 artificial fingerprint samples.

Espinoza and Champod proved that the pores of the skin of a fingerprint can be used as a feature that can discriminate bona fide and artificial fingerprints. The discriminative factor in their PAD scheme was the difference between the total number of pores in bona fide and artificial fingerprint samples. Their method achieved a 21.2% FAR and an 8.3% FRR using their own dataset.

Marasco and Sansone utilized a feature set combined of the residual noise of the fingerprint image to detect the coarseness of the artificial fingerprint, first-order statistics based on the gray level of each pixel, the intensity distribution to detect PAIs and the individual pore spacing, which is unique to every human. An SVM, decision tree, MLP and Bayesian classifier were chosen as classifiers, depending on the best performance per sensor. This method outperformed other approaches, exhibiting an ACE of 12.5% on the LivDet 2009 dataset, and offered significant gains in speed.

Figure 6. (A) Fingerprint image and (B) pores.
Pereira et al.\textsuperscript{[63]} used a combination of feature sets proposed in Refs.\textsuperscript{[64,65]}. The 17-dimensional feature vector was minimized with the sequential forward selection technique\textsuperscript{[66]}. A SVM and a MLP were used. The authors concluded that the proposed feature set improved performance by 33.56\% and the ACE was increased as more attempts for authentication were allowed. The best performance was reached on a single attempt for the acceptance scenario and it exhibited an ACE of 4.17\% for a SVM and 4.27\% for a MLP classifier. Furthermore, the SVM performed better in general as a classifier, except on biometrics acquired from elderly people where the MLP performed better.

Marcialis et al.\textsuperscript{[67]} proposed the utilization of features that are encountered in the production of artificial fingers. They utilized the Fourier power spectrum of the fingerprint image and concluded that these features can be relevant for discriminating bona fide fingerprints from artificial ones. Moreover, the fusion of features extracted from PAIs and bona fide presentations showed a significant improvement in performance. Their method was evaluated on the LivDet 2009 dataset and showed promising results.

Johnson and Schuckers\textsuperscript{[68]} proposed a perspiration-based PAD. After detecting the pores, a small surrounding area of the pore was inspected to ascertain the perspiration activity. A SVM classifier with a radial basis function kernel was utilized and the method was evaluated on the LivDet 2011-2013 datasets. Experimental results showed that the method performed well, especially when combined with other PAD techniques. More specifically, the best approach exhibited an EER of 12\% on the LivDet 2011 and an EER of 12.7\% on the LivDet 2013.

Lu et al.\textsuperscript{[69]} proposed a method where after the extraction of pore information using a Mexican hat (Mexh) wavelet transform and adaptive Gaussian filters, five statistical pore distribution features were utilized. These features were the pore number (total amount of pores), pore density, mean pore space, variance and the variation coefficient. A SVM was used for classification. This technique exhibited an ACE of 7.11\% on the LivDet 2011 and an ACE of 11.4\% on the ATVS datasets. Table 3 summarizes the aforementioned PAD techniques.

**Image quality features**

In this section, we present the state-of-the-art PAD methods that seek to find detectable differences in the scans of a living finger in comparison to an artificial one. Measures like continuity, clarity and strength of valleys and ridges are being utilized for anti-spoofing. Typically, features extracted from ridge-valleys are utilized but other features were proposed as well, as shown in Table 4. The advantages of these methods are the simplicity, low computational complexity and fast response times\textsuperscript{[14]}.

Tan\textsuperscript{[70]} proposed a PAD method that utilized noise analysis along the valleys in the ridge-valley structure of fingerprint images. Wavelet decomposition was utilized to acquire statistical features in multiresolution scales. Decision trees and neural networks were used for classification, while two datasets were used for evaluation. The first one was comprised of 58 live, 80 artificial and 25 cadaver samples, whilst the second included 28 bona fide and 28 artificial fingerprints. This method exhibited a correct classification rate from 90.9\% to 100\% depending on the technology of the scanner.

Galbally et al.\textsuperscript{[71]} proposed a PAD method that utilized ten different quality features of the image that depend on the ridge strength, continuity and clarity. LDA was used as a classifier. This method achieved an ACE of 6.56\% on the LivDet 2009 dataset.
Table 4. Image quality features

| Ref.       | Year | Dataset | Features                                                                 | Results                                                                                     |
|------------|------|---------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Tan        | 2008 | Own dataset | Noise analysis along the valleys in the ridge-valley structure of fingerprint images | Correct classification rate from 90.9% to 100% depending on the technology of the scanner   |
| Galbally et al. | 2009 | LivDet 2009 | Ten different quality features of the image that depend on Ridge-strength, Ridge-continuity and Ridge-clarity | ACE of 6.56%                                                                                   |
| Lee et al. | 2009 | Own dataset | The standard deviation of the fractional Fourier transform of a line that was detected when a fingerprint image was transformed into the spatial frequency domain | Error rate of 11.4%                                                                           |
| Jin et al. | 2011 | BERC    | Fusion of spectral band, middle ridge and valley line                      | Classification error rate approx. 6%                                                          |
| Galbally et al. | 2012 | LivDet 2009, ATVS | Ridge strength, ridge continuity, ridge clarity, integrity of the ridge-valley structure | ACE of 12.5% on the LivDet 2009 ACE on the ATVS was 5.4%                                       |
| Galbally et al. | 2014 | LivDet 2009 | 25 image quality features                                                  | APCER < 13% and BPCER ≤ 14%                                                                  |
| Sharma and Dey | 2019 | LivDet 2009, 2011, 2013, 2015 | 13 quality features that depend on the ridge-valley shape | ACE of 5.3% on the LivDet 2009 ACE of 7.80% on the LivDet 2011 ACE of 7.4% on the LivDet 2013 ACE of 4.2% on the LivDet 2015 |

ACE: Average classification error; APCER: attack presentation classification error rate; BPCER: bona fide presentation classification error rate; BERC: Biometrics Engineering Research Center.

Lee et al. proposed a novel PAD method that measured the standard deviation of the fractional Fourier transform of a line, which was detected when a fingerprint image was transformed into the spatial frequency domain. This transformation was accomplished with the use of a two-dimensional fast Fourier transform. For a dataset of 3750 bona fide and artificial fingerprint samples in total, this method exhibited an error rate of 11.4% when a certain region was utilized after the fractional Fourier transform.

In Ref., a method based on the fusion of the spectral band, middle ridge and valley line was proposed. SVMs and quadratic classifiers were used for the classification. This system was tested on the Biometrics Engineering Research Center dataset and exhibited better security than other fingerprint recognition schemes. It also has the advantage that it uses only one fingerprint. A classification error of ~6% was exhibited with the utilization of all three proposed features.

In Ref., image quality features that depend on the ridge strength, directionality, continuity and clarity and the integrity of the ridge-valley structure or estimated verification were measured to classify a fingerprint as artificial or not. The classification was performed by a LDA classifier. More specifically, their method showed ACEs of 12.5% and 5.4% on the LivDet 2009 and ATVS datasets, respectively. Compared to other similar methods, the fact that only one sample is needed, makes the sample acquisition process faster and less invasive.

In another work of Galbally et al., 25 image quality features were utilized to discriminate bona fide samples from artificial ones. Their method was tested on the LivDet 2009 dataset and achieved an APCER of < 13% and a BPCER of ≤ 14%.

Sharma and Dey proposed an architecture that utilized five novel and eight existing quality features that depend on the ridge-valley shape and are sensor independent. Thus, a 13-dimensional feature vector was formed and a sequential forward floating selection (SFFS) and a random forest feature selection algorithm were deployed to select the optimal feature set. A SVM, random forest and gradient boosted tree were utilized for classification. This approach showed ACEs of 5.3% on LivDet 2009, 7.80% on LivDet 2011, 7.4% on LivDet 2013 and 4.2% on LivDet 2015.
Textural features

Researchers have found that the textural features [Figure 7] of the fingertip, such as smoothness and morphology, can be used to distinguish real fingerprints from artificial ones\cite{78,79}. Methods belonging to this category make use of such textural features. The extracted features are then presented as input to a classifier, which in most cases is an SVM. These methods are described below and summarized in Table 5.

Nikam and Agarwal\cite{22} utilized curvelet features, such as energy, co-occurrence and fused signatures, to discriminate bona fide samples from artificial ones. To limit the dimensionality of the feature vector, they applied an SFFS algorithm. An ensemble classifier, on the basis of the “majority voting rule”, of three independent classifiers, namely, AdaBoost.M1, an SVM and an alternating decision tree, was used for classification. Their method was tested on their own dataset comprising of 185 bona fide and 240 artificial samples and on the FVC 2004\cite{80} dataset comprised of only bona fide samples. When the fusion of energy and co-occurrence signatures occurred, the proposed technique achieved a 99.29% correct classification rate, which outperformed the wavelet and power spectrum PAD techniques.

Ghiani et al.\cite{81} proposed a new feature set, extracted by the deployment of the textural analysis of the acquired image spectrum, known as rotation invariant local phase quantization (LPQ). This method exhibited an average EER of 12.3% on the LivDet 2011 dataset.

Gragnaniello et al.\cite{82} used textural classification by utilizing the Weber local descriptor (WLD). A linear kernel SVM classifier was used for classification. The classifier was trained on discriminative features build from the joint histograms of the differential excitation and orientation of every pixel of the acquired sample. This method presented good performance and it was further improved with the integration of other LPQ descriptors, especially if the latter relied on different image attributes. The ACE concerning WLD was 2.95%, while when the WLD and LPQ were combined, the ACE was 1.14% on the LivDet 2009 dataset. Experimental results on the LivDet 2011 dataset showed an ACE of 15.33% for the WLD, while the ACE for the fusion of the WLD and LPQ descriptors was 7.86%.

Jia et al.\cite{83} developed a descriptor known as multi-scale block local ternary patterns that depend on the average value of the pixel blocks. The differences amongst the pixels and the threshold constitute the ternary pattern. This method showed an ACE of 9.8% on the LivDet 2011 dataset.

Pereira et al.\cite{84} proposed spatial surface coarseness analysis (SSCA). SSCA is based on wavelet analysis of the fingerprint surface with the addition of spatial features. A polynomial kernel SVM was used for classification. SSCA exhibited an ACE of 12.8% on the LivDet 2011 dataset.

Ghiani et al.\cite{85} introduced a novel descriptor known as binarized statistical image features (BSIFs). This descriptor encodes the local fingerprint texture on a feature vector. This method was evaluated on the LivDet 2011 dataset and achieved an EER of 7.215% when a $7 \times 7$ window size was used in conjunction with a 4096-dimensional feature vector.

Jia et al.\cite{86} introduced a novel descriptor known as a multi-scale local binary pattern (MSLBP). The MSLBP can be implemented in two ways and both can achieve good performance for PAD. They tested MSLBP on the LivDet datasets and the best MSLBP implementation exhibited an ACE of 7.475%.
Table 5. Textural features

| Ref. | Year | Dataset | Method | Results |
|------|------|---------|--------|---------|
| Nikam and Agarwal[82] | 2010 | Own dataset | Curvelet features such as energy, co-occurrence and fused signatures | 99.29% classification rate |
| Ghiani et al.[83] | 2012 | LivDet 2011 | Textural analysis of the acquired image spectrum | Average EER of 12.3% |
| Gragnaniello et al.[84] | 2013 | LivDet 2009, 2011 | WLD | ACE was 1.14% on LivDet 2009 datasets, ACE of 15.33% (WLD) and 7.86% (WLD + LPQ) on the LivDet 2011 |
| Jia et al.[85] | 2013 | LivDet 2011 | Multi-scale block local ternary patterns | ACE of 9.8% |
| Pereira et al.[86] | 2013 | LivDet 2011 | Spatial surface coarseness analysis | ACE of 12.8% |
| Ghiani et al.[87] | 2013 | LivDet 2011 | Binarized statistical image features | EER of 7.215% |
| Jia et al.[88] | 2014 | LivDet 2011 | Multi-scale local binary pattern | ACE of 7.475% |
| Gragnaniello et al.[89] | 2014 | LivDet 2009 | Wavelet-Markov local descriptor | ACE of 2.8% |
| Zhang et al.[90] | 2014 | LivDet 2011, 2013 | Wavelet analysis and LBP | ACE of 11.47% on the LivDet 2011, ACE of 11.02% on the LivDet 2013 |
| Gottschlich et al.[91] | 2014 | LivDet 2013 | Histograms of invariant gradients | ACE of 12.2% |
| Jiang and Liu[92] | 2015 | LivDet 2009, 2011 | Co-occurrence matrices from image gradients | ACE of 6.8% on the LivDet 2009, ACE of 10.98% on the LivDet 2011 |
| Gragnaniello et al.[93] | 2015 | LivDet 2011 | Local contrast phase descriptor | ACE of 5.7% |
| Gottschlich[94] | 2016 | LivDet 2013 | Convolution comparison pattern | Accuracy of 93% |
| Dubey et al.[95] | 2016 | LivDet 2011, 2013 | SURF features and pyramid extension of the histograms of oriented gradient in conjunction with texture features | EER of 3.95% on the LivDet 2011, ACE of 2.27% on the LivDet 2013 |
| Yuan et al.[96] | 2016 | LivDet 2009, 2011, 2013 | Angular second moment, entropy, inverse differential moment and correlation to form the feature vector | ACE of 15.32% on the LivDet 2013, ACE of 9.28% on the LivDet 2011, ACE of 7.92 on the LivDet 2009 |
| Kim and Jung[97] | 2016 | LivDet 2009, 2011 | Local accumulate smoothing pattern descriptor | Classification rate of 88.49% on the LivDet 2009 and of 78.78% on the LivDet 2011 |
| Ghiani et al.[98] | 2017 | LivDet 2009, 2011, 2013 | Binarized statistical image features | ACE of 3.03% on the LivDet 2009, ACE of 9.62% on the LivDet 2011, ACE of 5.71% on the LivDet 2013 |
| Kim[99] | 2017 | ATVS, LivDet 2009, 2011, 2013, 2015 | Local coherence patterns | Accuracy of 93.49% on the ATVS datasets and of 78.02% on the LivDet datasets |
| Kumpituck et al.[100] | 2017 | LivDet 2009, 2013 | Wavelet-based local binary pattern | ACE of 9.95% on the LivDet 2009-2013 datasets |
| Xie et al.[101] | 2017 | LivDet 2009, 2011 | Co-occurrence matrices from image gradients | ACE of 6.2% on the LivDet 2009, ACE of 6.635% on the LivDet 2011 |
| González-Soler et al.[102] | 2017 | LivDet 2011 | SIFT features encoded with a spatial histogram of visual words | ACE of 4.7% |
| Kundargi and Karandikar[103] | 2018 | LivDet 2011 | Local binary pattern texture descriptor with wavelet transform | ACE of 8.3% |
| Jiang and Liu[104] | 2018 | LivDet 2011 | Uniform local binary pattern in three-layer spatial Gaussian pyramids | ACE of 21.205% |
| Mehta et al.[105] | 2018 | LivDet 2011 | Combined Shepard magnitude and orientation | Average error rate of 5.8, 2.2, and 5.3 on the LivDet 2011, 2013, and 2015, respectively |
| Xia et al.[106] | 2020 | LivDet 2011, 2013, 2015 | Weber local binary descriptor | ACE of 9.6775% on the LivDet 2015, ACE of 1.89% on the LivDet 2013, ACE of 5.96% on the LivDet 2011 |
| Tan et al.[107] | 2020 | LivDet 2011, 2013 | Guided filtering and hybrid image analysis | Average accuracy of 94.33% on the LivDet 2011 and of 98.08% on the LivDet 2013 |
| Kumar and Singh[108] | 2020 | ATVS, FVC 2000, 2002, 2004 | Presentation attack detection module utilizing supervised learning with minutiae extraction | Average performance of 96.06% |

WLD: Weber local descriptor; EER: equal error rate; LPQ: local phase quantization; ACE: average classification error; SIFT: scale invariant feature transform; SURF: speeded-up robust feature.
Gragnaniello et al.\cite{87} developed a method based on the wavelet-Markov local descriptor. The feature vector was formed by exploiting joint dependencies among wavelet coefficients. To limit the dimensionality of the feature vector, principal component analysis (PCA) was used. An SVM classifier achieved an ACE of 2.8% on the LivDet 2009 dataset.

Zhang et al.\cite{88} proposed a method that depends on wavelet analysis and LBP. Wavelet analysis was applied to produce the denoised image and the residual noise image. The LBP histograms were constructed based on the residual noise and denoised images. An SVM based on a polynomial kernel was deployed for classification. This approach offered ACEs of 11.47% on the LivDet 2011 and 11.02% on the LivDet 2013.

Gottschlich et al.\cite{89} proposed a descriptor known as histograms of invariant gradients. Fingerprint discrimination was based on multiple histograms of invariant gradients, computed from spatial neighborhoods within the fingerprint. The best variation of the proposed method achieved an ACE of 12.2% on the LivDet 2013 dataset.

Jiang and Liu\cite{90} used co-occurrence matrices from image gradients for feature extraction. The image was first quantized to decrease the dimensionality and increase the usefulness of the feature vector. Afterwards, the image differences were calculated from adjacent quantized pixels along the horizontal and vertical axes. These differences were then truncated in a range within a specific threshold. Finally, the truncated differences were used to produce the co-occurrence matrices, which were utilized as features. An SVM was trained on two datasets and the proposed method achieved ACEs of 6.8% and 10.98% on the LivDet 2009 and 2011 datasets, respectively.

Gragnaniello et al.\cite{91} developed a new local descriptor known as the local contrast phase. After the analysis of the acquired sample in the spatial and frequency domains, information on the local amplitude contrast and local behavior of the image was gathered depending on the selected transform coefficients. The two-dimensional contrast-phase histogram crafted from the information collected in the previous stage was used...

![Figure 7. Textural characteristics of a real fingerprint image\cite{22}.](image-url)
as a feature vector. A linear-kernel SVM classifier was utilized and an ACE of 5.7% was found for the LivDet 2011 dataset.

Gottschlich\[92] introduced a novel local image descriptor known as the convolution comparison pattern. This descriptor utilized rotation invariant image patches to compute the discrete cosine transform (DCT) and the comparison of pairs of two DCT coefficients to obtain binary patterns, which are summarized into histograms, comprised of the relative frequencies of pattern occurrences. The feature vector was acquired by the concatenation of multiple histograms and the classification was performed by an SVM. This descriptor, with the use of a specific configuration, achieved an accuracy of 93% on the LivDet 2013 dataset.

Dubey et al.\[93] used low level gradient features collected with the utilization of speeded-up robust features and the pyramid extension of the histograms of oriented gradient in conjunction with textural features acquired with the use of Gabor wavelets. This architecture exhibited an EER of 3.95% on the LivDet 2011 and achieved an ACE of 2.27% on the LivDet 2013 dataset.

Yuan et al.\[94] proposed the angular second moment, entropy and inverse differential moment and correlation to form the feature vector. These parameters were used as textural features and were extracted from eight difference co-occurrence matrices. The proposed method achieved ACEs of 15.32% on the LivDet 2013 dataset, 9.28% on the LivDet 2011 dataset and 7.92% on the LivDet 2009 dataset.

Kim and Jung\[95] proposed the local accumulate smoothing pattern descriptor. The feature vector of this classifier was based on the local textural patterns, as they were represented by the accumulated smoothing space. A linear SVM classifier was used for classification. This architecture achieved a classification rate of 88.49% on the LivDet 2009 dataset and of 78.78% on the LivDet 2011 dataset.

Ghiani et al.\[96] suggested a descriptor entitled BSIFs. BSIFs share similarities to LBPs and LPQ, but the formed feature vector is based on a set of filters that are learnt from natural images. The proposed descriptor achieved ACEs of 3.03% on the LivDet 2009 dataset, 9.62% on the LivDet 2011 dataset and 5.71% on the LivDet 2013 dataset.

Kim\[97] defined and utilized Local coherence patterns (LCPs) [Figure 8] as features in the dominant direction of the captured fingerprint image to determine if a fingerprint was artificial or not. This method exploited the fact that artificial fingerprints tend to disperse differently in the image gradient field than the bona fide ones. The classification was performed by a linear SVM. The LCP descriptor exhibited an accuracy of 93.49% on the ATVS Dataset and an accuracy of 78.02% on the LivDet 2009, 2011, 2013 and 2015 datasets.

Kumpituck et al.\[98] proposed the wavelet-based local binary pattern, which is based on the utilization of the LBP for capturing the local appearance of the sub-band images. Prior to the utilization of the LBP, the fingerprint image was decomposed by the two-dimensional discrete wavelet transform. An SVM was used for classification. The proposed method achieved an ACE of 9.95% on the LivDet 2009-2013 datasets.

Xia et al.\[99] proposed a method that utilized co-occurrence matrices constructed from image gradients. Second and third-order co-occurrence matrices were used to train an SVM classifier. When third-order co-occurrence matrices were utilized as features, the proposed architecture achieved ACEs of 6.2% on the LivDet 2009 and 6.635% on the LivDet 2011.
González-Soler et al.\textsuperscript{[100]} proposed a method based on the bag of words algorithm. After extracting the scale invariant feature transform (SIFT) features, they encoded them with a spatial histogram of visual words. The classification was performed by a SVM through a feature map. This architecture achieved an ACE of 4.7\% on the LivDet 2011 dataset.

Kundargi and Karandikar\textsuperscript{[101]} proposed a LBP texture descriptor with a wavelet transform that utilized the textural characteristics that differ in bona fide and artificial samples due to variations at the gray level of the image. The fingerprints were classified by linear and RBF kernel SVM classifiers. This method offered an ACE of 8.3\% on the LivDet 2011 dataset.

Jiang and Liu\textsuperscript{[102]} introduced a method that utilized the uniform local binary pattern in three-layer spatial Gaussian pyramids. This method achieved a 21.205\% ACE on the LivDet 2011 dataset.

Mehboob et al.\textsuperscript{[103]} proposed a novel descriptor known as the combined Shepard magnitude and orientation. This method extracts the global features of the fingerprint by computing the relation between the perceived Shepard magnitude and initial pixel intensities in the spatial domain. To achieve this, the fingerprint is considered as a two-dimensional vector. The descriptor first constructs perceived spatial stimuli by combining the logarithmic function of initial pixel intensities and the Shepard magnitude (SM) in the spatial domain. Next, the phase information (CO) is computed in the frequency domain. Finally, the SM and CO are concatenated and represented as a two-dimensional histogram. The rotation invariant version of LPQ was utilized for characteristic orientation computation. An SVM was used for classification and average error rates of 5.8\%, 2.2\% and 5.3\% on the LivDet 2011, 2013 and 2015 datasets were achieved, respectively.

Xia et al.\textsuperscript{[104]} also suggested a novel local descriptor entitled the Weber local binary descriptor (WLBD) that consists of two components that were used to extract intensity-variance and orientation features. The first is the local binary differential excitation module that captures the spatial structure of the local image patch and the second is the local binary gradient orientation module that is designed to extract gradient orientation from center-symmetric pixel pairs. The output of these components formed a discriminative feature vector [Figure 9] that was used as the input for an SVM classifier. The WLBD achieved ACEs of 9.67\% on the LivDet 2015 dataset, 1.89\% on the LivDet 2013 dataset and 5.96\% on the LivDet 2011 dataset.
In Ref. [106], a method utilizing the guided filtering and hybrid image analysis was proposed. After performing ROI extraction and guided filtering to acquire the denoised image, the co-occurrence of adjacent LBPs (CoALBPs) descriptor was utilized to form the feature vector from the original and the denoised image. An SVM with an RBF kernel was used and the proposed method exhibited average accuracies of 94.33% on the LivDet 2011 and 98.08% on the LivDet 2013 datasets. Moreover, the computation time was 4.5 times faster in comparison to deep learning methods.

Kumar and Singh [107] proposed a fingerprint authentication system with a PAD module, utilizing supervised learning with minutiae extraction and classification with an SVM. Features like homogeneity, contrast, energy, entropy and mean last histogram were extracted. The proposed module achieved an average performance of 96.06% on the FVS [108] and ATVS datasets.

**Neural networks**

Neural networks have been used for PAD with great success. Most of these methods share the similarity of the segmentation of the background or foreground of the fingerprint image and the extraction of local patches of the image that include the ROI. In recent years, researchers utilized deep learning methods to detect PAs. Deep neural networks like CNNs have been extensively utilized for several security tasks like steganalysis [109, 110], but nowadays they are also used for fingerprint PAD. CNNs are either utilized as feature extractors or even perform the classification. There are also proposed methods in the literature that use transfer learning. Transfer learning is the reuse of a pre-trained neural network on a new problem, i.e., it exploits the knowledge gained from a previous task to improve the generalization to another. Other methods exploit either generative adversarial networks (GANs) or restricted Boltzmann machines for PAD. Table 6 summarizes the state-of-the-art methods that utilize a neural network (shallow or deep) as a feature extractor or classifier.

Menotti et al. [111] proposed a detection technique that utilized neural networks. One of their approaches utilized an optimized convolutional neural network and an SVM for classification. A second approach was based on the backpropagation algorithm for filter optimization. They concluded that the combination of the two approaches performed better and achieved an ACC of 98.97% on the LivDet 2013.

Nogueira et al. [112] proved that pretrained CNNs achieve high accuracy in PAD. In their work, they analyzed the false fingerprint detection performance of VGG [109] and AlexNet [113] [Figure 10] that were trained on natural images and further tuned with fingerprint samples. The LivDet 2009, 2011 and 2013 datasets were used and the proposed CNN-VGG showed an ACE of 2.9% and won the LivDet 2015 competition.

![Figure 9.](image) (A) Live fingerprint image. (B) WLD-DE, (C) LBP and (D) LBDE calculated from (A) [104].
Table 6. Neural networks

| Ref.            | Year | Dataset                          | Neural network                                                                 | Results                                                                 |
|-----------------|------|----------------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Menotti et al.  | 2015 | LivDet 2013                      | Combination of CNN architecture and backpropagation algorithm for filter optimization | ACC of 98.97%                                                          |
| Nogueira et al. | 2016 | LivDet 2009, 2011, 2013          | CNN-VGG                                                                       | ACE of 2.9%                                                            |
| Kim et al.      | 2016 | LivDet 2013                      | Deep belief network                                                           | ACC of 97.10%                                                          |
| Marasco et al.  | 2016 | LivDet 2013                      | 3 CNNs                                                                        | CaffeNet (96.5%), GoogleLeNet (96.6%), Siamese (93.1%)                  |
| Pala and Bhanu  | 2017 | LivDet 2009, 2011, 2013          | Triplet of CNNs                                                               | ACE 1.75%                                                              |
| Chugh et al.    | 2018 | LivDet 2011, 2015, MSU-FPAD, Precise Biometrics Spoof-Kit | CNN                                                                          | APCER < 7.3% and an BPCER = 1%                                         |
| Jung and Heo    | 2018 | LivDet 2015                      | CNN                                                                          | Average accuracy 95.3%                                                |
| Pinto et al.    | 2018 | LivDet 2009, 2013                | Deep learning                                                                 | Not good generalization to unknown PAIs                                |
| Park et al.     | 2018 | LivDet 2011, 2013, 2015          | Patch-based PAD method that utilized a fully convolutional neural network      | ACE of 1.35%                                                          |
| Park et al.     | 2019 | LivDet 2011, 2013, 2015          | CNN                                                                          | ACE of 1.43%                                                          |
| Zhang et al.    | 2019 | LivDet 2017                      | Residual convolutional neural network                                         | Accuracy of 95.25%                                                    |
| Yuan et al.     | 2020 | LivDet 2013, 2015                | Autoencoders                                                                  | Accuracy of 19.62% on the LivDet 2013 ACE of 18% on the LivDet 2015    |
| Pereira et al.  | 2020 | LivDet 2015                      | GAN                                                                           | APCER of 0.60%                                                        |
| Uliyan et al.   | 2020 | LivDet 2013                      | Discriminative restricted Boltzmann machines in combination with deep Boltzmann machine | ACE of 3.6 %                                                          |
| Zhang et al.    | 2020 | LivDet 2013, 2015                | CNN                                                                           | ACE of 1.76% over all sensors ACE of 0.25% on the LivDet 2013          |
| Jian et al.     | 2021 | LivDet 2009-2015                 | Densely connected convolution network (DenseNet) along with a genetic algorithm utilized for network optimization | 98.22% accuracy                                                       |

ACC: Average detection accuracy; CNN: convolutional neural network; BPCER: bona fide presentation classification error rate; APCER: attack presentation classification error rate; PAIs: presentation attack instruments; PAD: presentation attack detection; GAN: generative adversarial network.

Kim et al. proposed an architecture based on a deep belief network (DBN) with multiple layers of a restricted Boltzmann machine, trained on a set of bona fide and artificial samples. The proposed DBN, when trained with augmented data, achieved an average accuracy of 97.10% on the LivDet 2013 dataset.
Marasco et al.\textsuperscript{[115]} experimented on the effectiveness of CNNs as PAD methods. They tested three CNNs that achieved the best accuracy on the LivDet 2013 dataset, namely, CaffeNet (96.5\%), GoogLeNet (96.6\%) and Siamese (93.1\%). They have also indicated that CNNs exhibited the ability to successfully adapt to PAD problems (if they were pre-trained on the ImageNet dataset\textsuperscript{[116]}) and achieved an area under the curve in the range of -3.6\% to +4.6\%.

Pala and Bhanu\textsuperscript{[117]} proposed a method based on a triplet of CNNs. Their method employs a variant of the triplet objective function that considers representations of fingerprint images, where the distance between feature points is used to discriminate artificial and bona fide samples. Their architecture scored an ACE of 1.75\% on the LivDet 2009, 2011 and 2013 datasets.

Chugh et al.\textsuperscript{[118]} proposed a method that was based on CNNs and minutiae information. For the training of the CNN, aligned and centered local patches (96 × 96 pixels) were utilized. They defined a “spoofness” score, which is the output of the softmax layer of the trained CNN. The “spoofness” score had a range of 0 to 1, where 1 denoted that the sample was artificial. They also crafted the Fingerprint Spoof Buster, which is a graphical user interface that permits the visual evaluation of the fingerprint by the human operator of the scanner. The proposed CNN was evaluated on the LivDet 2011, 2013 and 2015 datasets, as well as the MSU-FPAD and Precise Biometrics Spoof-Kit datasets. Experimental results showed a significant reduction in error rates, with an APCER lower than 7.3\% and a BPCER of 1\%.

Jung and Heo\textsuperscript{[119]} proposed a method, where the proposed CNN was trained directly from fingerprints, used the squared error layer and had no fully connected layer. The proposed architecture presented a higher average accuracy of 95.3\% on the LivDet 2015 dataset compared to other existing methods.

Pinto et al.\textsuperscript{[120]} utilized deep learning and concluded that it achieves very good performance in PAD tasks. The main drawback was the poor performance of deep learning when encountered PAs with instruments that were either not included at all or not included with a satisfactory number of samples in the training data. They also concluded that the best reliability is presented when models are based on both “handcrafted” and “data-driven” solutions.

Park et al.\textsuperscript{[121]} proposed a patch-based PAD method that utilized a fully convolutional neural network, the so-called Fire module of SqueezeNet, which had fewer parameters and demands, with only 2.0 Mb of memory required. This method utilized an optimal threshold, as opposed to the voting method, which decreased the misdetection rate. This architecture achieved an ACE of 1.35\% on the LivDet 2011, 2013 and 2015 datasets, when the training was carried out through data augmentation and the patch size was 48 × 48 pixels.

Park et al.\textsuperscript{[122]} proposed a convolutional network known as the patch-based CNN because it utilizes patches (small ROIs) of the fingerprint image. They used three categories for classification, i.e., live, artificial and background. The proposed architecture, when used on 48 × 48 pixel patches, achieved an ACE of 1.43\% on the LivDet 2011, 2013 and 2015 datasets in a radically reduced execution time.

Zhang et al.\textsuperscript{[123]} proposed a lightweight residual convolutional neural network (Slim-ResCNN) that requires less processing time and is robust to overfitting. Local patch extraction was based on statistical histograms and the center of gravity. The proposed method exhibited an overall accuracy of 95.25\% on the LivDet 2017 dataset.
Yuan et al.\cite{123} proposed a real-time fingerprint PAD method based on autoencoders. Automatic feature extraction was performed with the use of a stacked autoencoder. Unsupervised learning was used for pre-training, while the detection was performed with the use of supervised training. A Softmax classifier was utilized for classification. This method achieved ACEs of 19.62% on the LivDet 2013 and 18% on the LivDet 2015.

Pereira et al.\cite{124} tackled the PAD generalization problem, especially for PAs performed with materials not seen in training, with the use of an adversarial training methodology. The proposed method was evaluated with a MLP classifier and a CNN. The regularized CNN approach achieved an APCER of 0.60% on the LivDet 2015 dataset.

Uliyan et al.\cite{125} utilized discriminative restricted Boltzmann machines (DRBMs) in combination with a deep Boltzmann machine (DBM) to extract deep features from the acquired samples. A K-NN classifier was used for classification. The proposed DRBM-DBM architecture exhibited an ACE of 3.6% on the LivDet 2013 dataset.

Zhang et al.\cite{126} proposed a lightweight CNN known as FLD to achieve improved PAD on new materials and to minimize complexity. To address the issue of global average pooling, an attention pooling layer was used. Moreover, a novel block structure (Block D&R) was introduced where the residual path is integrated into the original dense block. FLDNet exhibited ACEs of 1.76%, over all sensors, on the LivDet 2015 dataset and 0.25% on the LivDet 2013 dataset.

Jian et al.\cite{127} proposed a densely connected convolutional network (DenseNet) along with a genetic algorithm utilized for network optimization. The genetic algorithm can automatically optimize DenseNet by finding the optimal structure from the solution space. The proposed model achieved 98.22% accuracy on a testing set containing the LivDet 2009-2015 datasets.

**Fusion of features**

In this category, approaches that combine features from the different aforementioned categories are presented. Moreover, hybrid methods that utilize both static and dynamic features will be discussed\cite{128-134}. These methods exploit the advantages and minimize the drawbacks of the aforementioned PAD methods, as these were presented in Dynamic methods, Anatomical or physiological features, Image quality features, Textural features and Neural networks. A summary of the presented methods is given in Table 7.

Derakhshani et al.\cite{128} proposed a method that detected the perspiration phenomenon and it was based on static and dynamic features acquired from two fingerprint samples captured with a time interval of 5 s. One static and four dynamic features were used as input to a back-propagation neural network, which was utilized for classification. The dataset for training and testing was comprised of 18 sets of fingerprint samples from live individuals, 18 from cadavers and 18 from spoof materials. On this dataset, the proposed scheme achieved an accuracy of 100%.

Parthasaradhi et al.\cite{128} proposed a method that depends on static features and on the changes due to perspiration to fingerprint images taken at 0, 2 and 5 s. By deploying a weight decade method during the training of a neural network classifier, they concluded that there was significant improvement in performance. On an image sequence dataset of 33 live subjects, 14 cadaver fingers and 33 artificial samples, their method achieved an FLR of 0% and an FSA in the range of 0%-18.2% depending on the sensor technology.
| Ref. | Year | Dataset | Feature extraction | Results |
|------|------|---------|--------------------|---------|
| Derakhshani et al. | 2003 | Own dataset | Detection of perspiration phenomenon | Accuracy of 100% |
| Parthasaradhi et al. | 2004 | Own dataset | Detection of perspiration phenomenon | FLR of 0% and FSA in the range of 0%-18.2% depending on the sensor technology |
| Parthasaradhi et al. | 2005 | Own dataset | Detection of perspiration phenomenon | FLR in the range of 6.77%-20%, FSA in the range of 5%-20% for optical, FLR in the range of 0%-26.9%, FSA in the range of 4.6%-14.3% for capacitive and FLR in the range of 6.9%-38.5%, FSA in the range of 0%-19% for electro optical |
| Tan and Schuckers | 2005 | Own dataset | Static and dynamic features acquired from intensity histograms | FLR of 0%, FSA of 8.3% for optical sensor, FLR of 6.7%, FSA of 0% for capacitive sensor and FLR of 7.7%, FSA of 5.3% for electro optical sensor |
| Tan and Schuckers | 2006 | Own dataset | Static and dynamic features acquired from intensity histograms | In the range of 90% to 100% for some scanners |
| Jia and Cai | 2007 | Own dataset | Detection of perspiration and skin elasticity | EER of 4.49% |
| Plesh et al. | 2019 | Own dataset | Detection of perspiration, skin elasticity and displacement of blood | Mean APCER of 3.55 % at 1.0% BPCER, mean APCER of 0.626% at 0.2% BPCER and standard deviation of 1.96% at 1.0% BPCER |
| Nogueira et al. | 2014 | LivDet 2009, 2011, 2013 | CNN and LBP for feature extraction | ACE of 4.71% |
| Yuan et al. | 2019 | LivDet 2013 | BP neural network | ACE of 6.78% |
| Agarwal and Chowdary | 2020 | LivDet 2011 dataset | Stacking and bagging ensemble learning approaches | Stacking average accuracy was 80.76% Bagging average accuracy was 75.12% |
| Anusha et al. | 2020 | LivDet 2011, 2013, 2015 | LBP and Gabor filters to extract features | ACE of 0.48%, 0.84%, 0.28% and 1.16% on the LivDet 2017, 2015, 2013 and 2011, respectively |
| Agarwal and Bansal | 2020 | LivDet 2013, 2015 | Fusion of pores perspiration and texture features | ACE of 0.1866% on the LivDet 2013 ACE of 0.3233% on the LivDet 2015 |
| Li et al. | 2020 | LivDet 2011, 2013, 2015 | Features extraction with SIFT, LBP and HOG | ACE of 4.6% on the LivDet 2011 ACE of 3.48% on the LivDet 2013 ACE of 4.03% on the LivDet 2015 |
| Sharma and Selwal | 2021 | LivDet 2009, 2011, 2013, 2015 | Three local and adaptive textural image features acquired with the use of LABP, CLBP and BSIF texture descriptors | ACER of 4.11% on the LivDet 2009, ACER of 3.19% on the LivDet 2011, ACER of 2.88% on the LivDet 2013, ACER of 2.97% on the LivDet 2015 |

FLR: False live rejection; FSA: false spoof acceptance; EER: equal error rate; APCER: attack presentation classification error rate; BPCER: bona fide presentation classification error rate; ACE: average classification error; CNN: convolutional neural network; LBP: local binary pattern; BP: backpropagation; SIFT: scale invariant feature transform; HOG: histograms of oriented gradients; ACER: average classification error rate.

In an extension of their previous work\[129\], Parthasaradhi et al.\[130\] used several classification methods, a shorter time window, a more diverse dataset and included other fingerprint sensor technologies. One static and six dynamic measures were used for classification and all classifiers achieved ~90% accuracy. More specifically, on a dataset of 75 samples per scanner, the proposed method achieved an FLR in the range of 6.77%-20% and an FSA in the range of 5%-20% for an optical scanner, and an FLR of 0%-26.9% and an FSA of 4.6%-14.3% for a capacitive scanner. Finally, the same method exhibited an FLR of 6.9%-38.5% and an FSA of 0%-19% for electro-optical scanners.
Tan and Schuckers\textsuperscript{[13]} proposed a PAD method that depends on the static and dynamic features acquired from intensity histograms of the 0 and 5 s images of a fingerprint. On a dataset of sequences of images (30 bona fide, 40 artificial and 14 cadaver fingerprints) captured by three different scanners, their method exhibited an FLR of 0% and an FSA of 8.3% for an optical sensor. The same method exhibited an FLR of 6.7% and an FSA of 0% for a capacitive sensor, and an FLR of 7.7% and an FSA of 5.3% for an electro-optical sensor.

Tan and Schuckers\textsuperscript{[132]} extended their previous work\textsuperscript{[131]}, by reducing the time between capturing fingerprint samples to 2 s instead of 5 s. On a dataset of 58 live, 50 artificial and 25 cadaver fingerprints, the augmented method showed an accuracy of 90%-100% for some scanners by using a classification tree.

Jia and Cai\textsuperscript{[133]} proposed an extension of their previous work\textsuperscript{[50]}. In this study, five features were utilized. Two of them represented skin elasticity, whilst the other three represented perspiration. This method computed two static features, while the remaining three were dynamic features. The proposed scheme was tested on a dataset comprising of 770 image sequences and achieved an EER of 4.49%.

Plesh \textit{et al.}\textsuperscript{[134]} used a sensor with time-series and color sensing capabilities to capture a gray scale static image and a time-series color capture simultaneously. A dynamic color capture has the ability to measure signs, such as the perspiration, skin elasticity deformation and the displacement of blood that occurs when a finger is pressed. In their work, the second capture (the dynamic one) was utilized for classification with two methods. Initially, static-temporal feature engineering was utilized and then the InceptionV3 CNN\textsuperscript{[135]} trained on ImageNet was used for classification. In their work, the classification performance was evaluated with the use of a fully connected DNN utilizing solely static or dynamic features and a fusion of the two feature sets. On a custom dataset comprising of over 36,000 image sequences and a state-of-the-art set of PA techniques, the approach that utilized the fusion of both static and dynamic features achieved a mean APCER, at a 1.0% BPCER operation point, of 3.55 %, a mean APCER, at a 0.2% BPCER operation point, of 0.626% and a standard deviation, at 1.0% BPCER, of 1.96%.

Nogueira \textit{et al.}\textsuperscript{[136]} evaluated the efficiency of two feature extraction techniques with data augmentation on an SVM classifier. After the preprocessing step, two feature extraction techniques, i.e., a CNN and LBP, were conducted and randomized PCA was utilized for dimensionality reduction. The proposed CNN, with the use of augmented data, exhibited an ACE of 4.71% on the LivDet 2009, 2011 and 2013 datasets.

Yuan \textit{et al.}\textsuperscript{[137]} suggested a backpropagation neural network that utilized gradient values calculated by the Laplacian operator. They also presented a system that used the methods shown in Ref.\textsuperscript{[94]} and Ref.\textsuperscript{[138]} to create more productive input data and category labels. This architecture offered an ACE of 6.78% on the LivDet 2013 dataset.

Agarwal and Chowdary\textsuperscript{[139]} proposed the utilization of stacking and bagging ensemble learning approaches in fingerprint PAD. The suggested algorithms considered the similarities of datasets utilized for PAD. Moreover, they are adaptive because they comply with the features extracted from bona fide and artificial fingerprint samples. The proposed algorithms achieved better performance in accuracy and false positive rate than the best individual base classifier. More specifically, the stacking average accuracy was 80.76%, while the bagging average accuracy was 75.12% on the LivDet 2011 dataset.
Anusha et al.\cite{140} proposed an architecture that utilized global image and local patch features. It used LBP and Gabor filters in the preprocessing process to extract features using DenseNet\cite{141}. For the extraction of local patch features, a second DenseNet was used in combination of a channel and spatial attention network module\cite{142}. For patch discrimination, a novel patch attention network was proposed. This network was also used for feature fusion. This method showed average accuracies of 99.52%, 99.16% and 99.72% on the LivDet 2017, 2015 and 2011, respectively.

Agarwal and Bansal\cite{143} proposed the fusion of pores, perspiration and textural features for PAD. The dimensionality of the extracted feature vector was reduced with the use of a stacked autoencoder pretrained in a greedy layer wise manner. A supervised trained Softmax classifier was utilized for classification. In terms of performance, this method achieved ACEs of 0.1866% on the LivDet 2013 and 0.3233% on the LivDet 2015 dataset.

Li et al.\cite{144} used features extracted with three algorithms, i.e., SIFT, LBP and HOG. As a result, the benefits of these algorithms were combined and the overall performance was increased. A fusion rule was developed to fuse the features and the produced feature vector was then classified by an SVM. This method showed ACEs of 4.6% on the LivDet 2011 dataset, 3.48% on the LivDet 2013 dataset and 4.03% on the LivDet 2015 dataset.

Sharma and Selwal\cite{145} proposed a method that utilized majority ensemble voting based on three local and adaptive textural image features. The features were acquired with a new LBP variant descriptor called the local adaptive binary pattern (LABP), combined with features gathered with the use of a CLBP and BSIF descriptors. This method achieved ACERs of 4.11%, 3.19%, 2.88% and 2.97% on the LivDet 2009, 2011, 2013 and 2015 datasets, respectively.

**Generalization efficient/wrapper methods**

In this category, PAD methods are presented that focus on the efficiency against PAIs made with materials not used during training. Moreover, the performance of methods that were evaluated on novel PAI materials are reported. Some of the presented PAD methods can be used as add-ons or wrappers to any PAD method, in order to improve the performance against PAIs of unknown materials. A summary of the presented methods is given in Table 8.

Rattani and Ross\cite{146} proposed the creation of a novel material detector that detects PAIs made of novel materials. These samples were then used to automatically retrain and update the PAD method. To keep the computational complexity low, the automatic adaptation procedure was executed when the presentation attack detector was offline. This scheme was evaluated on the LivDet 2011 dataset and it exhibited an average correct detection rate of up to 74% and an up to 46% improvement in presentation attack performance when the adaptive approach was utilized.

Jia et al.\cite{147}, in order to address the issue of lack of knowledge of the materials used for artificial fingerprints, suggested a one-class SVM with negative examples (OCSNE). The OCSNE showed an ACE of 23.6% on a modified dataset according to the needs of the evaluation the LivDet 2011, which was better than an SVM.

Rattani et al.\cite{148} proposed to handle PAD as an open set recognition problem. The authors claimed that their approach is useful, because during deployment novel materials different than the ones that the system was trained on may be used to construct artificial fingerprints. In their work a Weibull-calibrated SVM (W-SVM) was used as a novel material detector and as a PAD. They also developed a scheme to automatically
Table 8. Generalization efficient/wrapper methods

| Ref.                  | Year | Dataset      | Method                                                                 | Results                                                                 |
|-----------------------|------|--------------|------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Rattani and Ross [146] | 2014 | LivDet 2011 | Automatic adaptation to novel materials by the use of a novel material detector | Average correct detection rate up to 74% and an up to 46% improvement in performance |
| Jia et al. [147]      | 2014 | Modified version of the LivDet 2011 | One-class SVM with negative examples | ACE of 23.6% |
| Rattani et al. [148]  | 2015 | LivDet 2011 | Weibull-calibrated SVM | 44% improvement in performance than other methods |
| Sequeira and Cardoso [149] | 2015 | LivDet 2013 | Semi-supervised classification based on a mixture of Gaussians models | ACE of 8.35% |
| Nogueira et al. [112] | 2016 | LivDet 2009, 2011, 2013 | CNN-VGG | ACE of 16.1% on the LivDet 2011 ACE of 5.45% on the LivDet 2013 |
| Ding and Ross [160]   | 2017 | LivDet 2011 | Ensemble of one class SVMs based on descriptors that utilize different features | Average correct detection rate of 86.1% on known materials Average correct detection rate of 84.7% on unknown materials |
| Pala and Bhanu [107]  | 2017 | LivDet 2011, 2013 | Triplet of CNNs | ACE of 10.05% on the LivDet 2011 ACE of 3.35% on the LivDet 2013 |
| Gajawada et al. [151] | 2019 | LivDet 2015 | Universal Material Translator - generative adversarial network | BPCER1000 of 21.96% on unknown PAIs |
| Chugh and Jain [152]  | 2019 | MSU-FPAD | A deep convolutional neural network that utilized local patches centered and aligned using fingerprint minutiae | Average generalization performance of TDR = 75.24% when the leave-one-out method was used TDR of 97.20% with an FDR of 0.2% when all PAIs were used in training. |
| Engelsma and Jain [153] | 2019 | Own dataset | 3 Generative adversarial networks | BPCER500 of 50.20% |
| Zhang et al. [122]    | 2019 | LivDet 2015 | Residual convolutional neural network (Slim-Res CNN) | Accuracy of 96.82% on the LivDet 2015 |
| Park et al. [121]     | 2019 | LivDet 2015 | CNN | ACE of 1.9% |
| Grosz et al. [154]    | 2020 | LivDet 2011 & 2015 - MSU-FPAD | Adversarial representation learning | 92.94% TDR 0.2% FDR |
| Zhang et al. [126]    | 2020 | LivDet 2015 | CNN | ACE of 3.31% |
| González-Soler et al. [155] | 2021 | LivDet 2019 | Pyramid histogram of visual words (PHOW) | BPCER100 in range of 1.98%-17% |
| Chugh and Jain [156]  | 2021 | LivDet 2017 dataset | Universal Material Generator | TDR improvement from 75.24% to 91.78% when FDR was 0.2%. Average cross-sensor spoof detection performance improvement from 67.60% to 80.63% |

TDR: True detection rate; FDR: false detection rate; ACE: average classification error; SVM: support vector machine; CNNs: convolutional neural networks; PAIs: presentation attack instruments.

retrain and update the W-SVM depending on the artificial fingerprints it detects. This approach was tested on the LivDet 2011 dataset and it exhibits an up to 44% improvement in performance.

Sequeira and Cardoso [149] evaluated several classification methods and concluded that semi-supervised classification based on a mixture of Gaussians models yields better results. Moreover, they proposed the isolation of the fingerprint from the background by adding an automatic segmentation stage to the detection algorithms. The best method they evaluated exhibited an ACE of 8.35% on the LivDet 2013 datasets.

Nogueira et al. [112] tested their PAD method against attack with PAIs not seen in training and their method based on a CNN-VGG achieved average ACEs of 16.1% on the LivDet 2011 dataset and 5.45% on the LivDet 2013 dataset.
Ding and Ross\cite{150}, in their work based on performance metrics on the LivDet 2011 dataset, proved that using an ensemble of one-class SVMs based on descriptors that utilize different features achieves better accuracy than binary SVMs and also competed in performance with other state-of-the-art PAD algorithms immune to fabrication materials. Another advantage of this method is the limited number of artificial fingerprints used for training. The proposed method achieved an average correct detection rate on known PAI of 86.1%, while it presents an average correct detection rate on unknown materials of 84.7%, which is higher than the automatic adaption method presented in\cite{148}.

Pala and Bhanu\cite{117} also evaluated their PAD scheme against unknown attacks and their method achieved average ACEs of 10.05% on the LivDet 2011 and 3.35% on the LivDet 2013.

Gajawada et al.\cite{151}, to improve the efficiency of any PAD, especially against new materials, developed the Universal Material Translator (UMT) as a deep learning augmentation wrapper. They proposed the synthetization of artificial samples by utilizing only a small part of them. Along with the UMT, they also used a GAN. Although the authors believe that the combination of a UMT and a GAN produces better results, GANs insert certain artefacts and noise in the generated images that are detectable and negatively affect the performance of the classifiers. Their method was tested on the LivDet 2015 dataset and demonstrated a BPCER1000 of 21.96% on unknown PAIs.

Chugh and Jain\cite{152} experimented on the efficiency of the so-called spoof buster, a PAD wrapper developed in\cite{18}, which could be used on top of any PAD method to improve generalization and efficiency, especially against PAIs not seen in training. The spoof buster used a deep convolutional neural network that utilized local patches centered and aligned using fingerprint minutiae. The MSU-FPAD dataset was utilized and their method achieved a (weighted average generalization performance) TDR of 75.24% when the leave-one-out method was used, as opposed to a TDR of 97.20% with an FDR of 0.2% when all PAIs were used in the training.

Engelsma and Jain\cite{153} proposed the utilization of three GANs on a training set that contained only bona fide samples. Their method showed improvement in cross-material performance, compared to one class or binary state-of-the-art classifiers, on their own dataset that contains 5531 artificial samples (from 12 materials) and 11,880 bona fide samples. For this dataset, it achieved a BPCER500 of 50.20%.

A Slim-Res CNN\cite{122} also demonstrated, to some extent, robustness against attack with new materials and presented an accuracy of 96.82% on the LivDet 2015 dataset, whose testing sets consisted of artificial fingerprints made of unknown materials.

Park et al.\cite{121} also evaluated their proposed method on the LivDet 2015 and concluded that their method presents efficiency against attacks made from unknown materials. The patched based CNN exhibited an ACE of 1.9%.

Grosz et al.\cite{154} suggested the use of adversarial representation learning in DNNs. Their proposal can be added to any CNN that uses 96 × 96 aligned minutiae-centered patches for training, along with the utilization of a style transfer network wrapper. Their method achieved a 92.94% TDR and a 0.2% FDR on the LivDet 2011 and 2015 datasets and on the MSU-FPAD dataset.
Zhang et al.\textsuperscript{126} also tested their proposed method against attacks from new materials and achieved an ACE of 3.31\% on the LivDet 2015.

Gonzalez-Soler et al.\textsuperscript{155} suggested three techniques for PAD. Initially, the pyramid histogram of visual words was utilized for extracting the local features of the fingerprint with the use of dense SIFT descriptors. Afterwards, the feature vector was formed with the utilization of three methods: (1) bag-of-words; (2) Fisher vector (FV); and (3) vector locally aggregated descriptors. A linear SVM was used for classification. The FV encoding achieved the best detection accuracy on the LivDet 2019 competition. Fusion of the three encodings achieved even better performance and yielded a BPCER100 in the range of 1.98\%-17\% in the presence of unknown PAI species.

Chugh and Jain\textsuperscript{156} proposed the utilization of the Universal Material Generator (UMG) for the performance improvement of any PAD method against unknown materials [Figure 11]. The UMG is a CNN, trained on characteristics of known materials that artificial fingerprints are made off, in an effort to synthesize artificial samples of unknown materials. The UMG improves the performance by increasing the TDR from 75.24\% to 91.78\% when the FDR was 0.2\% and the average cross-sensor presentation attack detection performance from 67.60\% to 80.63\% on the LivDet 2017 dataset.

**DISCUSSION**

Biometric authentication systems have been widely used in recent years and therefore PAD has become crucial. This literature review revealed the immense research in the field of fingerprint PAD. Hardware-based approaches rely on the detection of signals that confirm that the subject of the recognition process is a genuine one. Although hardware-based approaches present higher performance and reliability, they are intrusive and require extra capturing hardware, added to the sensor of the fingerprint recognition scheme, which comes at great expense and in some cases adds a time delay on the verification process\textsuperscript{48}. These are mostly the reasons that a relatively small number of hardware-based solutions, in contrast to software-based methods, can be found in the literature. Furthermore, software PAD methods have the potential to protect against security vulnerabilities that are not categorized as PAs, e.g., attacks utilizing modified samples at the communication channel of the feature extraction module and the sensor\textsuperscript{14}.

Software-based PAD methods can be added to any fingerprint recognition system, without any extra cost and without modifying the sensor. The criteria of the taxonomy of software-based approaches presented in this study were the type of technique or the kind of features used for the information extraction from the fingerprint prior to classification. Every category of this taxonomy presents advantages, disadvantages and research opportunities.

PAD methods that utilize dynamic features exhibited a promising level of accuracy. The main drawback is the time consumption that is high due to the time interval between the capture of samples and the extraction of the dynamic features. This fact makes them unsuitable for real-time authentication, as noted by Nikam and Agarwal\textsuperscript{157}. Furthermore, another drawback is user inconvenience since some methods of these categories depend on certain moves of the finger of the user. These are the main reasons why dynamic PAD solutions are very rarely met in recent literature.

The features used in PAD methods that exploit physiological features are the several unique characteristics of the sweat pores and the perspiration phenomenon, which have substantial strength and discriminative power. These methods in some cases exhibit computational simplicity but also present high intra-class variability and usually require more than one image of the fingerprint, thus making the process slower with
increased computation time. According to Nikam and Agarwal\cite{157}, perspiration-based methods are not efficient for real-time authentication. Researchers worked mainly in the direction of rectifying these disadvantages but research interest was focused on approaches based mainly on CNNs and texture descriptors due to the advantages they exhibit. Recent works on PAD methods that rely solely on anatomical or physiological features are rare, but as proved by the work of Agarwal and Bansal\cite{143}, they are considered good supplement methods to approaches that fuse features.

PAD methods based on image quality features rely on the diversity between bona fide and artificial samples due to the coarseness of the surface of the fingerprint. This diversity exists on account of the agglomeration that happens during processing of the materials used for artificial samples because of the large organic molecules of these materials\cite{71}. The properties used for image quality-based PAD methods present different strengths, discriminative power and weaknesses. The main advantages of these methods rely mostly on their simplicity and the low computational complexity, thereby achieving fast response times\cite{14}. The major disadvantages are that the classifier’s efficiency depends on the kind of PA\cite{158} and the performance depends on environmental, scanner and user related (usability) conditions\cite{70,74}. Although image quality PAD methods have been used commercially, researchers’ attention has been focused mainly to local texture descriptors and CNNs that present superior performance. Nevertheless, their computational simplicity makes them ideal for approaches that utilize the fusion of features.

Local texture descriptors are straightforward, rapid and can be implemented in real-time fingerprint recognition schemes. Photometric, rotational and geometric effects have no effect on local descriptors. This fact is one of the reasons why these descriptors achieved superior performance in PAD approaches\cite{28}. Due to their accurate target localization, they generally perform better in cross-dataset and cross-material experiments than their neural network counterparts, which perform best for cross-sensor experiments\cite{159}. There are three major drawbacks for these methods: (1) the performance of the descriptors rely on the type
of the sensor used for the acquisition of the sample\textsuperscript{[160]}; (2) a large dataset is required for training\textsuperscript{[158]}; and (3) local texture descriptors generalize poorly against PAs accomplished with the use of materials not encountered in training\textsuperscript{[148]}.\n
Ghiani \textit{et al.}\textsuperscript{[78]} conducted experiments with features based on pore detection, ridge wavelets and several textural features. They concluded that the best method was LBP, although it has the disadvantages of being sensitive to image rotation and the need for longer computational time due to its long histogram.\n
According to González-Soler \textit{et al.}\textsuperscript{[161]}, DSIFT-based encoding achieves the best performance against unknown materials. González-Soler \textit{et al.}\textsuperscript{[79]} also reported that gradient-based features, such as black saturation, white saturation, lack of continuity, unwanted noises and ridge distortions, achieve the best performance amongst other descriptors and especially the fusion of gradient and textural features present even better performance.\n
Local feature descriptors are a very active field of PAD. There are many opportunities for research, especially concerning the creation of new feature descriptors. According to Sharma and Dey\textsuperscript{[162]}, methods for the accurate extraction of the contrast and orientation of the fingerprint image, which is mandatory for the design of a new descriptor, can be found in the literature.\n
CNNs provide an excellent solution to image recognition and have been used in many fields beyond computer vision, such as information security. CNN-based PAD methods provide promising accuracy but there are two drawbacks that limit their usage in commercial fingerprint recognition systems. The first is that these methods are sensor and material dependent. This fact makes them susceptible to PAs with unknown materials or with different capture devices. The cause of this limitation could be that the learning methods of these approaches utilize several filters that rely on known attacks and combine convolutional, pooling and fully connected layers, which do not present good generalization\textsuperscript{[79]}. The second drawback is that these method’s requirements regarding memory and computational time are high\textsuperscript{[162]}, making them unsuitable for usage in low resource environments, such as smartphones. This is the reason that there is a noticeable turn by researchers that use deep learning methods to solutions that require the least processing time.\n
The use of local patches instead of the whole fingerprint image is also widespread. Local patches are small regions of interest of the fingerprint image. Another major limitation of these methods relies on the number of training patterns. CNNs are complex algorithms that need tens of thousands, millions in some cases, of training patterns to perform and generalize well. Therefore, new datasets or mixture of datasets should be utilized. A different approach should be the augmentation of the datasets to provide more bona fide and artificial samples. Nogueira \textit{et al.}\textsuperscript{[136]} suggested the augmentation of the dataset by the artificial creation of images that present uneven illumination and random noise. They also proposed that different classifiers should be trained for different transformation types. Another possible solution should be the adoption of other deep learning approaches like one-shot learning\textsuperscript{[163]}.\n
Raja \textit{et al.}\textsuperscript{[164]} concluded that handcrafted textural features achieve the best performance on capacitive sensors, whereas naturally learned features achieve optimal performance on thermal and optical sensors. They also suggested the use of deep learning-based approaches with the utilization of large data sets for the creation of new reliable PAD methods. Pinto \textit{et al.}\textsuperscript{[119]} suggested that reliable PAD models should rely on both “hand-crafted” and “data-driven” solutions.
In general, feature fusion approaches exhibit superior accuracy than their single feature counterparts. Furthermore, their performance is competitive with state-of-the-art PAD methods. In Ref.\cite{18}, answers to the major challenges that feature fusion methods face are provided. They concluded that fusion is more effective at a feature level than at a decision level. Furthermore, proper transformation of the different views into a common latent space is the best method for harmonization or normalization of the features used for fusion. Moreover, reducing dimensionality of the classification space is best suited with the use of subspace transformation. Finally, the usage of deep learning methods is suitable for the automated learning of the way diverse features aggregate.

A common limitation to all the aforementioned PAD categories is their generalization ability against unknown materials. This is the main reason that new approaches (discussed in Generalization efficient/wrapper methods) have been proposed by researchers. These approaches are focused on increased performance against PAs not seen in training and in the case of wrappers-addons can be used on top of any PAD method and have a positive impact on performance. The drawback of the latter type of approach is the increase in computational time and memory usage. Nogueira et al.\cite{112} suggested that the PAD generalization error and the performance drop in presence of PAs not used in training, are mostly due to new sensors and not new materials. The low level of interoperability among different sensors, due to the influence in the image properties and more specifically in the corresponding feature space, on account of the unique characteristics of each different sensor was also reported by Tuveri et al.\cite{165}.

Marasco and Sansone\cite{166} concluded that PAD methods that rely on multiple PAD features are more robust against PAs realized with the use of materials not used in training. Finally, Marasco et al.\cite{115} noted that CNNs exhibit the ability to successfully adapt to PAD problems with the use of pre-training on ImageNet.

User authentication systems that rely on a single biometric trait, suffer from vulnerabilities, due to poor data quality and scalability. Multimodal biometrics utilize data acquired from different sources, resulting in better performance and reliability\cite{167}. This is the direct outcome of the fusion of data from different sources that makes possible the extraction of more distinctive features than the features extracted with the use of unimodal systems\cite{168}. Furthermore, these systems acquire data from different sensors, making them more robust against illumination conditions and other factors related to the sensors that have a negative impact on performance\cite{169}. A key factor in multimodal systems is the level in which the fusion of the information is accomplished. Fusion at the extraction level does not present advantages since there is a significant amount of data to be fused. Fusion at the matcher score level has attracted significant attention by researchers because of its simplicity. Finally, the best authentication performance is expected when fusion is performed at the decision level. The disadvantage of this approach is the fact that the extracted feature vectors may be incompatible\cite{170}. In the literature, there are proposed methods that fingerprint is used in conjunction with other biometric traits like face and iris recognition\cite{171,172}, face and speech\cite{173} and face\cite{174}.

Moreover, ECG signals were used along with the fingerprints with promising results, as discussed in HARDWARE-BASED PRESENTATION ATTACK DETECTION\cite{45,46,175-177}. Other cognitive factors, like EEGs, may also be utilized in conjunction with fingerprints. However, the aforementioned biometric traits require explicit, and sometimes expensive, capture equipment.

Another authentication scheme that presents a high level of security is the n-factor authentication scheme, where n denotes the number of combined factors. The factors may be knowledge, possession or inherence based. In the knowledge category, factors like personal ids, usernames or identification numbers are included. Possession-based factors include one-time password tokens, ID cards and smart cards. Inherence
factors include any biological trait. These systems utilize cryptography to improve security.

He and Wang proposed that the user should use their smart card, input their password and id, and then utilize their personal biometric impression. This system employed curve cryptography to further improve security. Qiu et al. proposed a similar authentication scheme that utilized the “fuzzy-verifiers” and “honeywords” techniques along with chaotic-maps for mobile lightweight devices. In n-factor authentication schemes, the fingerprint is one of the most used biometric traits.

By analyzing Tables 2-8, we reach the following conclusions:

- The majority of the presented state-of-the-art methods make use of the LivDet datasets. Therefore, they can be considered as benchmarks.

- There is a clear revulsion to the research, especially from 2015 and towards to textural features and deep learning methods, especially CNNs.

- The datasets that are utilized by the authors of presented publications consist of only a few thousand samples. The distribution of training and test sets for each one of the most utilized datasets is shown in Table 1.

Finally, Table 9 presents a comparative analysis of the aforementioned PAD techniques, highlighting the advantages and disadvantages of each category.

**Research challenges and potential research directions**

The presentation of the research methods proposed to the literature highlighted the current trends along with the advantages and disadvantages of each PAD category. Moreover, the research challenges and potential research directions emerged and are presented in this section.

The first challenge concerns the data that train the classifiers. The majority of the presented methods are sensor and dataset dependent, i.e., the training and test sets are from the same sensor and from the same dataset. “Good” data result to better training and eventually better classification results. A “good” dataset should be balanced and comprised of samples acquired from different sensors (the more the better). A thorough analysis of Table 1 reveals that only bona fide and artificial samples are present in the datasets. Nevertheless, as science evolves, the possibility that someone attacks a biometric system with natural samples, i.e., transplanted hands, fingerprints made of natural skin and plastic surgery results, becomes higher. Thus, the models should be trained with datasets comprising of these biological materials also. However, there is a significant lack of these data and therefore research in this field, i.e., biological presentation attack detection is limited. Hence, the sensor and dataset interoperability are major unresolved problems and have not been given much attention yet.

Regarding the methods that are mainly utilized by researchers, it is obvious that during the last five years, there has been a revulsion to deep learning methods, especially CNNs. These methods provide promising accuracy but the drawbacks that limit their usage in commercial fingerprint recognition systems must be addressed. CNNs are sensor and material dependent. The only effective way to overcome the first drawback is to create and utilize datasets comprising of samples acquired from more subjects, more sensors and containing biological materials.
Table 9. Comparative analysis of PAD categories

| Category of PAD                        | Advantages                                                                 | Disadvantages                                                                 | Research opportunities                                                                 |
|---------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Hardware based                        | Higher performance and reliability                                        | Intrusive and expensive although not immune to presentation attacks            | OCT, hybrid methods (software and hardware combined)                                     |
| Dynamic features                      | Satisfactory accuracy                                                     | Time consuming. Depending on the method, may be inconvenient for the user     | Fusion of features extracted with the use of textural descriptors or neural networks     |
| Anatomical or physiological features  | Computational simplicity depending on the approach                        | High intra-class variability, increased computation time depending on the approach | Fusion with other features                                                               |
| Image quality features                | Simplicity, low computational complexity, and fast response times          | Performance depends on environmental, scanner and user related conditions      | Fusion with other features                                                               |
| Texture features                      | Straightforward, quick, can be implemented in commercial fingerprint recognition schemes | Descriptor’s performance relies on the type of the sensor. A large dataset is required for training | Novel descriptors or variations of known descriptors (SIFT, LBP, LPQ etc.)                |
| Neural networks                       | Better performance - on cross sensor datasets compared to texture descriptors Better performance on datasets with many captured subjects | Sensor and material dependent High requirements in memory and computational time Low performance to low quality (small number of images and subjects) datasets Utilization of large data sets (deep learning) | Approaches that require low memory and less computational time. Augmentation of the datasets used for training One shot learning. Fusion with other features |
| Fusion of features                    | Superior accuracy compared the single feature counterparts competitive to state-of-the-art | Increased memory and computation time requirements than the single feature counterparts Utilization of large data sets (deep learning) | New approaches with fusion of features that fuse at feature level, have reduced dimensionality, and utilize harmonization or normalization of the features |
| Generalization efficient - Wrappers  | Increased performance against unknown PAIs                                | Increased memory and computation time requirements when used as addons or wrappers | Approaches that utilize multiple features                                                |

PAD: Presentation attack detection; OCT: optical coherence tomography; SIFT: scale invariant feature transform; LBP: local binary pattern; LPQ: local phase quantization; PAIs: presentation attack instruments.

Moreover, the required memory and the computational complexity are high\[^{162}\] and this makes them unsuitable for usage in low resource environments, such as mobiles or other wearable devices. On this basis, the generalization of the method should be improved. Nevertheless, the more data we use, the more time we have to train the deep networks. Thus, new approaches like transfer learning and one shot or zero shot learning are getting more notice due to the less computational resources they require.

Another interesting research direction is auxiliary supervision. As mentioned in DATASETS, fingerprint PAD is considered as a binary classification problem. Nevertheless, the proposed methods in the literature show poor generalization, i.e., poor performance on unseen data. To tackle this, auxiliary learning\[^{190}\] should be helpful. Recent research showed that auxiliary supervision with end-to-end learning provides better anti-spoofing\[^{191}\].
Another thing that also must be noted is that biometric sensors are no longer found only in access controls. Nowadays, the majority of mobiles and other wearable devices make use of these sensors. The acquired data from these sensors (GPS, accelerometer, gyroscope, magnetometer, microphone, NFC and heart rate monitors) can be utilized to distinguish a person. However, since these data are heterogeneous, methods that analyze and extract a concrete representation of them should be developed.

Multimodal biometrics is another research field that requires more attention, especially when one or more of the modalities concern the so-called cognitive biometrics. Cognitive biometrics concerns the bio-signals, like an EEG, ECG or the electrodermal response, which are generated by the brain, heart and the nervous system, respectively. These modalities when combined with the behavioral ones, i.e., fingerprint, iris and so on, may provide enhanced security.

Finally, a major concern and simultaneously a research challenge that needs to be addressed is the privacy of the individual. The acquired samples, regardless of their type (behavioral/cognitive) or the way that have been obtained, may be used to either to contravene the privacy of the subject or to profiling them. It is therefore crucial to the creation of relevant legislation describing how such data should be handled without violating the privacy of the individual. Furthermore, it is also vital that researchers ensure that the methods they propose consider privacy issues.

CONCLUSIONS
A comprehensive review regarding presentation attack detection methods has been presented. Moreover, both approaches of presentation attack detection techniques, i.e., hardware and software based, were thoroughly analyzed and a taxonomy concerning PAD methods was revisited. This literature review highlighted all recent advances in this field and pointed out areas for future research to help researchers design secure biometric systems.

DECLARATIONS
Authors’ contributions
The manuscript, study design, and the detailed survey of the literature: Karampidis K, Rousouliotis M, Linardos E, Kavallieratou E

Availability of data and materials
Not applicable.

Financial support and sponsorship
This research is co-financed by Greece and the European Union (European Social Fund - ESF) through the Operational Programme "Human Resources Development, Education and Lifelong Learning 2014-2020" in the context of the project "Creation of a Multimodal Biometric Password by using Steganography" (MIS 5050338).

Conflicts of interest
All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate
Not applicable.
REFERENCES

1. Pankanti S, Prabhakar S, Jain A. On the individuality of fingerprints. *IEEE Trans Pattern Anal Machine Intell* 2002;24:1010-25. DOI

2. Prasad PS, Sunitha Devi B, Janga Reddy M, Gunjan VK. A Survey of Fingerprint Recognition Systems and Their Applications. In: Kumar A, Mozar S, editors. ICCCE 2018. Singapore: Springer; 2019. p. 513-20. DOI

3. Yadav JKP, Jaffery ZA, Singh L. A short review on machine learning techniques used for fingerprint recognition. *Journal of Critical Reviews* 2020;7:2768-73. DOI

4. ISO - ISO/IEC 30107-1:2016 - Information technology - Biometric presentation attack detection - Part 1: framework. Available from: https://www.iso.org/standard/53227.html. [Last accessed on 12 Oct 2021].

5. Hosseini S. Fingerprint vulnerability: a survey. 2018 4th International Conference on Web Research (ICWR); 2018 Apr 25-26; Tehran, Iran. IEEE; 2018. p. 70-7. DOI

6. Coli P, Marcialis GL, Roli F. Vitality detection from fingerprint images: a critical survey. In: Lee S, Li SZ, editors. Advances in biometrics. Berlin: Springer Berlin Heidelberg; 2007. p. 722-31. DOI

7. Kundargi J, Karandikar RG. Integrating liveness detection technique into fingerprint recognition system: a review of various methodologies based on texture features. In: Sa PK, Sahoo MN, Murugappan M, Wu Y, Majhi B, editors. Progress in intelligent computing techniques: theory, practice, and applications. Singapore: Springer; 2018. p. 295-305. DOI

8. Maras E, Ross A. A survey on antispooﬁng schemes for ﬁngerprint recognition systems. *ACM Comput Surv* 2015;47:1-36. DOI

9. Sousedik C, Busch C. Presentation attack detection methods for ﬁngerprint recognition systems: a survey. *IET biom* 2014;3:219-33. DOI

10. Ghiani L, Yambay DA, Mura V, Marcialis GL, Roli F, Schuckers SA. Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. *Image Vis Comput* 2017;58:110-28. DOI

11. Orrù G, Casula R, Tuveri P et al. LivDet in action - ﬁngerprint liveness detection competition 2019. 2019 International Conference on Biometrics (ICB). 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-6. DOI

12. Yambay D, Ghiani L, Marcialis GL, Roli F, Schuckers S. Review of ﬁngerprint presentation attack detection competitions. In: Marcel S, Nixon MS, Fierrez J, Evans N, editors. Handbook of biometric anti-spoofing. Cham: Springer International Publishing; 2019. p. 109-31. DOI

13. LivDet - liveness detection competitions. Available from: http://livdet.org/competitions.php. [Last accessed on 12 Oct 2021].

14. Galbally J, Fierrez J, Cappelli R. An introduction to ﬁngerprint presentation attack detection. In: Marcel S, Nixon MS, Fierrez J, Evans N, editors. Handbook of biometric anti-spoofing. Cham: Springer International Publishing; 2019. p. 3-31. DOI

15. Marcel S, Nixon MS, Fierrez J, Evans N. Handbook of biometric anti-spoofing. 2nd ed. Cham: Springer International Publishing; 2019. DOI

16. ISO/IEC 30107-3:2017, Information technology - Biometric presentation attack detection - Part 3: Testing and reporting. Available from: https://www.iso.org/standard/67381.html. [Last accessed on 12 Oct 2021].

17. Galbally J, Fierrez J, Alonso-féndez F, Martinez-diaz M. Evaluation of direct attacks to fingerprint veriﬁcation systems. *Telecommun Syst* 2011;47:243-54. DOI

18. Chugh T, Cao K, Jain AK. Fingerprint Spoof Buster: use of minutiae-centered patches. *IEEE Trans Inform Forensic Secur* 2018;13:2190-202. DOI

19. Marcialis GL, Lewicke A, Tan B, et al. First International Fingerprint Liveness Detection Competition-LivDet 2009. In: Foggia P, Sansone C, Vento M, editors. Image Analysis and Processing -ICIAP 2009. Berlin: Springer Berlin Heidelberg; 2009. p. 12-23. DOI

20. Abhyankar AS, Schuckers SC. A wavelet-based approach to detecting liveness in fingerprint scanners. Biometric Technology for Human Identiﬁcation 2004; 2004 Aug 25; Orlando, USA. IEEE; 2004. p. 278-86. DOI

21. Tan B, Schuckers S. Spoofing protection for ﬁngerprint scanner by fusing ridge signal and valley noise. *Pattern Recognition* 2010;43:2845-57. DOI

22. Nikam SB, Agarwal S. Curvelet-based ﬁngerprint anti-spoofing. *SIViP* 2010;4:75-87. DOI

23. Putte T, Keuning J. Biometrical ﬁngerprint recognition: don’t get your ﬁngers burned. In: Domingo-ferrer J, Chan D, Watson A, editors. Smart card research and advanced applications. Boston: Springer US; 2000. p. 289-303. DOI

24. Osten DW, Carim HM, Arnesson MR, Blan BL. Biometric, personal authentication system. Available from: https://patents.google.com/patent/US5779950A/en. [Last accessed on 12 Oct 2021].

25. Drahanský M, Nötzel R, Wolfgang F. Liveness detection based on ﬁne movements of the ﬁnger tip surface. 2006 IEEE Information Assurance Workshop; 2006 Jun 21-23; West Point, NY, USA. IEEE; 2006. p. 42-7. DOI

26. Baldisserra D, Franco A, Maio D, Maltoni D. Fake ﬁngerprint detection by odor analysis. In: Zhang D, Jain AK, editors. Advances in biometrics. Berlin: Springer Berlin Heidelberg; 2005. p. 265-72. DOI

27. Noncommunicable diseases: hypertension. Available from: https://www.who.int/news-room/q-a-detail/noncommunicable-diseases-
hypertension. [Last accessed on 12 Oct 2021].

28. Hogan JN. Multiple reference OCT system. Available from: https://patents.google.com/patent/US9113782B2/en. [Last accessed on 12 Oct 2021].

29. Cheng Y, Larin KV. Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis. Appl Opt 2006;45:9238-45. DOI PubMed

30. Cheng Y, Larin KV. In vivo two- and three-dimensional imaging of artificial and real fingerprints with optical coherence tomography. IEEE Photon Technol Lett 2007;19:1634-6. DOI

31. Bossen A, Lehmann R, Meier C. Internal fingerprint identification with optical coherence tomography. IEEE Photon Technol Lett 2010;22:507-9. DOI

32. Liu M, Buma T. Biometric mapping of fingertip eccrine glands with optical coherence tomography. IEEE Photon Technol Lett 2010. DOI

33. Nasiri-avanki M, Meadway A, Bradau A, Khoshki RM, Hojjatoleslami A, Podoleanu AG. Anti-spoof reliable biometry of fingerprints using en-face/optical coherence tomography. OPJ 2011;01:91-6. DOI

34. Liu G, Chen Z. Capturing the vital vascular fingerprint with optical coherence tomography. Appl Opt 2013;52:5473-7. DOI PubMed PMC

35. Hussein ME, Spinoulas L, Xiong F, Abd-Almageed W. Fingerprint presentation attack detection using a novel multi-spectral capture device and patch-based convolutional neural networks. 2018 IEEE International Workshop on Information Forensics and Security (WIFS); 2018 Dec 11-13; Hong Kong, China. IEEE; 2018. p. 1-8. DOI

36. Tolosana R, Gomez-Barrero M, Kolberg J, Morales A, Busch C, Ortega-Garcia J. Towards fingerprint presentation attack detection based on convolutional neural networks and short wave infrared imaging. 2018 International Conference of the Biometrics Special Interest Group (BIOSIG); 2018 Sep 26-28; Darmstadt, Germany. IEEE; 2018. p. 1-5. DOI

37. Gomez-Barrero M, Kolberg J, Busch C. Multi-modal fingerprint presentation attack detection: analysing the surface and the inside. 2019 International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-8. DOI

38. Tolosana R, Gomez-Barrero M, Busch C, Ortega-garcia J. Biometric presentation attack detection: beyond the visible spectrum. IEEE Trans Inform Forensic Secur 2020;15:1261-75. DOI

39. Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014.

40. Howard AG, Zhu M, Chen B, et al. MobileNets: efficient convolutional neural networks for mobile vision applications. arXiv preprint arXiv:1704.04861, 2017.

41. Goicoechea-telleria I, Kiyokawa K, Liu-jimenez J, Sanchez-reillo R. Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes. IEEE Access 2019;7:7184-93. DOI

42. Engelsma JJ, Cao K, Jain AK. RaspiReader: open source fingerprint reader. IEEE Trans Pattern Anal Mach Intell 2019;41:2511-24. DOI PubMed

43. Palka N, Kowalski M. Towards fingerprint spoofing detection in the terahertz range. Sensors (Basel) 2020;20:3379. DOI PubMed PMC

44. Spinoulas L, Mirzaalian H, Hussein ME, Abdalmageed W. Multi-modal fingerprint presentation attack detection: evaluation on a new dataset. IEEE Trans Biom Behav Identity Sci 2021;3:347-64. DOI

45. Lapsley PD, Lee JA, Pare Jr DF, Hoffman N. Anti-fraud biometric scanner that accurately detects blood flow. Available from: https://patents.google.com/patent/US5737439A/en. [Last accessed on 12 Oct 2021].

46. Ribeiro Pinto J, Cardoso JS, Lourenco A. Evolution, current challenges, and future possibilities in ECG biometrics. IEEE Access 2018;6:34746-76. DOI

47. Paranjape RB, Mahovsky J, Benedicenti L, Koles Z. The electroencephalogram as a biometric. Canadian Conference on Electrical and Computer Engineering 2001. Conference Proceedings (Cat. No.01TH8555); 2001 May 13-16; Toronto, ON, Canada. IEEE; 2001. p. 1363-6. DOI

48. Mooolla Y, Darlow L, Sharma A, Singh A, van der Merwe J. Optical coherence tomography for fingerprint presentation attack detection. In: Marcel S, Nixon MS, Fierrez J, Evans N, editors. Handbook of biometric anti-spoofing. Cham: Springer International Publishing; 2019. p. 49-70. DOI

49. Antonelli A, Cappelli R, Maio D, Maltoni D. Fake finger detection by skin distortion analysis. IEEE Trans Inform Forensic Secur 2006;1:360-73. DOI

50. Jia J, Cai L, Zhang K, Chen D. A new approach to fake fingerprint detection based on skin elasticity analysis. In: Lee S, Li SZ, editors. Advances in biometrics. Berlin: Springer Berlin Heidelberg; 2007. p. 309-18. DOI

51. Zhang Y, Tian J, Chen X, Yang X, Shi P. Fake finger detection based on thin-plate spline distortion model. In: Lee S, Li SZ, editors. Advances in biometrics. Berlin: Springer Berlin Heidelberg; 2007. p. 742-9. DOI

52. Decann B, Tan B, Schuckers S. A novel region based liveness detection approach for fingerprint scanners. In: Tistarelli M, Nixon MS, editors. Advances in biometrics. Berlin: Springer Berlin Heidelberg; 2009. p. 627-36. DOI

53. Nikam SB, Agarwal S. Wavelet-based multisresolution analysis of ridges for fingerprint liveness detection. IJICS 2009;3:1. DOI

54. Abbvynkar A, Schuckers S. Integrating a wavelet based perspiration liveness check with fingerprint recognition. Pattern Recognition 2009;42:452-64. DOI

55. Abbvynkar A, Schuckers S. Modular decomposition of fingerprint time series captures for the liveness check. IJCEE 2010;2:1793-8163. DOI

56. Marcialis GL, Roli F, Tido A. Analysis of fingerprint pores for vitality detection. 2010 20th International Conference on Pattern
Pereira LFA, Pinheiro HNB, Silva JIS, et al. A fingerprint spoof detection based on MLP and SVM. The 2012 International Joint Conference on Biometrics: Theory, Applications and Systems (BTAS); 2013 Sep 29-Oct 2; Arlington, VA, USA. IEEE; 2013. p. 1-6.

Pereira L, Pinheiro H, Cavalcanti G, Ren TI. Spatial surface coarseness analysis: technique for fingerprint spoof detection. Sensors (Basel) 2021;21:2059. DOI PubMed PMC

Espinoza M, Champod C. Using the number of pores on fingerprint images to detect spoofing attacks. 2011 International Conference on Hand-Based Biometrics; 2011 Nov 17-18; Hong Kong, China. IEEE; 2011. p. 1-5. DOI

Marasco E, Sansone C. Combining perspiration- and morphology-based static features for fingerprint liveness detection. Pattern Recognition Letters 2012;33:1148-56. DOI

Pereira LFA, Pinheiro HNB, Silva JIS, et al. A fingerprint spoof detection based on MLP and SVM. The 2012 International Joint Conference on Neural Networks (IJCNN); 2012 Jun 10-15; Brisbane, QLD, Australia. IEEE; 2012. p. 1-7. DOI

Marasco E, Sansone C. An anti-spoofing technique using multiple textural features in fingerprint scanners. 2010 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications; 2010 Sep 9; Taranto, Italy. IEEE; 2010. p. 8-14. DOI

Galbally-Herrero J, Fierrez-Aguilar J, Rodriguez-Gonzalez JD, Alonso-Fernandez F, Ortega-Garcia J, Tapiador M. On the vulnerability of fingerprint verification systems to fake fingerprints attacks. Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology; 2006 Oct 16-19; Lexington, KY, USA. IEEE; 2006. p. 130-6. DOI

Gütlein M, Frank E, Hall M, Kariwath A. Large-scale attribute selection using wrappers. 2009 IEEE Symposium on Computational Intelligence and Data Mining; 2009 Mar 30-2009 Apr 2; Nashville, TN, USA. IEEE; 2009. p. 332-9. DOI

Marcialis GL, Coli P, Roli F. Fingerprint liveness detection based on fake finger characteristics. International Journal of Digital Crime and Forensics 2012;4:1-19. DOI

Johnson P, Schuckers S. Fingerprint pore characteristics for liveness detection. 2014 International Conference of the Biometrics Special Interest Group (BIOSIG); 2014 Sep 10-12; Darmstadt, Germany. IEEE; 2014. p. 1-8. DOI

Lu M, Chen Z, Sheng W. Fingerprint liveness detection based on pore analysis. In: Yang J, Yang J, Sun Z, Shan S, Zheng W, Feng J, editors. Biometric recognition. Cham: Springer International Publishing; 2015. p. 233-40. DOI

Tan B. New approach for liveness detection of fingerprint scanners based on valley noise analysis. J Electron Imaging 2008;17:011009. DOI

Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J. Fingerprint liveness detection based on quality measures. 2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS); 2009 Sep 22-23; Tampa, FL, USA. IEEE; 2009. p. 1-8. DOI

Lee H, Maeng H, Bae Y. Fake finger detection using the fractional fourier transform. In: Fierrez J, Ortega-garcia J, Esposito A, Drygajlo A, Faundez-zanuy M, editors. Biometric ID management and multimodal communication. Berlin: Springer Berlin Heidelberg; 2009. p. 318-24. DOI

Jin C, Li S, Kim H, Park E. Fingerprint liveness detection based on multiple image quality features. In: Chung Y, Yung M, editors. Information security applications. Berlin: Springer Berlin Heidelberg; 2011. p. 281-91. DOI

Choi H. Fake-fingerprint detection using multiple static features. Opt Eng 2009;48:047202. DOI

Galbally J, Alonso-fernandez F, Fierrez J, Ortega-garcia J. A high performance fingerprint liveness detection method based on quality related features. Future Generation Computer Systems 2012;28:311-21. DOI

Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. IEEE Trans Image Process 2014;23:710-24. DOI

Sharma RP, Dey S. Fingerprint liveness detection using local quality features. Vis Comput 2019;35:1393-410. DOI

Ghiani L, Denti P, Marcialis GL. Experimental results on fingerprint liveness detection. In: Perales FJ, Fisher RB, Moeslund TB, editors. Articulated motion and deformable objects. Berlin: Springer Berlin Heidelberg; 2012. p. 210-8. DOI

González-soler LJ, Gomez-barrero M, Kolberg J, Chang L, Pérez-suárez A, Busch C. Local feature encoding for unknown presentation attack detection: an analysis of different local feature descriptors. IET biom 2021;10:374-91. DOI

FVC2004 - Third International Fingerprint Verification Competition. Available from: http://bias.csr.unibo.it/fvc2004/databases.asp. [Last accessed on 12 Oct 2020].

Ghiani L, Marcialis GL, Roli F. Fingerprint liveness detection by local phase quantization. Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012); 2012 Nov 11-15; Tsukuba, Japan. IEEE; 2012. p. 537-40. DOI

Gragnaniello D, Poggi G, Sansone C, Verdoliva L. Fingerprint liveness detection based on Weber Local image Descriptor. 2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications; 2013 Sep 9; Napoli, Italy. IEEE; 2013. p. 46-50. DOI

Jia X, Yang X, Zang Y; et al. Multi-scale block local ternary patterns for fingerprints vitality detection. 2013 International Conference on Biometrics (ICB); 2013 Jun 4-7; Madrid, Spain. IEEE; 2013. p. 1-6. DOI

Pereira L, Pinheiro H, Cavalcanti G, Ren TI. Spatial surface coarseness analysis: technique for fingerprint spooof detection. Electron lett 2013;49:260-1. DOI

Ghiani L, Hadd A, Marcialis GL, Roli F. Fingerprint liveness detection using binarized statistical image features. 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS); 2013 Sep 29-Oct 2; Arlington, VA, USA. IEEE; 2013. p. 1-6 DOI
86. Jia X, Yang X, Cao K, et al. Multi-scale local binary pattern with filters for spoof fingerprint detection. *Information Sciences* 2014;268:91-102. DOI
87. Gragnaniello D, Poggi G, Sansone C, Verdoliva L. Wavelet-Markov local descriptor for detecting fake fingerprints. *Electron lett* 2014;50:439-41. DOI
88. Zhang Y, Fang S, Xie Y, Xu T. Fake fingerprint detection based on wavelet analysis and local binary pattern. In: Sun Z, Shan S, Sang H, Zhou J, Wang Y, Yuan W, editors. Biometric recognition. Cham: Springer International Publishing; 2014. p. 191-8. DOI
89. Gottschlich C, Marasco E, Yang AY, Cukic B. Fingerprint liveness detection based on histograms of invariant gradients. *IEEE International Joint Conference on Biometrics*; 2014 Sep 29-Oct 2; Clearwater, FL, USA. IEEE; 2014. p. 1-7. DOI
90. Jiang Y, Liu X. Spoof fingerprint detection based on co-occurrence matrix. *LISP* 2015;8:373-84. DOI
91. Gragnaniello D, Poggi G, Sansone C, Verdoliva L. Local contrast phase descriptor for fingerprint liveness detection. *Pattern Recognition* 2015;48:1050-8. DOI
92. Gottschlich C. Convolution comparison pattern: an efficient local image descriptor for fingerprint liveness detection. *PLoS One* 2016;11:e0148552. DOI PubMed PMC
93. Dubey RK, Goh J, Thing VLL. Fingerprint liveness detection from single image using low-level features and shape analysis. *IEEE Trans Inform Forensic Secur* 2016;11:1461-75. DOI
94. Yuan C, Xia Z, Sun X, Sun D, Lv R. Fingerprint liveness detection using multiscale difference co-occurrence matrix. *Opt Eng* 2016;55:063111. DOI
95. Kim W, Jung C. Local accumulated smoothing patterns for fingerprint liveness detection. *Electron lett* 2016;52:1912. DOI
96. Ghiani L, Hadid A, Marcialis GL, Roli F. Fingerprint liveness detection using local texture features. *IET biom* 2017;6:224. DOI
97. Kim W. Fingerprint liveness detection using local coherence patterns. *IEEE Signal Process Lett* 2017;24:51. DOI
98. Kumpituck S, Li D, Kunieda H, Isshiki T. Fingerprint spoof detection using wavelet based local binary pattern. Eighth International Conference on Graphical and Image Processing; 2017 Feb 8; Tokyo, Japan. 2017. DOI
99. Xia Z, Lv R, Zhu Y, Ji P, Sun H, Shi Y. Fingerprint liveness detection using gradient-based texture features. *SIVIP* 2017;11:381. DOI
100. González-Soler LJ, Chang L, Hernández-Palancar J, Pérez-Suárez A, Gomez-Barrero M. Fingerprint presentation attack detection method based on a bag-of-words approach. In: Mendenza M, Velastín S, editors. Progress in pattern recognition, image analysis, computer vision, and applications. Cham: Springer International Publishing; 2018. p. 263-71. DOI
101. Kundargi J, Karandikar RG. Fingerprint liveness detection using wavelet-based adapted LBP descriptor. In: Chaudhuri BB, Kankanhalli MS, Ramamohan R, editors. Proceedings of 2nd International Conference on Computer Vision & Image Processing. Singapore: Springer; 2018. p. 187-202. DOI
102. Jiang Y, Liu X. Uniform local binary pattern for fingerprint liveness detection in the gaussian pyramid. *Journal of Electrical and Computer Engineering* 2018;2018:1. DOI
103. Mebboob R, Dawood H, Dawood H, Ilyas MU, Guo P, Banjar A. Live fingerprint detection using magnitude of perceived spatial stimuli and local phase information. *J Electron Imag* 2018;27:1. DOI
104. Xia Z, Yuan C, Lv R, Sun X, Xiong NN, Shi Y. A novel weber local binary descriptor for fingerprint liveness detection. *IEEE Trans Syst Man Cybern, Syst* 2020;50:1526-36. DOI
105. Tan G, Zhang Q, Hu H, Zhu X, Wu X. Fingerprint liveness detection based on guided filtering and hybrid image analysis. *IET Image Processing* 2020;14:1710-5. DOI
106. Nosaka R, Ohkawa Y, Fukui K. Feature extraction based on co-occurrence of adjacent local binary patterns. In: Ho Y, editor. Advances in image and video technology. Berlin: Springer Berlin Heidelberg; 2012. p. 82-91. DOI
107. Kumar M, Singh P. Liveness detection and recognition system for fingerprint images. In: Saini HS, Singh RK, Tariq Beg M, Sahabji NS, editors. Innovations in electronics and communication engineering. Singapore: Springer; 2020. p. 467-77. DOI
108. FVC-onGoiNG: On-line evaluation of fingerprint recognition algorithms. Available from: https://biolab.csr.unibo.it/fvcgoing/UI/Form/Home.aspx. [Last accessed on 12 Oct 2021].
109. Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications* 2018;40:217-35. DOI
110. Karampidis K, Kavallieratou E, Papadourakis G. A dilated convolutional neural network as feature selector for spatial image steganalysis - a hybrid classification scheme. *Pattern Recognit Image Anal* 2020;30:342-58. DOI
111. Menotti D, Chiachia G, Pinto A, et al. Deep representations for iris, face, and fingerprint spoofing detection. *IEEE Trans Inform Forensic Secur* 2015;10:864-79. DOI
112. Nogueira RF, de Alencar Lotufo R, Campos Machado R. Fingerprint liveness detection using convolutional neural networks. *IEEE Trans Inform Forensic Secur* 2016;11:1206-13. DOI
113. Krizhevsky A, Sutskever I, Hinton GE. ImageNet classification with deep convolutional neural networks. *Advances in neural information processing systems* 2012;25:1097-105. DOI
114. Kim S, Park B, Song BS, Yang S. Deep belief network based statistical feature learning for fingerprint pattern recognition. *Pattern Recognition Letters* 2016;77:58-65. DOI
115. Marasco E, Wild P, Cukic B. Robust and interoperable fingerprint spoof detection via convolutional neural networks. 2016 IEEE Symposium on Technologies for Homeland Security (HST); 2016 May 10-11; Waltham, MA, USA. IEEE; 2016. p. 1-6. DOI
116. Deng J, Dong W, Socher R, Li LJ, Li K, Li FF. ImageNet: a large-scale hierarchical image database. 2009 IEEE Conference on Computer Vision and Pattern Recognition; 2009 Jun 20-25; Miami, FL, USA. IEEE; 2009. p. 248-55. DOI
117. Pala F, Bhanu B. Deep triplet embedding representations for liveness detection. In: Bhanu B, Kumar A, editors. Deep learning for
biometrics. Cham: Springer International Publishing; 2017. p. 287-307. DOI
118. Jung H, Heo Y. Fingerprint liveness map construction using convolutional neural network. Electron lett 2018;54:564-6. DOI
119. Pinto A, Pedrini H, Krumdick M, et al. Counteracting presentation attacks in face, fingerprint, and iris recognition. In: Vatsa M, Singh R, Majumdar A, editors. Deep learning in biometrics. CRC Press; 2018. p. 245-93. DOI
120. Park E, Cui X, Kim W, Liu J, Kim H. Patch-based fake fingerprint detection using a fully convolutional neural network with a small number of parameters and an optimal threshold. arXiv preprint arXiv:1803.07817, 2018.
121. Park E, Cui X, Nguyen THB, Kim H. Presentation attack detection using a tiny fully convolutional network. IEEE Trans Inform Forensic Secur 2019;14:3016-25. DOI
122. Zhang Y, Shi D, Zhan X, Cao D, Zhu K, Li Z. Slim-ResCNN: a deep residual convolutional neural network for fingerprint liveness detection. IEEE Access 2019;7:9476-87. DOI
123. Yuan C, Chen X, Yu P, et al. Semi-supervised stacked autoencoder-based deep hierarchical semantic feature for real-time fingerprint liveness detection. J Real-Time Image Proc 2020;17:55-71. DOI
124. Pereira JA, Sequeira AF, Pernes D, Cardoso JS. A robust fingerprint presentation attack detection method against unseen attacks through adversarial learning. 2020 International Conference of the Biometrics Special Interest Group (BIOSIG); 2020 Sep 16-18; Darmstadt, Germany. IEEE; 2020. p. 1-5. DOI
125. Uliyan DM, Sadeghi S, Jalab HA. Anti-spoofing method for fingerprint recognition using patch based deep learning machine. Engineering Science and Technology, an International Journal 2020;23:264-73. DOI
126. Zhang Y, Pan S, Zhan X, Li Z, Gao M, Gao C. FLDNet: light dense CNN for fingerprint liveness detection. IEEE Access 2020;8:84541-52. DOI
127. Jian W, Zhou Y, Liu H. Densely connected convolutional network optimized by genetic algorithm for fingerprint liveness detection. IEEE Access 2021;9:2229-43. DOI
128. Derakhshani R, Schuckers SA, Hornak LA, O’gorman L. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition 2003;36:383-96. DOI
129. Parthasaradhi STV, Derakhshani R, Hornak LA, Schuckers SC. Improvement of an algorithm for recognition of liveness using perspiration in fingerprint devices. Biometric Technology for Human Identification; 2004 Aug 25; Orlando, Florida, USA. 2004. p. 270-7. DOI
130. Parthasaradhi S, Derakhshani R, Hornak L, Schuckers S. Time-series detection of perspiration as a liveness test in fingerprint devices. IEEE Trans Syst, Man, Cybern C 2005;35:335-43. DOI
131. Tan B, Schuckers S. Liveness detection using an intensity based approach in fingerprint scanner. Proceedings of Biometrics Symposium (BSYM2005); Arlington, VA. 2005. p. 19-21.
132. Tan B, Schuckers S. Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. Biometric Technology for Human Identification III; 2006 Apr 17; Orlando (Kissimmee), Florida, USA. 2006. DOI
133. Jia J, Cai L. Fake finger detection based on time-series fingerprint image analysis. In: Huang D, Heutte L, Loog M, editors. Advanced intelligent computing theories and applications. With aspects of theoretical and methodological issues. Berlin: Springer Berlin Heidelberg; 2007. p. 1140-50. DOI
134. Plesh R, Bahmani K, Jang G, et al. Fingerprint presentation attack detection utilizing time-series, color fingerprint captures. 2019 International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-8. DOI
135. Szegedy C, Vanhoucke V, Ioffe S, Shlens J, Wojna Z. Rethinking the inception architecture for computer vision. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR); 2016. p. 2818-26. DOI
136. Nogueira RF, de Alencar Lotufo R, Campos Machado R. Evaluating software-based fingerprint liveness detection using Convolutional Networks and Local Binary Patterns. 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings; 2014 Oct 17; Rome, Italy. IEEE; 2014. p. 22-9. DOI
137. Yuan C, Sun X, Wu QMJ. Difference co-occurrence matrix using BP neural network for fingerprint liveness detection. Soft Comput 2019;23:5159-69. DOI
138. Yuan C, Sun X, Rui L. Fingerprint liveness detection based on multi-scale LPQ and PCA. China Commun 2016;13:60-5. DOI
139. Agarwal S, Chowdary CR. A stacking and a bagging: adaptive versions of ensemble learning algorithms for spoof fingerprint detection. Expert Systems with Applications 2020;146:113160. DOI
140. Anusha BVS, Banerjee S, Chaudhuri S, DeFraudNet-End2End fingerprint spoof detection using patch level attention. Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (WACV); 2020. p. 2695-704. DOI
141. Huang G, Liu Z, van der Maaten L, Weinberger KQ. Densely connected convolutional networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR); 2017. p. 4700-8. DOI
142. Woo S, Park J, Lee J, Kweon IS. CBAM: convolutional block attention module. In: Ferrari V, Hebert M, Sminchisescu C, Weiss Y, editors. Computer vision - ECCV 2018. Cham: Springer International Publishing; 2018. p. 3-19. DOI
143. Agarwal D, Bansal A. Fingerprint liveness detection through fusion of pores perspiration and texture features. Journal of King Saud University - Computer and Information Sciences 2020. DOI
144. Li X, Cheng W, Yuan C, Gu W, Yang B, Cui Q. Fingerprint Liveness detection based on fine-grained feature fusion for intelligent devices. Mathematics 2020;8:517. DOI
145. Sharma D, Selwad A. HyFiPAD: a hybrid approach for fingerprint presentation attack detection using local and adaptive image features. Vis Comput 2021. DOI
146. Rattani A, Ross A. Automatic adaptation of fingerprint liveness detector to new spoof materials. IEEE International Joint Conference on Biometrics; 2014 Sep 29-Oct 2; Clearwater, FL, USA. IEEE; 2014. p. 1-8. DOI
Karampidis et al. J Survell Secur Saf 2021;2:117-61 | https://doi.org/10.20517/jsss.2021.07

147. Jia X, Zang Y, Zhang N, Yang X, Tian J. One-class SVM with negative examples for fingerprint liveness detection. In: Sun Z, Shan S, Sang H, Zhou J, Wang Y, Yuan W, editors. Biometric recognition. Cham: Springer International Publishing; 2014. p. 216-24. DOI

148. Rattani A, Scheirer WJ, Ross A. Open set fingerprint spoof detection across novel fabrication materials. IEEE Trans Inform Forensic Secur 2015;10:2447-60. DOI

149. Sequeira AF, Cardoso JS. Fingerprint liveness detection in the presence of capable intruders. Sensors (Basel) 2015;15:14615-38. DOI PubMed PMC

150. Ding Y, Ross A. An ensemble of one-class SVMs for fingerprint spoof detection across different fabrication materials. 2016 IEEE International Workshop on Information Forensics and Security (WIFS); 2016 Dec 4-7; Abu Dhabi, United Arab Emirates. IEEE; 2016. p. 1-6. DOI

151. Gajawada R, Popli A, Chugh T, Namboodiri A, Jain AK. Universal material translator: towards spoof fingerprint generalization. 2019 International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-8. DOI

152. Chugh T, Jain AK. Fingerprint presentation attack detection: generalization and efficiency. 2019 International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-8. DOI

153. Engelsma JJ, Jain AK. Generalizing fingerprint spoof detector: learning a one-class classifier. 2019 International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-8. DOI

154. Grosz SA, Chugh T, Jain AK. Fingerprint presentation attack detection: a sensor and material agnostic approach. 2020 IEEE International Joint Conference on Biometrics (IJCB); 2020 Sep 28-Oct 1; Houston, TX, USA. IEEE; 2020. p. 1-10. DOI

155. González-Soler LJ, Gomez-Barrero M, Chang L, Perez-Suarez A, Busch C. Fingerprint presentation attack detection based on local features encoding for unknown attacks. IEEE Access 2021;9:5806-20. DOI

156. Chugh T, Jain AK. Fingerprint spoof detector generalization. IEEE Trans Inform Forensic Secur 2021;16:42-55. DOI

157. Nikam SB, Agarwal S. Ridgelet-based fake fingerprint detection. Neurocomputing 2009;72:2491-506. DOI

158. Babu A, Paul V, Baby DE. An investigation of biometric liveness detection using various techniques. 2017 International Conference on Inventive Systems and Control (ICISC); 2017 Jan 19-20; Coimbatore, India. IEEE; 2017. p. 1-5. DOI

159. Agarwal S, Rattani A, Chowdary CR. A comparative study on handcrafted features v/s deep features for open-set fingerprint liveness detection. Pattern Recognition Letters 2021;147:34-40. DOI

160. Kim W. Towards real biometrics: an overview of fingerprint liveness detection. 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA); 2016 Dec 13-16; Jeju, Korea (South). IEEE; 2016. p. 1-3. DOI

161. González-Soler LJ, Gomez-Barrero M, Chang L, Suárez AP, Busch C. Fingerprint presentation attack detection based on local features encoding for unknown attacks. International Conference on Biometrics (ICB); 2019 Jun 4-7; Crete, Greece. IEEE; 2019. p. 1-6. DOI

162. Sharma RP, Dey S. A comparative study of handcrafted local texture descriptors for fingerprint liveness detection under real world scenarios. Multimed Tools Appl 2021;80:9993-10012. DOI

163. Li FF, Fergus R, Perona P. One-shot learning of object categories. IEEE Trans Pattern Anal Mach Intell 2006;28:594-611. DOI PubMed

164. Raja KB, Raghavendra R, Venkatesh S, Gomez-barrero M, Rathgeb C, Busch C. A study of hand-crafted and naturally learned features for fingerprint presentation attack detection. In: Marcel S, Nixon MS, Fierrez J, Evans N, editors. Handbook of biometric anti-spoofing. Cham: Springer International Publishing; 2019. p. 33-48. DOI

165. Tuveri P, Ghianni L, Zurutuza M, Mura V, Marcialis GL. Interoperability among capture devices for fingerprint presentation attacks detection. In: Marcel S, Nixon MS, Fierrez J, Evans N, editors. Handbook of biometric anti-spoofing. Cham: Springer International Publishing; 2019. p. 71-108. DOI

166. Marasco E, Sansone C. On the robustness of fingerprint liveness detection algorithms against new materials used for spoofing. Proceedings of the International Conference on Bio-inspired Systems and Signal Processing (MPBS-2011); Setubal: SciTePress; 2011. p. 553-8. DOI

167. Singh M, Singh R, Ross A. A comprehensive overview of biometric fusion. Information Fusion 2019;52:187-205. DOI

168. Ross A, Jain A. Information fusion in biometrics. Pattern Recognition Letters 2003;24:2003-25. DOI

169. Unar J, Seng WC, Abbasi A. A review of biometric technology along with trends and prospects. Pattern Recognition 2014;47:2673-88. DOI

170. Dahe W, Fadewar HS. Multimodal biometric system: a review. International Journal of Research in Advanced Engineering and Technology 2018;4:25-31. DOI

171. Goswami G, Mittal P, Majumdar A, Vatsa M, Singh R. Group sparse representation based classification for multi-feature multimodal biometrics. Information Fusion 2016;32:3-12. DOI

172. Hamad AM, Elhadary RS, Elkhateeb AO. Multimodal biometric personal identification system based on Iris & Fingerprint. International Journal of Computer Science & Communication Networks 2013;3:53-60. DOI

173. Jain AK, Hong L, and Kulkarni Y. A multimodal biometric system using fingerprint, face, and speech. International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA); 1999. p. 182-7. DOI

174. . Ben Ayed NG, Masmoudi AD, Masmoudi DS. A new human identification based on fusion fingerprints and faces biometrics using LBP and GWN descriptors. Eighth International Multi-Conference on Systems, Signals & Devices; 2011 Mar 22-25; Sousse, Tunisia. IEEE; 2011. p. 1-7. DOI

175. Kwon YB, Kim J. Multi-modal authentication using score fusion of ECG and fingerprints. Journal of information and communication convergence engineering 2020;18:132-46. DOI

176. Jomaa RM, Islam MS, Mathkour H. Improved sequential fusion of heart-signal and fingerprint for anti-spoofing. 2018 IEEE 4th
International Conference on Identity, Security, and Behavior Analysis (ISBA); 2018 Jan 11-12; Singapore. IEEE; 2018. p. 1-7. DOI

177. Alajlan N, Islam MS, Ammour N. Fusion of fingerprint and heartbeat biometrics using fuzzy adaptive genetic algorithm. World Congress on Internet Security (WorldCIS-2013); 2013 Dec 9-12; London, UK. IEEE; 2013. p. 76-81. DOI

178. O’gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proc IEEE 2003;91:2021-40. DOI

179. He D, Wang D. Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal 2015;9:816-23. DOI

180. Qiu S, Wang D, Xu G, Kumari S. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE Trans Dependable and Secure Comput 2020. DOI

181. Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Dependable and Secure Comput 2018;15:708-22. DOI

182. Juels A, Rivest RL. Honeywords: making password-cracking detectable. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS ’13); 2013 Nov 04; New York, NY, USA. Springer; 2013. p.145-160. DOI

183. Kim H, Lee S, Yoo K. ID-based password authentication scheme using smart cards and fingerprints. SIGOPS Oper Syst Rev 2003;37:32-41. DOI

184. Scott M. Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints. SIGOPS Oper Syst Rev 2004;38:73-5. DOI

185. Lin C, Lai Y. A flexible biometrics remote user authentication scheme. Computer Standards & Interfaces 2004;27:19-23. DOI

186. Khan MK, Zhang J. Improving the security of ‘a flexible biometrics remote user authentication scheme’. Computer Standards & Interfaces 2007;29:82-5. DOI

187. Rhee HS, Kwon JO, Lee DH. A remote user authentication scheme without using smart cards. Computer Standards & Interfaces 2009;31:6-13. DOI

188. Chen C, Lee C, Hsu C. Mobile device integration of a fingerprint biometric remote authentication scheme. Int J Commun Syst 2012;25:585-97. DOI

189. Khan MK, Kumari S, Gupta MK. More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing 2014;96:793-816. DOI

190. Liu S, Davison AJ, and E. Johns E. Self-supervised generalisation with meta auxiliary learning. arXiv preprint arXiv:1901.08933, 2019.

191. Atoum Y, Liu Y, Jourabloo A, Liu X. Face anti-spoofing using patch and depth-based CNNs. 2017 IEEE International Joint Conference on Biometrics (IJCB); 2017 Oct 1-4; Denver, CO, USA. IEEE; 2017. p. 319-28. DOI