Applied Computing Journal https://doi.org/10.52098/acj.20255460
ISSN: 2788-9688 Volume 5, Issue 4, pp 423-438, October 2025
Received: 24/6/2025 Revised: 15/7/2025 Accepted: 18/7/2025

Hardware and Software Approaches to Fingerprint Liveness Detection: A Comparative Review

Aya Abdulkareem Hameed[1,*], and Abbas H. Hassin Al-Asadi1[1,2]
[1]Computer Science and Information Technology College, University of Basrah, Basrah, Iraq,
[2]IEEE, ACIT member.
* Corresponding author: Aya Abdulkareem[2], ayakareen312@gmail.com

Abstract

Despite being widely utilized, fingerprint recognition systems can be compromised by spoof attacks. Fingerprint liveness detection (FLD) techniques aim to differentiate between genuine and false fingerprints. This paper offers a thorough overview of these methods. In addition to discussing the difficulties presented by sophisticated spoofing materials and techniques, we explore several kinds of spoof attacks, including direct and indirect approaches. FLD methods that are based on hardware and software are examined in this paper, along with their advantages and disadvantages. Strong security is provided by hardware-based methods, such as those that use pressure, scent, electrical, or temperature sensors, however, they frequently need extra hardware parts. In contrast, software-based methods check fingerprint images for liveness cues including texture, color, and motion by employing different algorithms of image processing and pattern recognition. The purpose of this study is to review the most recent FLD research to shed light on the field's present trends and potential prospects. We wrap up by talking about the issues that still need to be resolved and possible directions for further studies, like creating more reliable and effective FLD methods that can adjust to changing spoof assaults. Additionally, we touch on some types of datasets specifically designed for the development of FLD algorithms as well as the metrics utilized to assess the performance of these algorithms to classify real and spoof fingerprints.

Keywords: Fingerprint liveness; Spoof attack; Vitality detection; Handcrafted-based methods; Learning-based methods.

1. Introduction

Automated fingerprint identification systems (AFIS) are extensively utilized in various daily applications, such as electronic payment, accessing smart devices, user identity recognition systems, etc. Simultaneously, the protection of these systems is of increasing anxiety because of the challenges of fingerprint spoof attacks (Marcel et al., 2019).

Two main types of attacks compromise the security of AFIS. The first one is called a direct attack/presentation attack which occurs at the sensor level and involves exposing a spoof artificial fingerprint to the sensor to gain unauthorized access (Srivastava et al., 2023; Alkishri et al., 2024). This type of attack is the most common because it does not require much effort or specialized skills. The second one is called indirect attack which occurs in the rest of the AFIS except for the sensor, by using advanced software and technologies to control the AFIS and gain unauthorized access. This type requires expertise in software programming, which is why it is less common than the first type (Marasco & Ross, 2014; Ametefe et al., 2022).

In this paper, we will focus on the first type of attack, which is called direct attack/presentation. Artificial fingerprint fakes, called spoofs, can be simply made up by several cheap and usually available synthetic materials, including Silicone, Play-Doh, wood glue, and gelatin (Arora et al., 2016; Schultz et al., 2018). In addition, improved 3D printing methods are also used in fingerprint presentation attacks (Arora et al., 2017). Two well-known methods for replicating real fingerprints and fabricating fake ones from them. The first one can be conducted cooperatively by the fingerprint owner and this way provides better quality, reduces time and effort, and eliminates legal disputes. On the other hand, fake fingerprints can be conducted non-cooperatively, by utilizing the latent fingerprints that remain on surfaces, such as the surface of fingerprint sensor (Sousedik & Busch, 2014) (Al-Ajlan, 2013).

Due to these challenges, fingerprint liveness detection (FLD) is considered a main strategy to mitigate this threat and thwarts spoof attacks through using various hardware-based and software-based techniques to determine whether the fingerprint belongs to a live user or not (Abhyankar & Schuckers, 2004; Coli et al., 2007). This survey focuses on explaining these methods and the researchers' attempts to improve their detection by summarizing the related research.

2. Fingerprint Liveness Detection

In general, Fingerprint liveness detection (FLD) methods are mainly categorized into hardware-based and software-based depending on whether they use extra sensors alongside the biometric system or not (Coli et al., 2007). Figure 1 presents the taxonomy of FLD methods.

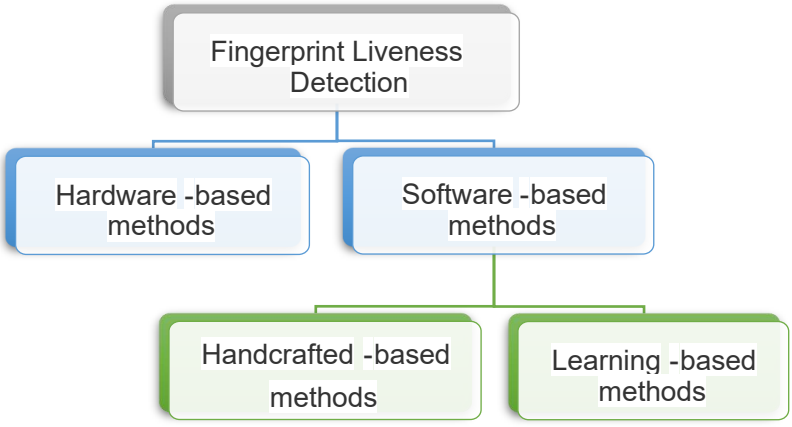

Figure 1: Taxonomy of FLD methods.

2.1. Hardware-Based Methods

In the early stages of FLD, researchers relied on methods that used additional sensors alongside the biometric system to reveal the biological and physiological measurement of the finger as a vitality feature such as pulse and blood flow, blood pressure, skin distortion, temperature, or odor (Sepasian et al., 2009).

Lapsley et al. (Lapsley et al., 1998) introduced an innovative biometric scanner designed to detect the spoof by examining whether the scanned finger displays blood flow characteristics indicative of a live human. By utilizing a lighting source for enlightening the object, a photodetector to measures the target's light energy, and processing methods for managing the light source and processing the output. The main problem when using the blood flow and pulse as a sign of liveness is that the human pulse varies from person to person, also it is dependent upon the current emotions of the individual, and the physical exercises carried out before the scan. Furthermore, the fake finger's blood flow and pulse may be identified as a live finger and accepted even when the attacker uses a light artificial fake fingerprint (Chetty & Yang, 2011; Schuckers, 2002).

Baldisserra et al. (Baldisserra et al., 2006) introduced the first research that used finger scent as a sign of liveness depending on the fact that human skin odor differs from the odor of synthetic materials. They proposed a spoofed detection approach based on a scent sensor (electronic nose) to test the scent signals and applied an algorithm to distinguish whether the scent is of human skin or synthetic materials like silicone and gelatin, etc. The equal error rate (EER) of Baldisserra approach is 7.48%. However, the limitation of using odor as a signal of liveness is that some artificial materials such as gelatin have the same sensor response as a live finger. Furthermore, the scent of human skin changes with several environmental factors, such as the food type and climatic conditions.

Drahansky et al. (Drahansky et al., 2006; Drahansky et al., 2008) proposed an FLD method based on the examination of the fingertip surface subtle movements and measuring the variations in the volume of the fingertip caused by the blood flow which sign of heart activity using two optical solutions, the first one based on CCD camera and macro-objective, and the other one based on triangulation distance laser sensor. They noted that this method required extra time to acquire a sequence of images, in addition to extra hardware (CCD camera or laser sensor). However, this method did not execute testing to prove the validity of it.

Reddy et al. (Reddy et al., 2008) proposed a method based on the principle of pulse oximetry (Blood oxygen measurement) to determine the fingerprint vitality by determining hemoglobin's oxygen saturation (%SPO2). Furthermore, they used the heart pulse as another vitality measurement. The main challenges the researchers face in this study include determining the oxygen saturation threshold, which plays a critical role in determining fingerprint liveness. The oxygen level can be influenced by the user's health condition, such as anemia, or low body temperature. Additionally, it is difficult to eliminate the impact of ambient light, which requires the device to be used either in a dark room or under sunlight and this is an impractical solution. Moreover, the measurement is affected by certain physical factors such as skin elasticity and body oils.

Drahansky (Drahansky, 2008) and many other studies (Van der Putte & Keuning, 2000; Sandstrom, 2004) have shown that using skin temperature as a measure for FLD is inappropriate, unsafe, and inefficient. All researchers reached a consensus that in a normal environment, the skin temperature of humans is 8-10 □C higher than room temperature. For instance, if the room temperature is 18-20 □C, the skin temperature would be 26-30 □C. When using

thin silicone or gelatin artificial fingerprint, it reduces the skin temperature that reaches the sensor by 2□C approximately. This slight difference is considered within the normal range; therefore, using thin synthetic materials may go undetected. Additionally, skin temperature is influenced by the user's illness, such as fever or impaired circulation.

Furthermore, when replicating fake fingerprints, only the features of the outer layer of the human skin can be replicated. So, Cheng and Larin (Cheng & Larin, 2006) utilized the technique of optical coherence tomography (OCT) to differentiate fake fingerprints from real ones by extracting the internal features under the skin. The OCT images for real finger skin show three layers (stratum corneum, epidermis, and dermis) visible, and the OCT images for gelatin placed over a human finger were also analyzed. They found that gelatin appears as a homogeneous medium with a less scattering OCT signal compared to natural skin and the natural skin layers beneath it remain visible. Furthermore, autocorrelation analysis was performed on a specific region of the OCT images. The results indicate the autocorrelation function values for synthetic materials rapidly drop to zero as depth increases due to their homogeneous structure. In contrast, natural skin is heterogeneous, so the values decrease almost linearly as depth increases. Although this method achieved good results, the main limitation is that the cost of the OCT system is higher than the common fingerprint sensors.

Moon et al. (Moon et al., 2005) used a Digital Reflex camera and observed that the external layer of the spoof fingerprint has a rougher texture compared to live ones. The large molecules in synthetic materials frequently tend to cluster together, this makes the out layer of spoof fingerprint rougher than that of live fingerprint. Therefore, this feature was used to detect fingerprint liveness. It is worth noting that this method requires a high-resolution sensor to capture this difference (1000 dpi). Additionally, due to this high resolution, it does work on a fixed-size patch of the original image, rather than on the whole image. To extract this texture feature, the remaining noise resulting from the noise reduction process applied to the initial patch and calculate the noise 's standard deviation to focus on the rough differences of both live and spoof fingerprints.

Since the method in (Moon et al., 2005) requires high-resolution sensors, Pereira et al. (Pereira et al., 2013) suggested a method based on the spatial surface coarseness analysis (SSCA) for traditional fingerprint sensors resolution (500 dpi) in three primary steps: coarseness plotting, descriptor extraction and final classification. The average classification error (ACE) was 70.09%, which is less than that obtained in (Moon et al., 2005). This enhancement is due to the presentation of spatial features in texture analysis of fingertip surfaces.

Chang et al. (Chang et al., 2011) introduced a simple and practical algorithm that used a spectrum analysis for liveness detection. The physical characteristics of both artificial and real fingerprints were analyzed, such as the mean energy of the fingerprint image and the mean energy of the edge of the image. Images captured by nine various wavelengths were utilized to contrast real and fake fingerprints. The analysis reveals that when exposed to nearinfrared light, artificial fingerprints reflect and scatter the light energy from a deeper surface compared to real fingerprints. Additionally, living tissues absorb more light, resulting in less reflected light from real fingerprints, which preserves better image details.

However, utilizing the hardware-based methods will make the system more complex, requiring regular maintenance to ensure it operates correctly, in addition to the high costs which are considered the main drawbacks of these methods (Marasco & Ross, 2014).

2.2. Software-Based Methods

As an alternative of using extra hardware and avoiding its drawbacks and limitations, fingerprint liveness detection can be done using several image processing algorithms to obtain vitality features from the fingerprint images, then utilizing those characteristics to determine whether the target fingerprint is alive (Marcel et al., 2019). The fundamental rationale behind using software-based methods is that certain features of live fingerprints differ significantly from those of fake fingerprints and cannot be detected or replicated (Coli et al., 2007). However, due to the lack of extra hardware as seen in hardware-based methods, software-based methods are less complex, significantly cheaper, and more flexible and reliable (Ametefe et al., 2022).

2.2.1. Fingerprint Features

In software-based methods, several features in the fingerprint surface can be utilized to detect fingerprint vitality, as seen in Figure 2.

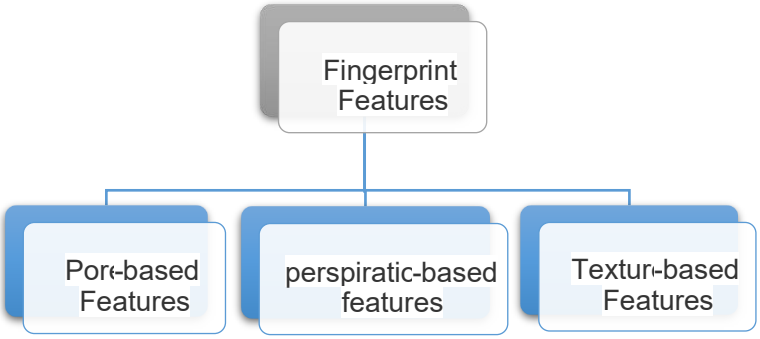

Figure 2: Fingerprint features for liveness detection.

2.2.1.1. Pore-Based Features

In live fingerprints, to ensure physiological thermal control, there are several pores distributed alongside the ridge path (Coli et al., 2007), formed by the duct of sweat glands (Roddy & Stosz, 1997). Such fine details would be extremely complex and difficult to replicate with adequate quality using synthetic materials. Espinoza and Champod (Espinoza & Champod, 2011) have demonstrated that even sweat pores can be artificially replicated, pore quantities in fake fingerprints will inevitably differ from those in live fingerprints. Consequently, this distinction can be used as a discriminating factor for vitality detection. Choi et al. (Choi et al., 2007) introduced a technique that analyzes the pores and utilizes the statistics based on the distance between them (individual pore spacing) as a feature to distinguish live fingerprints from fake ones. The method has an approximately 85% classification rate only.

2.2.1.2. Perspiration-Based Features

As is well known, these pores are the source of perspiration. When live fingerprints touch the surface of the scanner, the skin become moist due to the increased amount of sweat. Many researchers have presented their findings on this phenomenon using a single image.

Derakhshani et al (Derakhshani et al., 2003) proved that the patterns of sweating were detected just on live fingerprints. Jin et al. (Jin et al., 2011) opined that the pores in the live fingerprint image differ from those obtained from fake ones due to the phenomenon of sweating.

Also, the physiological phenomenon of sweating can be noted by capturing consecutive frames over a defined interval of a few seconds. Consequently, the change in skin moisture will result in differences in the gray level distribution of the consecutive images. To assess this feature, the captured frames are converted into two-dimensional signals. Various statistical metrics are suggested based on the acquired signals, such as in (Derakhshani et al., 2003), DM1 (overall swing ratio), DM2 (Min/Max growth proportion), DM3 (mean of the difference between the last and first fingerprint signals), and DM4 (percent change in standard deviation). It was essential to make some adjustments to the initial method. Parthasaradhi et al. (Parthasaradhi et al., 2005) draw up a great analysis of several scanner technology. The device's dynamic could yield to a overloaded signal due to a surplus moisture, under these circumstances, the feature DM2(Min/Max growth proportion) lost its original efficiency. To prevent this issue, two other features known as DM5 (variation in percentage of dry saturation) and DM6 (variation in percentage of wet saturation) were introduced.

Based on the work presented by Parthasaradhi et al. (Parthasaradhi et al., 2005) and Coli et al. (Coli et al. 2006) utilized these new features (DM5 and DM6) besides other features to detect fingerprint vitality on the extended database. In particular, DM5 and DM6 were acquired respectively 60,7% and 82.1% classification accuracy.

2.2.1.3. Texture-Based Features

The structure quality of fingerprint texture can be relied upon as a feature for detecting vitality, for several reasons: The significant distinction in texture structure between live and fake fingerprints such as continuity, integrity, structure, orientation, roughness, and regularity of ridges. Furthermore, in the fabrication of fake fingerprints, it is difficult to replicate the extremely fine details present in live ones. Additionally, there are differences in elasticity properties between them (Sousedik & Busch, 2014).

Due to the presence of these pores, live fingerprint images exhibit an irregular pattern and ridge paths. When fake fingerprints are fabricated, these fine details cannot be replicated with sufficient quality, leading to a more regular ridge bath. Therefore, researchers have proposed analyzing this feature using wavelets. Tan and Schuckers (Tan & Schuckers, 2006) and Derakhshani et al. (Derakhshani et al., 2003) introduced an approach based on sweat with two types of transformation, (Tan & Schuckers, 2006) with Wavelet Space and (Derakhshani et al., 2003) with Fourier Space using a single fingerprint image. In (Tan & Schuckers, 2006) the fingerprint image improved the clearness of ridge and valley structure and converted into one-dimensional signal (a data sequence that can be mathematically analyzed), followed by wavelet analysis of this signal using multi-resolution scheme: the mean value of each wavelet coefficient, the standard deviation, and the signals from the original and last approximation are calculated. The final classification stage will use the 14 parameters as a feature vector for. In (Derakhshani et al., 2003) after extracting the 2D fingerprint structure image, it is converted into a one-dimensional signal which denotes the gray-level value alongside the ridge structure. This signal is then analyzed using the Fast Fourier Transform (FFT) to investigate the gray value variability due to the presence of pores. The entire energy of the ridge signal is computed, and finally, the

fingerprint images are categorized by the energy thresholding. However, due to the personal properties of pore periodicity, it is inadequate to detect fingerprint vitality by using simple threshold values.

Tan and Schuckers (Tan & Schuckers, 2010) analyze the ridge signals and valleys noise. These ridge signals of live fingerprints are periodically dictated by the regular presence of active sweat pores. This contrasts with what is found in fake fingerprints. Due to the lack of a sweating process, the ridge signals do not exhibit similar periodic nature, as they do not contain active sweat pores. This makes the ridge patterns appear different, and irregular compared to those of live fingerprints. Their method achieved an average error rate (AER) of 0.9%.

Marasco and Sansone (Marasco & Sansone, 2012) introduced a method that combines a set of static features derived from sweat and the variations between the morphologies of authentic and counterfeit fingerprints. The morphology-based features are first-order statistics which measure the likelihood of the presence of a gray value at the randomly selected location in the image, and residual noise which represent the difference between the initial image and the filtered image. In addition, the perspiration-based features are the space between the pores and the graylevel intensity. Their method achieved a mean error rate of 12.47% which is considered high to consider its practical applications. Jin et al. (Jin et al., 2011) pointed out that the median ridge-valley signals are noteworthy liveness features. Their findings pointed out that live fingerprints show more pores in the middle ridge line (MRL) signals and higher graylevel values in the middle valley line (MVL) signals compared to fake fingerprints. Additionally, fake fingerprints have less periodic middle ridge signals and noisier middle valley signals, because of the difficulties in replicating the pores, and this is what the researchers also found in (Tan & Schuckers, 2010).

Tan and Schuckers (Tan & Schuckers, 2008) introduced a method based on analyzing the noise alongside the valley structure of the fingerprint. Since real fingerprints have a clear valley structure, fake fingerprints have noticeable noise scattering because of the properties of synthetic materials. Antonelli et al. (Antonelli et al., 2006) introduced a dynamic procedure to detect fingerprint vitality according to elastic deformation. The user is instructed to rotate the scanner after placing his fingerprint on its surface. These movements generate elastic tension across the entire fingerprint surface, resulting in elastic deformation that depends on the skin's elasticity level of the live fingerprint, or the synthetic materials used to fabricate the fake fingerprint. A dynamic acquirement process captures a consecutive image at an elevated frame rate (more than 20 frames per second). The authors refer to the feature vector representing the elastic deformation between consecutive frames as "distortion code", obtained by calculating the optical flow which measures the temporal variations caused by the image's rotation.

Galbally et al. (Galbally et al., 2012) proposed an FLD method that leverages various quality measures derived from fingerprint features, including ridge strength, continuity, and the ridge-valley integrity. Additionally, the method measures the verification performance of the fingerprint image in question. To extract these features, they utilized information from the direction field, Gabor filters (which provide additional representation of directional angles), pixel strength from gray-scale images, and power spectrum analysis. The method achieved a total ACE of 10.4%.

As seems, the above fingerprint features can be obtained into two states (Marcel et al., 2019):

The static state of the features which are typically derived from a single image/impression of the fingerprint. The dynamic state of the features which are typically extracted based on the examination of sequential image frames

of the same fingerprint, which is captured while the user puts his fingerprint on the sensor surface at a certain time (e.g., 0-5 sec) (Coli et al., 2007). Figure 3 shows Multiple frames of real and fake fingerprints.

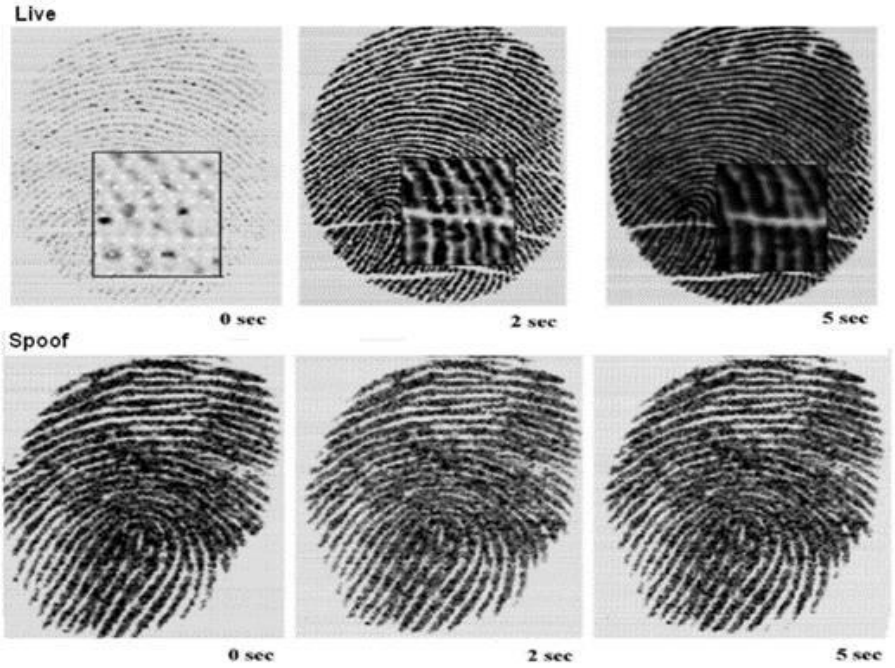

Figure 3: Multiple frames of real and spoof fingerprints (Parthasaradhi et al., 2005).

2.2.2. Liveness Detection Methods

Software-based methods are mainly categorized into two categories: Handcrafted-based methods and Learningbased methods. (as shown in Figure 1).

2.2.2.1. Handcrafted-Based Methods

The initial software-based methods suggested for liveness detection relieve on hand-crafted features that are significantly influenced by the expertise and domain knowledge of the specialist (Yuan et al., 2017). Based on this drastic difference between live and fake fingerprints, early works proposed many texture descriptor algorithms measuring the quality of the above fingerprint features (Galbally et al., 2009). Wang and He (Wang & He, 1990) introduced a texture investigation based on "texture-unit (TU)", where a texture image can be represented by its texture continuum. The TU is exemplified by eight elements, each one has one of three values (0,1,2) achieved from 3×3 area pixels. In total, there are possible 38 = 6561 TUs explaining spatial three level patterns in 3×3 neighborhoods. Then the distribution of TUs computed which represents the texture spectrum.

Ojala et al. (Ojala et al., 1996) proposed an updated two-level variant of the Wang and He method (Wang & He, 1990), which offers a strong approach for representing basic local binary patterns (LBP) in texture analysis. In this method, the original 3×3 neighborhood is the threshold based on the center pixel's value. Then the pixel values in this threshold neighborhood are multiplied by specific weights assigned to the corresponding pixels. See the example in Figure 4. The total sum of the values from the eight pixels gives the TU value which is in the example equal to 169.

The LBP method is invariant with grayscale changes and can be simply merged with a contrast measure by calculating the average gray level variation between the pixels with values of 1 and 0.

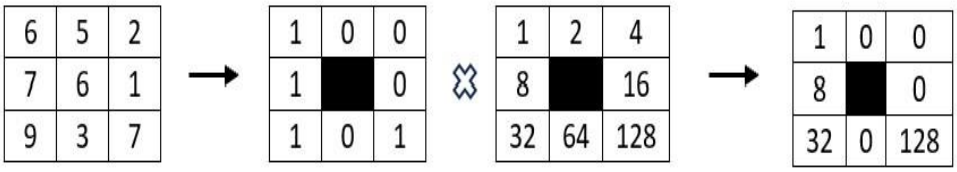

Figure 4: Example of the LBP of texture unit.

The original LBP method in (Ojala et al., 1996) is constrained by its limited spatial coverage area (3×3) which might fail to identify the essential texture features. As a result, in 2002 Ojala et al. (Ojala et al., 2002) expanded to accommodate various sizes of the circular vicinity and assessed the pixel values in the image using linear estimation. Thus, LBP can be applied at any radius or for any pixel count in a specific vicinity. The LBP value of any pixel (Gc) derived from the gray values of the symmetrically circular vicinity (Gp) is calculated as mentioned in Equation (1).

$$LBR_{P,R} = \sum_{P=0}^{P-1} \mathrm{S}\left(\mathrm{G}_p - G_c\right) * 2_p \quad \ldots. (1)$$

P represents the quantity of sampling points located on a circle with a radius of R, and the value of S(x) is determined as mentioned in Equation (2).

$$\mathrm{S(x)} = \begin{cases} 1, \text{if } \mathrm{x} \geq 0 \\ 0, \text{if } \mathrm{x} < 0 \end{cases} \quad \ldots (2)$$

Furthermore, to enhance the area affected by LBP, they Presented a multi-scale rotation-invariant technique in LBP, employing three different radii to represent the texture information. The fingerprint texture is too intricate to be fully represented by the aforementioned LBP. Thus, Jia et al. (Jia et al., 2014) proposed an updated approach utilizing a multi-scale local binary pattern (MSLBP) for detecting spoof fingerprints. In general, the MSLBP can be put into practice in two different ways, whether by increasing the radius of the circular neighborhoods which augment the quantity of samples at each radius, or by using a series of filters on the image followed by applying the LBP at a constant radius.

After LBP proved its effectiveness through its applications to a wide range of texture classification problems, such as the classification of endoscopic images and face recognition. Nikam and Agarwal (Nikam and Agarwal, 2008) introduced FLD's initial use of texture features, using local binary pattern (LBP) histograms to acquire the textural minutiae. They considered three distinct spatial and angular resolutions associated with (P, R) values of (8, 1), (16, 2), and (24, 3) respectively. They obtained rotation-invariant uniform histograms with 10, 18, and 26 bins correspondingly. Then these histograms are summed up resulting in a 54-dimensional feature vector. Finally, this feature vector is used to represent and evaluate the texture features in fingerprint images and use a hybrid classifier for liveness classification.

Xia et al. (Xia et al., 2018) introduced an innovative descriptor known as Weber Local Binary Descriptor (WLBD) for FLD, which involves two modules: the local binary differential excitation (LBDE) module to extract strengthchange features and local binary gradient orientation (LBGO) module to extract direction features. Then the

cooccurrence likelihood is computed to compose a distinguishing feature vector which is input into the support vector machine (SVM) classifier for final classification. WLBD achieved a total ACE of 5.96% on the LivDet 2011 dataset,

1.89% on the LivDet 2013 dataset, and 9.67% on the LivDet 2015 dataset. Gragnaniello et al. (Gragnaniello et al., 2013) investigated the use of (WLBD) and (LBP) for FLD on LivDet 2009 and LivDet 2011 and compared it with several algorithms. The results indicate that combining the local features of WLD and LPQ achieves a great performance in distinguishing life from fake fingerprints, significantly surpassing other methods and enhancing detection accuracy. Gragnaniello et al. (Gragnaniello et al., 2015) proposed a local descriptor called Local Contrast Phase Descriptor (LCPD), by observing the fingerprint image in spatial domains and frequency domains. This dual analysis captures key details about the local scale contrast in the spatial domain and local phase behavior in the frequency domain through specific transform coefficients. Then, these details are used to construct a two-dimensional contrast-phase histogram, which serves as the feature vector representing the fingerprint image. Finally, use the SVM classifier to ascertain if the fingerprint is genuine or fake. LCPD achieved a total ACE of 5.7%.

Ghiani et al. (Ghiani et al., 2012) offered new features set derived from fingerprint images based on the Local Phase Quantization (LPQ), which is a insensitive texture classification to represent all spectrum features of images in a very dense representation to avoid redundant or blurred information. LPQ achieved an Equal Error Rate (EER) of

12.3%. Yuan et al. (Yuan et al., 2016) proposed a method based on a multiscale differential co-occurrence matrix (DCM). The multiscale wavelet transformation is performed on the original image, then the DCM are calculated consuming the Laplacian operator, calculating the horizontal and vertical of DCM, the elements of processing DCM considered the texture features of the original image and classified them using support vector machine (SVM) classifier. The DCM method achieved an ACE of 7.59% in the LivDet 2013 dataset and 6.185% in the LivDet 2011 dataset. However, the above algorithms are complicated to generalize due to the absence of strength versus unidentified materials and variety of sensors. Additionally, the descriptors of texture are a class of shallow feature that only exhibit the out-layer features, while leaving those critical ones unidentified (Zhang et al., 2020).

2.2.2.2. Learning -Based Methods

The handcrafted-based methods primarily identify fingerprint vitality using a single feature in its initial stages and it has not demonstrated high performance across different synthetic materials. Deep learning techniques introduce a powerful method to enhance system performance (Khamis & Yousif, 2022; Alkishri et al., 2023). However, deep learning methods progressively acquire knowledge about fake fingerprints (Uliyan et al., 2020). Recently, deep learning has been widely used in several biometric systems to develop FLD algorithms that are highly robust and interpretable.

CNNs have significantly contributed to the progress of the FLD system. Many deep learning techniques are utilized for FLD such as GoogLeNet (Marasco et al., 2016) and VGG-19 (Nogueira et al. 2016) which are based on CNN was pre-trained using natural images as an alternative of re-designing a new network structure specifically for FLD. Conversely, there is a massive differentiation between fingerprint images and natural images that make the parameters of pre-trained models on natural images fail to achieve the anticipated performance on FLD. Moreover, the randomly

cropped fingerprint images and adjusted resolution to fit the network input size will result in the distortion of the fingerprint image and loss of critical fingerprint information which led to a reduction the accuracy (Zhang et al., 2019).

Nogueira et al. (Nogueira et al., 2014) implemented and evaluated two different feature extraction techniques: the first one is a convolution neural network (CNN) with random weights, and the other one is Local Binary Patterns (LBP). Both were applied that used support vector machine (SVM) classifier. They implemented them into two pipelines, the first one without performing augmentation: LBP with SVM achieves 21.28% ACE, and CNN with SVM achieves 9.47% ACE. However, after performing augmentation, the results became 9.67% and 4.71% respectively. It seems that LBP has an extremely low cross-validation error (almost 0%), which causes overfitting when dataset augmentation procedures are not used.

Based on the results of (Nogueira et al., 2014), Yuan et al. (Yuan et al., 2017) apply a convolution neural network (CNN) to differentiate real fingerprints from spoof ones and perform Region of Interest (ROI) and Principal

Components Analysis (PCA) operations to reduce the redundant information and extract the utmost distinct features. Finally, the obtained features are fed into support vector machine (SVM) classifier. This method achieves 4.57% ACE in LivDet 2013 dataset and 7.25% in LivDet 2011. Chugh et al. (Chugh et al., 2018) proposed a Convolutional neural network (CNN) network and employed a vote strategy utilizing several local patches placed around minutiae. However, their approach demonstrated limitations in accurately extracting minutiae from fake fingerprint images. Many counterfeit fingerprints can yield over 100 minutiae, which complicates the localization process and increases computational cost and time due to the need to analyze such many patches.

Moreover, deep learning models started with a single network architecture, but as advancements were made, more complex hybrid models combining multiple network types were developed and applied in some studies.

Uliyan et al. (Uliyan et al., 2020) introduced a method that utilized Deep Boltzmann Machines (DBM) and Deep Restricted Boltzmann Machines (DRBM) to extract deep features of grayscale fingerprints through their probabilistic multilayer architecture and K-Nearest neighbor (KNN) classifier is used with the ROIs feature vectors which are extracted by the DBM to detect spoof fingerprints. The Average Classification Error (ACE) of this method is 3.6%.

Sandouka et al. (Sandouka et al., 2021) proposed architecture founded on generative adversarial networks (GANs) and transformers to address the weak generalization capability of fingerprint presentation attack detection (PAD) across several sensors and spoof materials. To decrease the division gap between source and target samples, CycleGAN transforms the source samples to be like a few real target samples. This adaptation makes the source data more compatible with the target domain. Then, a hybrid network of CNN and Transformer is trained on both original and CycleGAN-augmented source samples which enhances the model's generalization across varied sensor data. The proposed architecture rose the classification accuracy from 68.52% to 83.12%.

In addition to the challenge mentioned in (Chugh et al., 2018), another issue has arisen as FLD systems are increasingly shifting toward embedded and mobile devices, where computational power and storage capacity are significantly limited. Therefore, the need arises to design lightweight networks to improve computational efficiency, reduce memory usage, and enable real-time processing on resource-constrained devices. Zhang et al. (Zhang et al., 2019) introduced a modified version of the novel residual network (ResNet) named Slim-ResCNN, which was a

lightweight but effective residual convolutional neural network specifically designed for FLD. Slim-ResCNN effectively mitigates issues of overfitting and reducing the processing time, with an overall accuracy of 95.25%.

Zhang et al. (Zhang et al., 2020) also introduced an efficient and lightweight CNN architecture consisting of only 0.48 M parameters, named FLDNet. The model incorporates an attention pooling layer that addresses the limitations of Global Average Pooling (GAP) in fingerprint liveness detection (FLD). The primary drawback of GAP is its tendency to give equal weight to each unit within the feature representation which is not optimal for FLD applications. FLDNet achieves an Average Classification Error (ACE) of 1.76%.

Nguyen et al. (Nguyen et al., 2018) proposed a PAD method using convolutional Neural Networks (CNN) called fPADnet, which is a compact neural network based on the SqueezeNet architecture, which emphasizes design efficiency and reduced size by minimizing the number of filters and optimizing the internal distribution of feature maps. It employs a Gram-K module to compute Gram matrices for texture representation while preserving all information, allowing the network to process images in their original sizes. This design integrates these features into a small, effective model suitable for practical applications. fPAnet achieved an ACE of 2.8% without augmentation and 5.0% with augmentation of the datasets. Zhang et al. (Zhang et al., 2023) designed a lightweight FLD network named LFLDnet based on ResNet with a Multi-head self-attention (MASH) mechanism to improve recognition accuracy and reduce the overall network parameters (only 0.83M). Also, they used the CycleGan networks for fingerprint image style transfer to enhance the model generalization ability. LFLDnet Achieved an ACE of 1.72%.

3. FLD datasets

Fingerprint liveness detection involves various datasets consisting of many different real and fake fingerprints which are captured by different sensors and fake fingerprints fabricated from different synthetic materials.

Fingerprint Liveness Detection Competition (LivDet) is a prominent and accessible forum for academic and private firms that specialize in presentation attack detection challenge, aims to evaluate the performance of fingerprint presentation attack detection (FPAD) algorithms through the use of standardized experimental protocol and datasets. Since 2009, the biannual LivDet competition has introduced a unique set of challenges with each edition, pushing competitors to develop new solutions to detect fingerprint vitality. Micheletto et al. (Micheletto et al., 2023) introduced a comprehensive review of LivDet publications covering the years 2009–2021 and highlighted their development.

Sokoto Coventry Fingerprint Dataset (SOCOFing) is another dataset for FLD tasks that is available on Kaggle. The SOCOFing dataset comprises 6,000 real fingerprint images from 600 African people, each providing ten fingerprints. Synthetic alterations were applied using the STRANGE toolbox, producing images with varying difficulty: 17,934 easy, 17,067 medium, and 14,272 hard, totaling 55,273 images (Shehu et al., 2018). Another database known as ATVS-FakeFingerprint Database (ATVS-FFp DB) has 3,168 fingerprint images divided into two subsets: the first one is dataset with cooperation of fingerprint owner in generating the gummy fingers, contains of 816 real and 816 fake images. The second one contains 768 real and 768 fake images, obtained without user cooperation.

4. Models Evaluations

The following parameters are used for evaluating the classification performance:

- TP (True Positives): The count of live fingerprints accurately identified as live.

- TN (True Negatives): The count of spoof fingerprints accurately identified as spoof.
- FP (False Positives): The count of spoof fingerprints mistakenly identified as live.
- FN (False Negatives): The count of live fingerprints mistakenly identified as a spoof.

4.1. Average Classification Error (ACE)

The ACE can be mathematically defined as shown in Equation (3).

$$ACE = \frac{1}{n}\sum_{i=1}^{n}(error_i) \quad \dots (3)$$

Where N : is the entire number of fingerprint samples tested.

Error: is the classification error for the i sample.

4.2. Accuracy rate (ACC)

Accuracy is the percentage of properly classified examples (both live and spoof fingerprints) out of the total instances tested. It can be mathematically expressed as shown in Equation (4).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \dots (4)$$

4.3. Recall

Also referred to as sensitivity or true positive ratio which evaluates the capability of a system to exactly identify live fingerprints within all actual live examples. Recall is mathematically defined as shown in Equation (5).

$$Recall = \frac{TP}{TP+FN} \quad \dots (5)$$

4.4. Precision

Precision represents the balance of correctly classified live fingerprints among all fingerprints that the system classifies as live. Precision is mathematically defined as shown in Equation (6).

$$\text{Precision} = \frac{TP}{TP+FP} \quad \dots (6)$$

4.5. F1 Score

F1- Score is the harmonical meaning of precision and recall defined as shown in Equation (7).

$$\text{F1 Score} = 2x\frac{\text{Precision x recall}}{\text{Precision + recal}} \quad \dots (7)$$

5. Conclusion

Fingerprint presentation attack detection (PAD) has garnered important attention from researchers. This paper provides a comparative review of the various methods of fingerprint liveness detection (FLD) and examines algorithms developed from the 1990s to the present, highlighting the evolution from hardware-based approaches and handcrafted algorithms to modern deep learning techniques. Additionally, it discusses the fingerprint features utilized to differentiate between real and phony fingerprints and the methods for extracting these features. Furthermore, several datasets specifically designed for this field are mentioned, along with performance evaluation metrics for networks and algorithms. Despite the existence of many PAD techniques that address various types of fingerprint presentation

attacks, there remains a pressing need for a reliable and effective fingerprint PAD system capable of adapting to diverse fingerprint artifacts.

Acknowledgment

The research leading to these results has received no Research Grant Funding.

Author contribution: All authors have contributed, read, and agreed to the published version of the manuscript results.

Conflict of interest: The authors declare no conflict of interest.

References

[1]. Abhyankar, A. S., & Schuckers, S. C. (2004, August). A wavelet-based approach to detecting liveness in fingerprint scanners. In Biometric Technology for Human Identification (Vol. 5404, pp. 278-286). SPIE.

[2]. Al-Ajlan, A. (2013, April). Survey on fingerprint liveness detection. In 2013 International Workshop on Biometrics and Forensics (IWBF) (pp. 1-5). IEEE.

[3]. Alkishri, W., Widyarto, S., & Yousif, J. H. (2024). Evaluating the effectiveness of a Gan fingerprint removal approach in fooling deepfake face detection. Journal of Internet Services and Information Security (JISIS), 14(1), 85-103.

[4]. Alkishri, W., Widyarto, S., Yousif, J. H., & Al-Bahri, M. (2023). Fake face detection based on colour textual analysis using deep convolutional neural network. Journal of Internet Services and Information Security, 13(3), 143-155.

[5]. Ametefe, D. S., Sarnin, S. S., Ali, D. M., & Zaheer, M. Z. (2022). Fingerprint liveness detection schemes: A review on presentation attack. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 10(2), 217-240.

[6]. Antonelli, A., Cappelli, R., Maio, D., & Maltoni, D. (2006). Fake finger detection by skin distortion analysis. IEEE Transactions on Information Forensics and Security, 1(3), 360-373.

[7]. Arora, S. S., Cao, K., Jain, A. K., & Paulter, N. G. (2016). Design and fabrication of 3D fingerprint targets. IEEE Transactions on Information Forensics and Security, 11(10), 2284-2297.

[8]. Arora, S. S., Jain, A. K., & Paulter, N. G. (2017). Gold fingers: 3D targets for evaluating capacitive readers. IEEE transactions on information forensics and security, 12(9), 2067-2077.

[9]. Baldisserra, D., Franco, A., Maio, D., & Maltoni, D. (2006, January). Fake fingerprint detection by odor analysis. In International Conference on Biometrics (pp. 265-272). Berlin, Heidelberg: Springer Berlin Heidelberg.

[10]. Chang, S., Secker, J., Xiao, Q., Reid, B., Bergeron, A., & Almuhtadi, W. (2011). Artificial finger detection by spectrum analysis. International Journal of Biometrics, 3(4), 376-389.

[11]. Cheng, Y., & Larin, K. V. (2006). Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis. Applied optics, 45(36), 9238-9245.

[12]. Chetty, G., & Yang, J. (Eds.). (2011). Advanced Biometric Technologies. BoD–Books on Demand.

[13]. Choi, H., Kang, R., Choi, K., & Kim, J. (2007, July). Aliveness detection of fingerprints using multiple static features. In Proc. of World Academy of Science, Engineering and Technology (Vol. 22).

[14]. Chugh, T., Cao, K., & Jain, A. K. (2018). Fingerprint spoof buster: Use of minutiae-centered patches. IEEE Transactions on Information Forensics and Security, 13(9), 2190-2202.

[15]. Coli, P., Marcialis, G. L., & Roli, F. (2006, August). Analysis and selection of features for the fingerprint vitality detection. In Joint IAPR International Workshops on Statistical Techniques in Pattern Recognition (SPR) and Structural and Syntactic Pattern Recognition (SSPR) (pp. 907-915). Berlin, Heidelberg: Springer Berlin Heidelberg.B. Tan and S. Schuckers, "Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing," in 2006 Conf. Comput. Vis. Pattern Recognit. Workshop (CVPRW'06), 2006, pp. 2626.

[16]. Coli, P., Marcialis, G. L., & Roli, F. (2007, August). Vitality detection from fingerprint images: a critical survey. In International Conference on Biometrics (pp. 722-731). Berlin, Heidelberg: Springer Berlin Heidelberg.

[17]. Derakhshani, R., Schuckers, S. A., Hornak, L. A., & O'Gorman, L. (2003). Determination of vitality from a noninvasive biomedical measurement for use in fingerprint scanners. Pattern recognition, 36(2), 383-396.

[18]. Drahansky, M. (2008, August). Experiments with skin resistance and temperature for liveness detection. In 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 1075-1079). IEEE.

[19]. Drahansky, M., & Lodrova, D. (2008, April). Liveness detection for biometric systems based on papillary lines. In 2008 International Conference on Information Security and Assurance (isa 2008) (pp. 439-444). IEEE.
[20]. Drahansky, M., Notzel, R., & Funk, W. (2006, June). Liveness detection based on fine movements of the fingertip surface. In 2006 IEEE Information Assurance Workshop (pp. 42-47). IEEE.
[21]. Espinoza, M., & Champod, C. (2011, November). Using the number of pores on fingerprint images to detect spoofing attacks. In 2011 International Conference on Hand-Based Biometrics (pp. 1-5). IEEE.
[22]. Galbally, J., Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. (2012). A high performance fingerprint liveness detection method based on quality related features. Future Generation Computer Systems, 28(1), 311321.
[23]. Galbally, J., Alonso-Fernandez, F., Fierrez, J., & Ortega-Garcia, J. (2009, September). Fingerprint liveness detection based on quality measures. In 2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS) (pp. 1-8). IEEE.
[24]. Gragnaniello, D., Poggi, G., Sansone, C., & Verdoliva, L. (2013, September). Fingerprint liveness detection based on weber local image descriptor. In 2013 IEEE workshop on biometric measurements and systems for security and medical applications (pp. 46-50). IEEE.
[25]. Gragnaniello, D., Poggi, G., Sansone, C., & Verdoliva, L. (2015). Local contrast phase descriptor for fingerprint liveness detection. Pattern Recognition, 48(4), 1050-1058.
[26]. Jia, X., Yang, X., Cao, K., Zang, Y., Zhang, N., Dai, R., ... & Tian, J. (2014). Multi-scale local binary pattern with filters for spoof fingerprint detection. Information Sciences, 268, 91-102.
[27]. Jin, C., Li, S., Kim, H., & Park, E. (2010, August). Fingerprint liveness detection based on multiple image quality features. In International Workshop on Information Security Applications (pp. 281-291). Berlin, Heidelberg: Springer Berlin Heidelberg.
[28]. Khamis, Y., & Yousif, J. H. (2022). Deep learning Feedforward Neural Network in predicting model of Environmental risk factors in the Sohar region. Artificial Intelligence & Robotics Development Journal, 201-2013.
[29]. L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in Proceedings of the 21st international conference on pattern recognition (ICPR2012), 2012, pp. 537-540.
[30]. Lapsley, P. D., Lee, J. A., Pare Jr, D. F., & Hoffman, N. (1998). U.S. Patent No. 5,737,439. Washington, DC: U.S. Patent and Trademark Office.
[31]. Marasco, E., & Ross, A. (2014). A survey on antispoofing schemes for fingerprint recognition systems. ACM Computing Surveys (CSUR), 47(2), 1-36.
[32]. Marasco, E., & Sansone, C. (2012). Combining perspiration-and morphology-based static features for fingerprint liveness detection. Pattern Recognition Letters, 33(9), 1148-1156.
[33]. Marasco, E., Wild, P., & Cukic, B. (2016, May). Robust and interoperable fingerprint spoof detection via convolutional neural networks. In 2016 IEEE symposium on technologies for homeland security (HST) (pp. 16). IEEE.
[34]. Marcel, S., Fierrez, J., & Evans, N. (Eds.). (2023). Handbook of biometric anti-spoofing: Presentation attack detection and vulnerability assessment (Vol. 1). Cham, Switzerland: Springer.
[35]. Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the fingerprint liveness detection (livdet) competition series: from 2009 to 2021. Handbook of biometric antispoofing: presentation attack detection and vulnerability assessment, 57-76.
[36]. Moon, Y. S., Chen, J. S., Chan, K. C., So, K., & Woo, K. C. (2005). Wavelet based fingerprint liveness detection. Electronics Letters, 41(20), 1112-1113.
[37]. Nguyen, T. H. B., Park, E., Cui, X., Nguyen, V. H., & Kim, H. (2018). fPADnet: Small and efficient convolutional neural network for presentation attack detection. Sensors, 18(8), 2532.
[38]. Nikam, S. B., & Agarwal, S. (2008, July). Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems. In 2008 first international conference on emerging trends in engineering and technology (pp. 675-680). IEEE.
[39]. Nogueira, R. F., de Alencar Lotufo, R., & Machado, R. C. (2014, October). Evaluating software-based fingerprint liveness detection using convolutional networks and local binary patterns. In 2014 IEEE workshop on biometric measurements and systems for security and medical applications (BIOMS) Proceedings (pp. 2229). IEEE.
[40]. Nogueira, R. F., de Alencar Lotufo, R., & Machado, R. C. (2016). Fingerprint liveness detection using convolutional neural networks. IEEE transactions on information forensics and security, 11(6), 1206-1213.
[41]. Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. Pattern recognition, 29(1), 51-59.

[42]. Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on pattern analysis and machine intelligence, 24(7), 971-987.
[43]. Parthasaradhi, S. T., Derakhshani, R., Hornak, L. A., & Schuckers, S. A. (2005). Time-series detection of perspiration as a liveness test in fingerprint devices. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 35(3), 335-343.
[44]. Pereira, L. F. A., Pinheiro, H. N. B., Cavalcanti, G. D., & Ren, T. I. (2013). Spatial surface coarseness analysis: technique for fingerprint spoof detection. Electronics letters, 49(4), 260-261.
[45]. Reddy, P. V., Kumar, A., Rahman, S. M. K., & Mundra, T. S. (2008). A new antispoofing approach for biometric devices. IEEE transactions on biomedical circuits and systems, 2(4), 328-337.
[46]. Roddy, A. R., & Stosz, J. D. (1997). Fingerprint features-statistical analysis and system performance estimates. Proceedings of the IEEE, 85(9), 1390-1421.
[47]. Sandouka, S. B., Bazi, Y., & Alajlan, N. (2021). Transformers and generative adversarial networks for liveness detection in multitarget fingerprint sensors. Sensors, 21(3), 699.
[48]. Sandström, M. (2004). Liveness detection in fingerprint recognition systems.
[49]. Schuckers, S. A. (2002). Spoofing and anti-spoofing measures. Information Security technical report, 7(4), 5662.
[50]. Schultz, C. W., Wong, J. X., & Yu, H. Z. (2018). Fabrication of 3D fingerprint phantoms via unconventional polycarbonate molding. Scientific reports, 8(1), 9613.
[51]. Sepasian, M., Mares, C., & Balachandran, W. (2009). Liveness and spoofing in fingerprint identification: Issues and challenges. In Proc. 4th WSEAS Int. Conf. Comput. Eng. Appl.(CEA) (pp. 150-158).
[52]. Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). Sokoto coventry fingerprint dataset. arXiv preprint arXiv:1807.10609.
[53]. Sousedik, C., & Busch, C. (2014). Presentation attack detection methods for fingerprint recognition systems: a survey. Iet Biometrics, 3(4), 219-233.
[54]. Srivastava, D., Sharma, N., Sinwar, D., Yousif, J. H., & Gupta, H. P. (Eds.). (2023). Intelligent Internet of Things for Smart Healthcare Systems. CRC Press.
[55]. Tan, B., & Schuckers, S. (2008). New approach for liveness detection in fingerprint scanners based on valley noise analysis. Journal of Electronic Imaging, 17(1), 011009-011009.
[56]. Tan, B., & Schuckers, S. (2010). Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. Pattern Recognition, 43(8), 2845-2857.
[57]. Uliyan, D. M., Sadeghi, S., & Jalab, H. A. (2020). Anti-spoofing method for fingerprint recognition using patch based deep learning machine. Engineering Science and Technology, an International Journal, 23(2), 264-273.
[58]. Van der Putte, T., & Keuning, J. (2000, September). Biometrical fingerprint recognition: don't get your fingers burned. In Smart Card Research and Advanced Applications: IFIP TC8/WG8. 8 Fourth Working Conference on Smart Card Research and Advanced Applications September 20–22, 2000, Bristol, United Kingdom (pp. 289303). Boston, MA: Springer US.
[59]. Wang, L., & He, D. C. (1990). Texture classification using texture spectrum. Pattern recognition, 23(8), 905910.
[60]. Xia, Z., Yuan, C., Lv, R., Sun, X., Xiong, N. N., & Shi, Y. Q. (2018). A novel weber local binary descriptor for fingerprint liveness detection. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(4), 15261536.
[61]. Yuan, C., Li, X., Wu, Q. M., Li, J., & Sun, X. (2017). Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. Computers, Materials & Continua, 53(4).
[62]. Yuan, C., Xia, Z., Sun, X., Sun, D., & Lv, R. (2016). Fingerprint liveness detection using multiscale difference co-occurrence matrix. Optical Engineering, 55(6), 063111-063111.
[63]. 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 Jul 8;7:91476-87.
[64]. Zhang, K., Huang, S., Liu, E., & Zhao, H. (2023). LFLDNet: lightweight fingerprint liveness detection based on ResNet and transformer. Sensors, 23(15), 6854.
[65]. Zhang, Y., Pan, S., Zhan, X., Li, Z., Gao, M., & Gao, C. (2020). Fldnet: Light dense cnn for fingerprint liveness detection. IEEE Access, 8, 84141-84152.