Chapter 1
An Introduction to Fingerprint Presentation Attack Detection

Javier Galbally, Julian Fierrez and Raffaele Cappelli

Abstract This chapter provides an introduction to Presentation Attack Detection (PAD), also coined anti-spoofing, in fingerprint biometrics, and summarizes key developments for that purpose in the last two decades. After a review of selected literature in the field, we also revisit the potential of quality assessment for presentation attack detection. We believe that, beyond the interest that the described techniques may intrinsically have by themselves, the case study presented may serve as an example of how to develop and validate fingerprint PAD techniques based on common and publicly available benchmarks and following a systematic and replicable protocol.

1.1 Introduction

"*Fingerprints cannot lie, but liars can make fingerprints*". Unfortunately, this paraphrase of an old quote attributed to Mark Twain[1] has been proven right on many occasions now.

J. Galbally
European Commission, Joint Research Centre, Ispra, Italy
e-mail: javier.galbally@ec.europa.eu

J. Fierrez (✉)
Universidad Autonoma de Madrid, Madrid, Spain
e-mail: julian.fierrez@uam.es

R. Cappelli
Università di Bologna, Cesena, Italy
e-mail: raffaele.cappelli@unibo.it

[1] Figures do not lie, but liars do figure.

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*,
Advances in Computer Vision and Pattern Recognition,
https://doi.org/10.1007/978-3-319-92627-8_1

As the deployment of fingerprint systems keeps growing year after year in such different environments as airports, laptops, or mobile phones, people are also becoming more familiar to their use in everyday life and, as a result, the security weaknesses of fingerprint sensors are becoming better known to the general public. Nowadays, it is not difficult to find websites or even tutorial videos, which give detail guidance on how to create fake fingerprints which may be used for spoofing biometric systems.

As a consequence, the fingerprint stands out as one of the biometric traits which has arisen the most attention not only from researchers and vendors, but also from the media and users, regarding its vulnerabilities to Presentation Attacks (PAs) (aka spoofing). This increasing interest of the biometric community in the security evaluation of fingerprint recognition systems against presentation attacks has led to the creation of numerous and very diverse initiatives in this field: the publication of many research works disclosing and evaluating different fingerprint presentation attack approaches [1–4]; the proposal of new Presentation Attack Detection (PAD) (aka anti-spoofing) methods [5–7]; related book chapters [8, 9]; PhD and MSc Theses which propose and analyze different fingerprint PA and PAD techniques [10–13]; several patented fingerprint PAD mechanisms both for touch-based and contactless systems [14–18]; the publication of Supporting Documents and Protection Profiles in the framework of the security evaluation standard Common Criteria for the objective assessment of fingerprint-based commercial systems [19, 20]; the organization of competitions focused on vulnerability assessment to fingerprint presentation attacks [21, 22]; the acquisition of specific datasets for the evaluation of fingerprint protection methods against direct attacks [23, 24], the creation of groups and laboratories which have the evaluation of fingerprint security as one of their major tasks [25–27]; or of several European Projects on fingerprint PAD as one of their main research interests [28, 29].

The aforementioned initiatives and other analogue studies have shown the importance given by all parties involved in the development of fingerprint-based biometrics to the improvement of the systems security and the necessity to propose and develop specific protection methods against PAs in order to bring this rapidly emerging technology into practical use. This way, researchers have focused on the design of specific countermeasures that enable fingerprint recognition systems to detect fake samples and reject them, improving this way the robustness of the applications.

In the fingerprint field, besides other PAD approaches such as the use of multi-biometrics or challenge–response methods, special attention has been paid by researchers and industry to the so-called *liveness detection* techniques. These algorithms use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [30]: (i) noninvasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; (ii) user-friendly, people should not be reluctant to use it; (iii) fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost, a wide use cannot be expected if the cost is excessively high; (v) performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

Liveness detection methods are usually classified into one of two groups: (i) *Hardware-based* techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or odor); (ii) *Software-based* techniques, in this case, the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as presentation attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor [31, 32].

Although, as shown above, a great amount of work has been done in the field of fingerprint PAD and big advances have been reached over the last decade, the attacking methodologies have also evolved and become more and more sophisticated. This way, while many commercial fingerprint readers claim to have some degree of PAD embedded, many of them are still vulnerable to presentation attack attempts using different artificial fingerprint samples. Therefore, there are still big challenges to be faced in the detection of fingerprint direct attacks.[2]

This chapter represents an introduction to the problem of fingerprint PAD, including an example of experimental methodology [33], and example results extracted from [34]. More comprehensive and up to date surveys of recent advances can be found elsewhere [35–37]. After a review of early works in fingerprint PAD, we analyze and evaluate the potential of quality assessment for liveness detection purposes. In particular, we consider two different sets of features: (i) one based on fingerprint-specific quality measures (i.e., quality measures which may only be extracted from a fingerprint image); (ii) a second set based on general image quality measures (i.e., quality measures which may be extracted from any image). Both techniques are tested on publicly available fingerprint spoofing databases where they have reached results fully comparable to those obtained on the same datasets and following the same experimental protocols by top-ranked approaches from the state of the art.

In addition to their very competitive performance, as they are software-based, both methods present the usual advantages of this type of approaches: fast, as they only

[2] https://www.iarpa.gov/index.php/research-programs/odin/

need one image (i.e., the same sample acquired for verification) to detect whether it is real or fake; nonintrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required).

The rest of the chapter is structured as follows. A review of relevant early works in the field of fingerprint PAD is given is Sect. 1.2. A brief description of large and publicly available fingerprint spoofing databases is presented in Sect. 1.3. A case study based on the use of quality assessment as PAD tool is introduced in Sect. 1.4 where we give some key concepts about image quality assessment and the rationale behind its use for biometric protection. The two fingerprint PAD approaches studied in the chapter based on fingerprint-specific and general quality features are described respectively in Sects. 1.5 and 1.6. The evaluation of the methods and experimental results are given in Sect. 1.7. Conclusions are finally drawn in Sect. 1.8.

1.2 Early Works in Fingerprint Presentation Attack Detection

The history of fingerprint forgery in the forensic field is probably almost as old as that of fingerprint development and classification itself. In fact, the question of whether or not fingerprints could be forged was positively answered [38] several years before it was officially posed in a research publication [39].

Regarding modern automatic fingerprint recognition systems, although other types of attacks with dead [40] or altered [41] fingers have been reported, almost all the available vulnerability studies regarding presentations attacks are carried out either by taking advantage of the residual fingerprint left behind on the sensor surface, or by using some type of gummy fingertip (or even complete prosthetic fingers) manufactured with different materials (e.g., silicone, gelatin, plastic, clay, dental molding material, or glycerin). In general, these fake fingerprints may be generated with the cooperation of the user, from a latent fingerprint or even from a fingerprint image reconstructed from the original minutiae template [1–3, 23, 42–46].

These very valuable works and other analogue studies have highlighted the necessity to develop efficient protection methods against presentation attacks. One of the first efforts in fingerprint PAD initiated a research line based on the analysis of the skin perspiration pattern which is very difficult to be faked in an artificial finger [5, 47]. These pioneer studies, which considered the periodicity of sweat and the sweat diffusion pattern, were later extended and improved in two successive works applying a wavelet-based algorithm and adding intensity-based perspiration features [48, 49]. These techniques were finally consolidated and strictly validated on a large database of real, fake, and dead fingerprints acquired under different conditions in [24]. More recently, a novel region-based liveness detection approach also based on perspiration parameters and another technique analyzing the valley noise have been proposed by the same group [50, 51]. Part of these approaches has been implemented in commercial products [52], and has also been combined with other morphological features [53, 54] in order to improve the presentation attack detection rates [55].

A second group of fingerprint liveness detection techniques has appeared as an application of the different fingerprint distortion models described in the literature [56–58]. These models have led to the development of a number of liveness detection techniques based on the flexibility properties of the skin [6, 59–61]. In most of these works the user is required to move his finger while pressing it against the scanner surface, thus deliberately exaggerating the skin distortion. When a real finger moves on a scanner surface, it produces a significant amount of distortion, which can be observed to be quite different from that produced by fake fingers which are usually more rigid than skin. Even if highly elastic materials are used, it seems very difficult to precisely emulate the specific way a real finger is distorted, because the behavior is related to the way the external skin is anchored to the underlying derma and influenced by the position and shape of the finger bone.

Other liveness detection approaches for fake fingerprint detection include: the combination of both perspiration and elasticity-related features in fingerprint image sequences [62]; fingerprint-specific quality-related features [7, 34]; the combination of the local ridge frequency with other multiresolution texture parameters [53]; techniques which, following the perspiration-related trend, analyze the skin sweat pores visible in high definition images [63, 64]; the use of electric properties of the skin [65]; using several image processing tools for the analysis of the finger tip surface texture such as wavelets [66], or three very related works using Gabor filters [67], ridgelets [68] and curvelets [69]; analyzing different characteristics of the Fourier spectrum of real and fake fingerprint images [70–74].

A critical review of some of these solutions for fingerprint liveness detection was presented in [75]. In a subsequent work [76], the same authors gave a comparative analysis of the PAD methods efficiency. In this last work, we can find an estimation of some of the best performing static (i.e., measured on one image) and dynamic (i.e., measured on a sequence of images) features for liveness detection, that were later used together with some fake-finger specific features in [77] with very good results. Different static features are also combined in [78], significantly improving the results of the individual parameters. Other comparative results of different fingerprint PAD techniques are available in the results of the Fingerprint Liveness Detection Competitions (LivDet series) [21, 22].

In addition, some very interesting hardware-based solutions have been proposed in the literature applying: multispectral imaging [79, 80], an electrotactile sensor [81], pulse oxiometry [82], detection of the blood flow [14], odor detection using a chemical sensor [83], or another trend based on Near Infrared (NIR) illumination and Optical Coherence Tomography (OCT) [84–89].

More recently, a third type of protection methods which fall out of the traditional two-type classification software- and hardware-based approaches has been started to be analyzed in the field of fingerprint PAD. These protection techniques focus on the study of biometric systems under direct attacks at the *score level*, in order to propose and build more robust matchers and fusion strategies that increase the resistance of the systems against presentation attack attempts [90–94].

Outside the research community, some companies have also proposed different methods for fingerprint liveness detection such as the ones based on ultrasounds

[95, 96], light measurements [97], or a patented combination of different unimodal experts [98]. A comparative study of the PAD capabilities of different commercial fingerprint sensors appears in [99].

Although the vast majority of the efforts dedicated by the biometric community in the field of fingerprint presentation attacks and PAD are focused on touch-based systems, some preliminary works have also been conducted to study the vulnerabilities of contactless fingerprint systems against direct attacks and some protection methods to enhance their security level have been proposed [17, 47, 100].

The approaches mentioned above represent the main historical developments in fingerprint PAD until ca. 2012–2013. For a survey of more recent and advanced methods in the last 5 years we refer the reader to [36, 37], and the ODIN program.[3]

1.3 Fingerprint Spoofing Databases

The availability of public datasets comprising real and fake fingerprint samples and of associated common evaluation protocols is basic for the development and improvement of fingerprint PAD methods.

However, in spite of the large amount of works addressing the challenging problem of fingerprint protection against direct attacks (as shown in Sect. 1.2), in the great majority of them, experiments are carried out on proprietary databases which are not distributed to the research community.

Currently, the two largest fingerprint spoofing databases publicly available for researchers to test their PAD algorithms are:

- LivDet DBs [21, 22]: These datasets were generated for the different campaigns of the Fingerprint Liveness Detection Competition series (in 2009, 2011, 2013, 2015, and 2017). Most of the data can be found in the LivDet series website.[4] Each dataset is complemented with specific training and testing protocols and most campaigns contain over 10,000 samples from over 100 fingers generated with materials such as: silicone, gelatine, latex, wood glue, ecoflex, and playdoh.
- ATVS-Fake Fingerprint DB (ATVS-FFp DB) [34]: This database is available from the website.[5] It contains over 3,000 real and fake fingerprint samples coming from 68 different fingers acquired using a flat optical sensor, a flat capacitive sensor, and a thermal sweeping sensor. The gummy fingers were generated with and without the cooperation of the user (i.e., recovered from a latent fingerprint) using modeling silicone.

[3] https://www.iarpa.gov/index.php/research-programs/odin/

[4] http://livdet.org/

[5] http://atvs.ii.uam.es/index.jsp

1.4 A Case Study: Quality Assessment Versus Fingerprint Spoofing

The problem of presentation attack detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake (Fig. 1.1).

Simple visual inspection of an image of a real fingerprint and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some differences between the real and fake fingerprints may become evident once the images are translated into a proper feature space.

Therefore, the key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "liveness" given the extracted set of features.

In the present chapter, we explore and evaluate the potential of quality assessment for fingerprint liveness detection. In particular, we consider two different sets of features: (i) one based on fingerprint-specific quality measures (i.e., quality measures which may only be extracted from a fingerprint image); (ii) a second set based on general image quality measures (i.e., quality measures which may be extracted from any image).

The use of quality assessment for PAD purposes is promoted by the assumption that: "*It is expected that a fake image captured in an attack attempt will have a different quality than a real sample acquired in the normal operation scenario for which the sensor was designed.*"

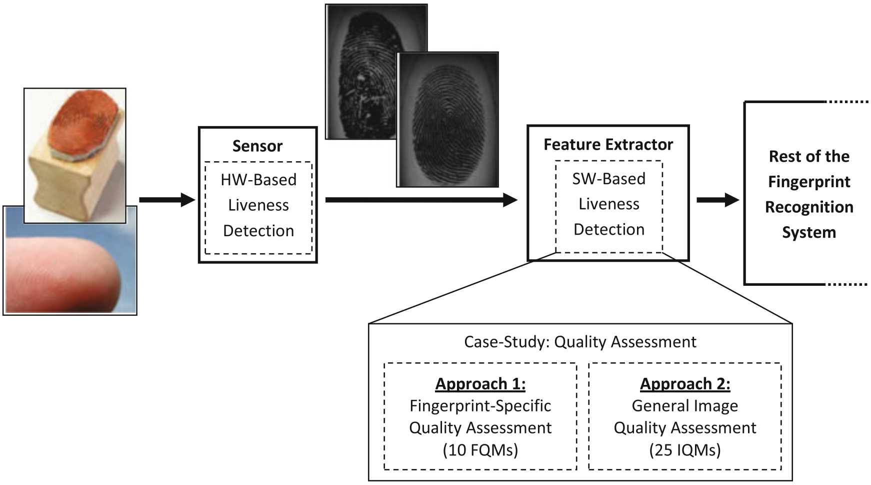

Sensor
HW-Based Liveness Detection
Feature Extractor
SW-Based Liveness Detection
Rest of the Fingerprint Recognition System
Case-Study: Quality Assessment
Approach 1:
Fingerprint-Specific Quality Assessment (10 FQMs)
Approach 2:
General Image Quality Assessment (25 IQMs)

Fig. 1.1 General diagram of the fingerprint PAD case study considered in Sect. 1.4. Approach 1 and Approach 2 are described in Sects. 1.5 and 1.6, respectively. FQMs stands for Fingerprint Quality Measures, while IQMs stands for Image Quality Measures

Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both types of images (entropy), structural distortions, or natural appearance. For example, it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches, or that they have a lower definition of ridges and valleys due to the lack of moisture.

In the current state of the art, the rationale behind the use of quality assessment features for liveness detection is supported by three factors:

- Image quality has been successfully used in previous works for image manipulation detection [101, 102] and steganalysis [103–105] in the forensic field. To a certain extent, many fingerprint presentation attacks may be regarded as a type of image manipulation which can be effectively detected, as shown in the present research work, by the use of different quality features.
- Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. The different metrics and methods implemented here for quality assessment intend to estimate in an objective and reliable way the perceived appearance of fingerprint images.
- Moreover, different quality measures present different sensitivity to image artifacts and distortions. For instance, measures like the mean squared error respond more to additive noise, whereas others such as difference measured in the spectral domain are more sensitive to blur; while gradient-related features react to distortions concentrated around edges and textures. Therefore, using a wide range of quality measures exploiting complimentary image quality properties should permit to detect the aforementioned quality differences between real and fake samples expected to be found in many attack attempts.

All these observations lead us to believe that there is sound proof for the "quality difference" hypothesis and that quality measures have the potential to achieve success in biometric protection tasks.

In the next sections, we describe two particular software-based implementations for fingerprint PAD. Both methods use only one input image (i.e., the same sample acquired for authentication purposes) to distinguish between real and fake fingerprints. The difference between the two techniques relies on the sets of quality-based features used to solve the classification problem: (i) the first PAD method uses a set of 10 fingerprint-specific quality measures (see Sect. 1.5); (ii) the second uses a set of 25 general image quality measures (see Sect. 1.6). Later, both techniques are evaluated on two publicly available databases and their results are compared to other well-known techniques from the state of the art (see Sect. 1.7).

1.5 Approach 1: Fingerprint-Specific Quality Assessment (FQA)

The parameterization proposed in this section comprises ten Fingerprint-specific Quality Measures (FQMs). A number of approaches for fingerprint image quality computation have been described in the literature [110]. Fingerprint image quality can be assessed by measuring one of the following properties: ridge strength or directionality, ridge continuity, ridge clarity, integrity of the ridge–valley structure, or estimated verification performance when using the image at hand. A number of information sources are used to measure these properties: (i) angle information provided by the direction field, (ii) Gabor filters, which represent another implementation of the direction angle [111], (iii) pixel intensity of the gray-scale image, (iv) power spectrum, and (v) neural networks. Fingerprint quality can be assessed either analyzing the image in a holistic manner, or combining the quality from local non-overlapped blocks of the image.

In the following, we give some details about the ten fingerprint-specific quality measures used in this PAD method. The features implemented have been selected in order to cover the different fingerprint quality assessment approaches mentioned above so that the maximum degree of complementarity among them may be achieved. This way, the protection method presents a high generality and may be successfully

Table 1.1 Summary of the 10 Fingerprint-specific Quality Measures (FQMs) implemented in Sect. 1.5 for fingerprint PAD. All features were either directly taken or adapted from the references given. For each feature, the fingerprint property measured and the information source used for its estimation is given. For a more detailed description of each feature, we refer the reader to Sect. 1.5

List of 10 FQMs implemented

#	Acronym	Name	Ref.	Property measured	Source
1	OCL	Orientation Certainty Level	[106]	Ridge strength	Local angle
2	PSE	Power Spectrum Energy	[107]	Ridge strength	Power spectrum
3	LOQ	Local Orientation Quality	[108]	Ridge continuity	Local angle
4	COF	Continuity of the Orientation Field	[106]	Ridge continuity	Local angle
5	MGL	Mean Gray Level	[76]	Ridge clarity	Pixel intensity
6	SGL	Standard Deviation Gray Level	[76]	Ridge clarity	Pixel intensity
7	LCS1	Local Clarity Score 1	[108]	Ridge clarity	Pixel intensity
8	LCS2	Local Clarity Score 2	[108]	Ridge clarity	Pixel intensity
9	SAMP	Sinusoid Amplitude	[109]	Ridge clarity	Pixel intensity
10	SVAR	Sinusoid Variance	[109]	Ridge clarity	Pixel intensity

used to detect a wide range of presentation attacks. A classification of the ten features and of the information source exploited by each of them is given in Table 1.1.

As the features used in this approach evaluate fingerprint-specific properties, prior to the feature extraction process, it is necessary to segment the actual fingerprint from the background. For this preprocessing step, the same method proposed in [112] is used.

1.5.1 Ridge Strength Measures

- **Orientation Certainty Level (OCL)** [106] measures the energy concentration along the dominant direction of ridges using the intensity gradient. It is computed as the ratio between the two eigenvalues of the covariance matrix of the gradient vector. A relative weight is given to each region of the image based on its distance from the centroid, since regions near the centroid are supposed to provide more reliable information [107]. An example of Orientation Certainty Level computation for a real and fake fingerprints is shown in Fig. 1.2.
- **Power Spectrum Energy (PSE)** [107] is computed using ring-shaped bands. For this purpose, a set of bandpass filters is employed to extract the energy in each frequency band. High quality images will have the energy concentrated in few bands while poor ones will have a more diffused distribution. The energy concentration is measured using the entropy. An example of quality estimation using the global quality index PSE is shown in Fig. 1.3 for fake and real fingerprints.

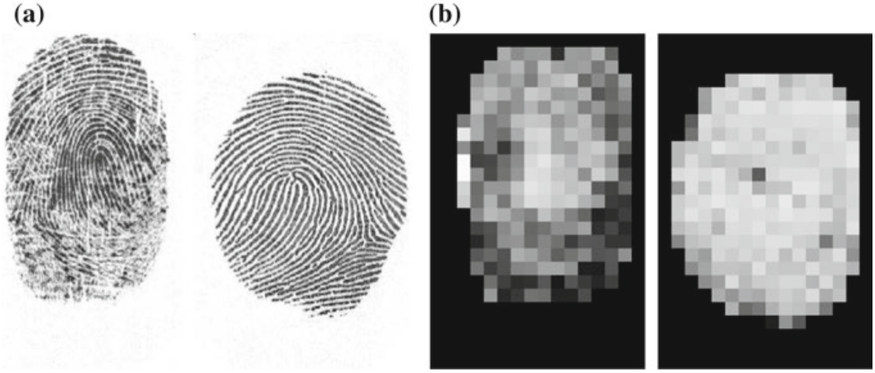
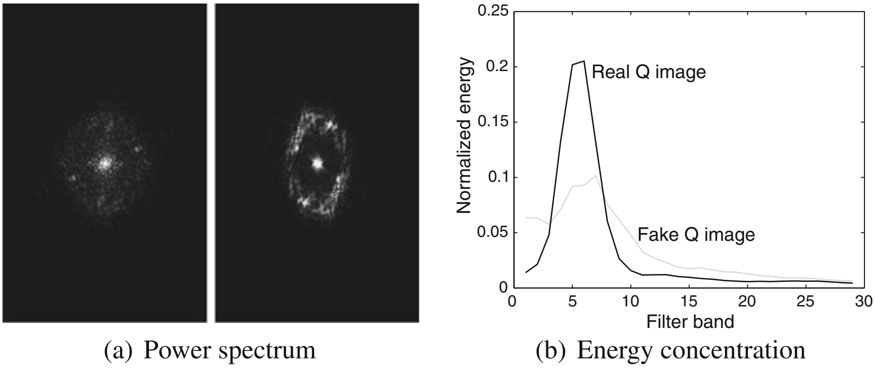


Fig. 1.2 Computation of the Orientation Certainty Level (OCL) for fake and real fingerprints. Panel **a** are the input fingerprint (left is fake, right is real). Panel **b** are the block-wise values of the OCL; blocks with brighter color indicate higher quality in the region



(a) Power spectrum (b) Energy concentration

Fig. 1.3 Computation of the energy concentration in the power spectrum for fake and real fingerprints. Panel **a** are the power spectra of the images shown in Fig. 1.2. Panel **b** shows the energy distributions in the region of interest

1.5.2 Ridge Continuity Measures

- **Local Orientation Quality (LOQ)** [108] is computed as the average absolute difference of direction angle with the surrounding image blocks, providing information about how smoothly direction angle changes from block to block. Quality of the whole image is finally computed by averaging all the Local Orientation Quality scores of the image. In high quality images, it is expected that ridge direction changes smoothly across the whole image. An example of Local Orientation Quality computation is shown in Fig. 1.4 for fake and real fingerprints.
- **Continuity of the Orientation Field (COF)** [106]. This method relies on the fact that, in good quality images, ridges and valleys must flow sharply and smoothly in a locally constant direction. The direction change along rows and columns of the image is examined. Abrupt direction changes between consecutive blocks are then accumulated and mapped into a quality score. As we can observe in Fig. 1.4, ridge direction changes smoothly across the whole image in case of high quality.

1.5.3 Ridge Clarity Measures

- **Mean Gray Level (MGL)** and **Standard Deviation Gray Level (SGL)**, computed from the segmented foreground only. These two features had already been considered for liveness detection in [76].
- **Local Clarity Score (LCS1 and LCS2)** [108]. The sinusoidal-shaped wave that models ridges and valleys [109] is used to segment ridge and valley regions (see Fig. 1.5). The clarity is then defined as the overlapping area of the gray level distributions of segmented ridges and valleys. For ridges/valleys with high clarity,

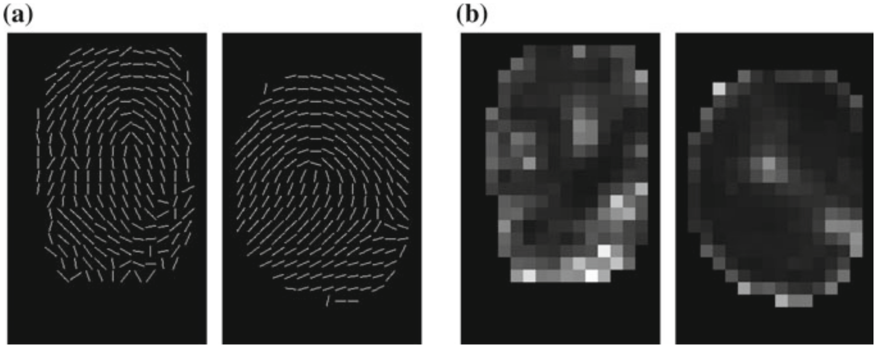
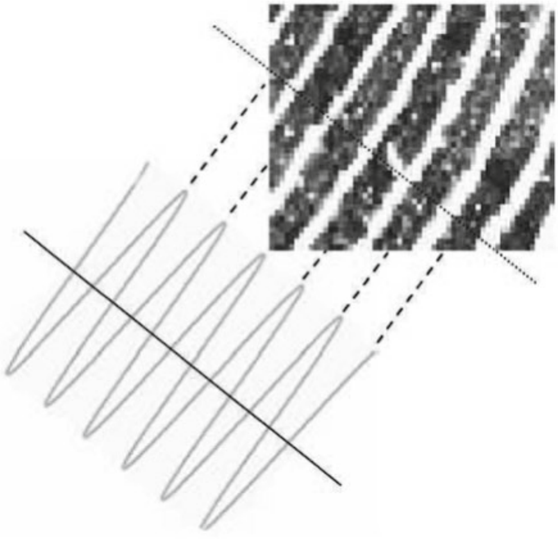


Fig. 1.4 Computation of the Local Orientation Quality (LOQ) for fake and real fingerprints. Panel **a** are the direction fields of the images shown in Fig. 1.2a. Panel **b** are the block-wise values of the average absolute difference of local orientation with the surrounding blocks; blocks with brighter color indicate higher difference value and thus, lower quality

Fig. 1.5 Modeling of ridges and valleys as a sinusoid



both distributions should have a very small overlapping area. An example of quality estimation using the Local Clarity Score is shown in Fig. 1.6 for two fingerprint blocks coming from fake and real fingerprints. It should be noted that sometimes the sinusoidal-shaped wave cannot be extracted reliably, specially in bad quality regions of the image. The quality measure LCS1 discards these regions, therefore being an optimistic measure of quality. This is compensated with LCS2, which does not discard these regions, but they are assigned the lowest quality level.

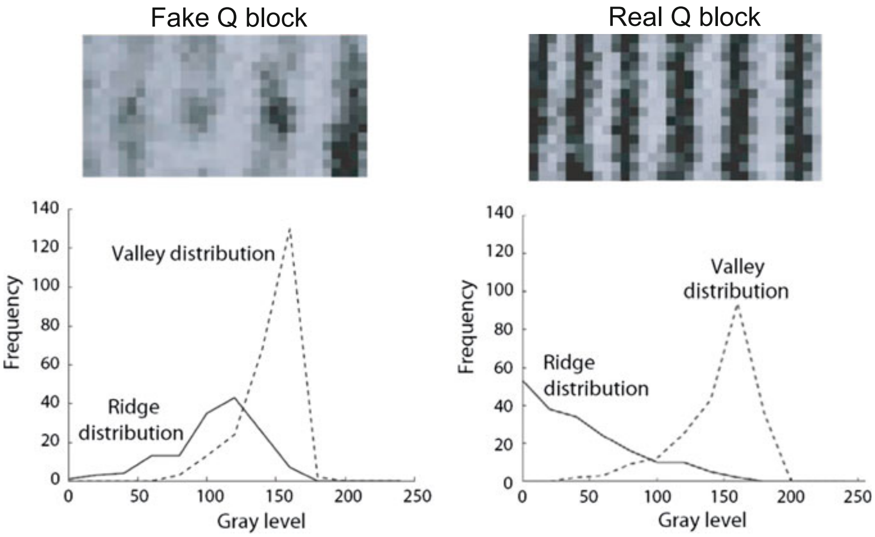


Fig. 1.6 Computation of the Local Clarity Score for two blocks coming from real and fake fingerprints. The fingerprint blocks appear on top, while below we show the gray level distributions of the segmented ridges and valleys. The degree of overlapping for the real and fake blocks is 0.22 and 0.10, respectively

- **Amplitude and Variance of the Sinusoid that models Ridges and Valleys (SAMP and SVAR)** [109]. Based on these parameters, blocks are classified as *good* and *bad*. The quality of the fingerprint is then computed as the percentage of foreground blocks marked as *good*.

1.6 Approach 2: General Image Quality Assessment (IQA)

The goal of an objective Image Quality Measure (IQM) is to provide a quantitative score that describes the degree of fidelity or, conversely, the level of distortion of a given image. Many different approaches for objective Image Quality Assessment (IQA) have been described in the literature [113]. From a general perspective, IQ metrics can be classified according to the availability of an original (distortion-free) image, with which the distorted image is to be compared. Thus, objective IQA methods can fall in one of two categories: (i) *full reference* techniques, which include the majority of traditional automatic image estimation approaches, and where a complete reference image is assumed to be known (e.g., with a large use in the field of image compression algorithms) [114]; (ii) *no-reference* techniques (also referred as *blind*), which assess the quality of the test image without any reference to the original sample, generally using some pretrained statistical model [115].

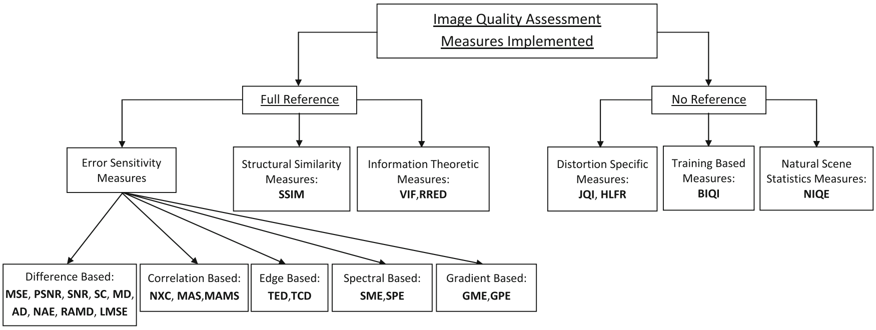


Image Quality Assessment Measures Implemented
Full Reference
No Reference
Error Sensitivity Measures
Structural Similarity Measures: SSIM
Information Theoretic Measures: VIF,RRED
Distortion Specific Measures: JQI, HLFR
Training Based Measures: BIQI
Natural Scene Statistics Measures: NIQE
Difference Based: MSE, PSNR, SNR, SC, MD, AD, NAE, RAMD, LMSE
Correlation Based: NXC, MAS,MAMS
Edge Based: TED,TCD
Spectral Based: SME,SPE
Gradient Based: GME,GPE

Fig. 1.7 Classification of the 25 image quality measures implemented in Sect. 1.6. Acronyms (in bold) of the different measures are explained in Table 1.2

The parameterization proposed in this section and applied to fingerprint liveness detection comprises 25 image quality measures (IQMs) both full reference and blind. In order to generate a system as general as possible in terms of number of attacks detected, we have given priority to IQMs which evaluate complementary properties of the image (e.g., sharpness, entropy or structure). In addition, to assure a user-friendly nonintrusive system, big importance has been given to the complexity and the feature extraction time of each IQM, so that the overall speed of the final fake detection algorithm allows it to operate in real-time environments.

Furthermore, as the method operates on the whole image without searching for any fingerprint-specific properties, it does not require any preprocessing steps (e.g., fingerprint segmentation) prior to the computation of the IQ features. This characteristic minimizes its computational load.

The final 25 selected image quality measures are summarized in Table 1.2. Details about each of these 25 IQMs are given in Sects. 1.6.1 and 1.6.2. For clarity, in Fig. 1.7, we show a diagram with the general IQM classification followed in these sections. Acronyms of the different features are highlighted in bold in the text and in Fig. 1.7.

1.6.1 Full Reference IQ Measures

As described previously, Full Reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection system only has access to the input sample. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in [101] and for steganalysis in [103] is implemented here.

The input gray-scale image $\mathbf{I}$ (of size $N \times M$) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size 3×3) in order to generate a distorted version $\hat{\mathbf{I}}$. Then, the quality between both images ($\mathbf{I}$ and $\hat{\mathbf{I}}$) is computed according to the corresponding

Table 1.2 List of the 25 Image Quality Measures (IQMs) implemented in Sect. 1.6 for fingerprint PAD. All the features were either directly taken or adapted from the references given. In the table: $\mathbf{I}$ denotes the reference clean image (of size $N \times M$) and $\hat{\mathbf{I}}$ the distorted version of the reference image. For other notation specifications and undefined variables or functions, we refer the reader to the description of each particular feature in Sect. 1.6. Also, for those features with no mathematical definition, the exact details about their computation may be found in the given references

	List of the 25 IQMs implemented				
#	Type	Acronym	Name	Ref.	Description
1	FR	MSE	Mean Squared Error	[118]	MSE $(\mathbf{I}, \hat{\mathbf{I}}) = \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal-to-Noise Ratio	[119]	PSNR$(\mathbf{I}, \hat{\mathbf{I}}) = 10 \log \left(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I}, \hat{\mathbf{I}})} \right)$
3	FR	SNR	Signal-to-Noise Ratio	[120]	SNR$(\mathbf{I}, \hat{\mathbf{I}}) = 10 \log \left(\frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j})^2}{N \cdot M \cdot MSE(\mathbf{I}, \hat{\mathbf{I}})} \right)$
4	FR	SC	Structural Content	[121]	SC$(\mathbf{I}, \hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N} \sum_{j=1}^{M} (\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[121]	MD$(\mathbf{I}, \hat{\mathbf{I}}) = \max \lvert \mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j} \rvert$
6	FR	AD	Average Difference	[121]	AD$(\mathbf{I}, \hat{\mathbf{I}}) = \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[121]	NAE$(\mathbf{I}, \hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} \lvert \mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j} \rvert}{\sum_{i=1}^{N} \sum_{j=1}^{M} \lvert \mathbf{I}_{i,j} \rvert}$
8	FR	RAMD	R-Averaged MD	[118]	RAMD$(\mathbf{I}, \hat{\mathbf{I}}, R) = \frac{1}{R} \sum_{r=1}^{R} \max_r \lvert \mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j} \rvert$
9	FR	LMSE	Laplacian MSE	[121]	LMSE$(\mathbf{I}, \hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1} \sum_{j=2}^{M-1} (h(\mathbf{I}_{i,j}) - h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1} \sum_{j=2}^{M-1} h(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	[121]	NXC$(\mathbf{I}, \hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j} \cdot \hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N} \sum_{j=1}^{M} (\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	[118]	MAS$(\mathbf{I}, \hat{\mathbf{I}}) = 1 - \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} \left(\frac{2}{\pi} \cos^{-1} \frac{\langle \mathbf{I}_{i,j}, \hat{\mathbf{I}}_{i,j} \rangle}{\lvert\lvert \mathbf{I}_{i,j} \rvert\rvert \lvert\lvert \hat{\mathbf{I}}_{i,j} \rvert\rvert} \right)$

(continued)

Table 1.2 (continued)

	List of the 25 IQMs implemented				
#	Type	Acronym	Name	Ref.	Description
12	FR	MAMS	Mean Angle Magnitude Similarity	[118]	$\mathrm{MAMS}(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\lVert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rVert}{255}])$
13	FR	TED	Total Edge Difference	[122]	$\mathrm{TED}(\mathbf{I_E},\hat{\mathbf{I}}_\mathbf{E}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I_E}_{i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\rvert$
14	FR	TCD	Total Corner Difference	[122]	$\mathrm{TCD}(N_{cr},\hat{N}_{cr}) = \frac{\lvert N_{cr}-\hat{N}_{cr}\rvert}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	[123]	$\mathrm{SME}(\mathbf{F},\hat{\mathbf{F}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{F}_{i,j}\rvert-\lvert\hat{\mathbf{F}}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	[123]	$\mathrm{SPE}(\mathbf{F},\hat{\mathbf{F}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\langle\mathbf{F}_{i,j}\rangle-\langle\hat{\mathbf{F}}_{i,j}\rangle\rvert^2$
17	FR	GME	Gradient Magnitude Error	[124]	$\mathrm{SME}(\mathbf{G},\hat{\mathbf{G}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{G}_{i,j}\rvert-\lvert\hat{\mathbf{G}}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	[124]	$\mathrm{SPE}(\mathbf{G},\hat{\mathbf{G}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\langle\mathbf{G}_{i,j}\rangle-\langle\hat{\mathbf{G}}_{i,j}\rangle\rvert^2$
19	FR	SSIM	Structural Similarity Index	[125]	See [125] and practical implementation available in [126]
20	FR	VIF	Visual Information Fidelity	[127]	See [127] and practical implementation available in [126]
21	FR	RRED	Reduced Ref. Entropic Difference	[128]	See [128] and practical implementation available in [126]
22	NR	JQI	JPEG Quality Index	[129]	See [129] and practical implementation available in [126]
23	NR	HLFI	High-Low Frequency Index	[130]	$\mathrm{SME}(\mathbf{I}) = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}\lvert\mathbf{I}_{i,j}\rvert-\sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\lvert\mathbf{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
24	NR	BIQI	Blind Image Quality Index	[131]	See [131] and practical implementation available in [126]
25	NR	NIQE	Naturalness Image Quality Estimator	[132]	See [132] and practical implementation available in [126]

full reference IQA metric. This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. Assumption which is confirmed by the experimental results given in Sect. 1.7.

1.6.1.1 FR-IQMs: Error Sensitivity Measures

Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features.

Although their efficiency as signal fidelity measures is somewhat controversial [116], up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system [117], they are easy to calculate and usually have very low computational complexity.

Several of these metrics have been included in the 25-feature parameterization applied in the present work. For clarity, these features have been classified here into five different categories (see Fig. 1.7) according to the image property measured [118]:

- **Pixel Difference Measures** [118, 121]. These features compute the distortion between two images on the basis of their pixelwise differences. Here we include: Mean Squared Error (**MSE**), Peak Signal-to-Noise Ratio (**PSNR**), Signal-to-Noise Ratio (**SNR**), Structural Content (**SC**), Maximum Difference (**MD**), Average Difference (**AD**), Normalized Absolute Error (**NAE**), R-Averaged Maximum Difference (**RAMD**) and Laplacian Mean Squared Error (**LMSE**). The formal definitions for each of these features are given in Table 1.2.
  In the RAMD entry in Table 1.2, $\max_r$ is defined as the r-highest pixel difference between two images. For the present implementation, $R = 10$.
  In the LMSE entry in Table 1.2, $h(\mathbf{I}_{i,j}) = \mathbf{I}_{i+1,j} + \mathbf{I}_{i-1,j} + \mathbf{I}_{i,j+1} + \mathbf{I}_{i,j-1} - 4\mathbf{I}_{i,j}$.
- **Correlation-Based Measures** [118, 121]. The similarity between two digital images can also be quantified in terms of the correlation function. A variant of correlation-based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include (also defined in Table 1.2): Normalized Cross-Correlation (**NXC**), Mean Angle Similarity (**MAS**), and Mean Angle Magnitude Similarity (**MAMS**).
  In the MAMS entry in Table 1.2, $\alpha_{i,j} = \frac{2}{\pi} \cos^{-1} \frac{\langle \mathbf{I}_{i,j}, \hat{\mathbf{I}}_{i,j} \rangle}{||\mathbf{I}_{i,j}|| ||\hat{\mathbf{I}}_{i,j}||}$
- **Edge-Based Measures**. Edges and other two-dimensional features such as corners are some of the most informative parts of an image, which play a key role in the human visual system and in many computer vision algorithms including quality assessment applications [122].
  Since the structural distortion of an image is tightly linked with its edge degradation, here we have considered two edge-related quality measures: Total Edge Difference (**TED**) and Total Corner Difference (**TCD**).

In order to implement both features, which are computed according to the corresponding expressions given in Table 1.2, we use: (i) the Sobel operator to build the binary edge maps $\mathbf{I_E}$ and $\hat{\mathbf{I}}_{\mathbf{E}}$; (ii) the Harris corner detector [133] to compute the number of corners N_{cr} and $\hat{N}_{cr}$ found in $\mathbf{I}$ and $\hat{\mathbf{I}}$.

- **Spectral Distance Measures**. The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment [118, 123]. In this work, we will consider as IQ spectral-related features: the Spectral Magnitude Error (**SME**) and the Spectral Phase Error (**SPE**), defined in Table 1.2 (where $\mathbf{F}$ and $\hat{\mathbf{F}}$ are the respective Fourier transforms of $\mathbf{I}$ and $\hat{\mathbf{I}}$).
- **Gradient-Based Measures**. Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured [124].
  Two simple gradient-based features are included in the biometric protection system studied here: Gradient Magnitude Error (**GME**) and Gradient Phase Error (**GPE**), defined in Table 1.2 (where $\mathbf{G}$ and $\hat{\mathbf{G}}$ are the gradient maps of $\mathbf{I}$ and $\hat{\mathbf{I}}$ defined as $\mathbf{G} = \mathbf{G}_x + i\mathbf{G}_y$, where $\mathbf{G}_x$ and $\mathbf{G}_y$ are the gradients in the x and y directions).

1.6.1.2 FR-IQMs: Structural Similarity Measures

Although being very convenient and widely used, the aforementioned image quality metrics based on error sensitivity present several problems which are evidenced by their mismatch (in many cases) with subjective human-based quality scoring systems [116]. In this scenario, a recent new paradigm for image quality assessment based on structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field [125]. Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones.

Among these recent objective perceptual measures, the Structural Similarity Index Measure (**SSIM**) has the simplest formulation and has gained widespread popularity in a broad range of practical applications [125, 134]. In view of its very attractive properties, the SSIM has been included in the 25-feature parameterization.

1.6.1.3 FR-IQMs: Information Theoretic Measures

The quality assessment problem may also be understood, from an information theory perspective, as an information fidelity problem (rather than a signal fidelity problem). The core idea behind these approaches is that an image source communicates to a receiver through a channel that limits the amount of information that could flow through it, thereby introducing distortions. The goal is to relate the visual quality of the test image to the amount of information shared between the test and the reference signals, or more precisely, the mutual information between them. Under this general framework, image quality measures based on information fidelity exploit the (in some cases unprecise) relationship between statistical image information and visual quality [127, 128].

In the present work, we consider two of these information theoretic features: the Visual Information Fidelity (**VIF**) which measures quality fidelity as the ratio between the total information ideally extracted by the brain from the distorted image and that from the reference sample [127]; and the Reduced Reference Entropic Difference index (**RRED**), which approaches the problem of QA from the perspective of measuring distances between the reference image and the projection of the distorted image onto the space of natural images [128].

1.6.2 No-Reference IQ Measures

Unlike the objective reference IQA methods, in general, the human visual system does not require of a reference sample to determine the quality level of an image. Following this same principle, automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images in the absence of a reference. Presently, NR-IQA methods generally estimate the quality of the test image according to some pretrained statistical model. Depending on the images used to train this model and on the a priori knowledge required, the methods are coarsely divided into one of three trends [115]:

- **Distortion-Specific Approaches**. These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion. The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. Two of these measures have been included in the biometric protection method studied in the present work.
  The JPEG Quality Index (**JQI**) evaluates the quality in images affected by the usual block artifacts found in many compression algorithms running at low bit rates such as the JPEG [129].
  The High-Low Frequency Index (**HLFI**) is formally defined in Table 1.2. It was inspired by previous work which considered local gradients as a blind metric to detect blur and noise [130]. Similarly, the HLFI feature is sensitive to the sharpness of the image by computing the difference between the power in the lower and upper frequencies of the Fourier Spectrum. In the HLFI entry in Table 1.2, i_l, i_h, j_l, j_h are respectively the indices corresponding to the lower and upper frequency thresholds considered by the method. In the current implementation, $i_l = i_h = 0.15N$ and $j_l = j_h = 0.15M$.
- **Training-Based Approaches**. Similarly to the previous class of NR-IQA methods, in this type of techniques a model is trained using clean and distorted images. Then, the quality score is computed based on a number of features extracted from the test image and related to the general model [131]. However, unlike the former

approaches, these metrics intend to provide a general quality score not related to a specific distortion. To this end, the statistical model is trained with images affected by different types of distortions.

This is the case of the Blind Image Quality Index (**BIQI**) described in [131], which is part of the 25 feature set used in the present work. The BIQI follows a two-stage framework in which the individual measures of different distortion-specific experts are combined to generate one global quality score.

- **Natural Scene Statistic Approaches**. These blind IQA techniques use a priori knowledge taken from natural scene distortion-free images to train the initial model (i.e., no distorted images are used). The rationale behind this trend relies on the hypothesis that undistorted images of the natural world present certain *regular* properties which fall within a certain subspace of all possible images. If quantified appropriately, deviations from the regularity of natural statistics can help to evaluate the perceptual quality of an image [132].

  This approach is followed by the Natural Image Quality Evaluator (**NIQE**) used in the present work [132]. The NIQE is a completely blind image quality analyzer based on the construction of a quality aware collection of statistical features (derived from a corpus of natural undistorted images) related to a multi-variate Gaussian natural scene statistical model.

1.7 Results

In order to achieve reproducible results, we have used in the experimental validation two of the largest publicly available databases for fingerprint spoofing (introduced in Sect. 1.3): (i) the LivDet 2009 DB [21] and (ii) the ATVS-FFp DB [34]. This has allowed us to compare, in an objective and fair way, the performance of the proposed system with other existing state-of-the-art liveness detection solutions.

According to their associated protocols, the databases are divided into a: train set, used to train the quadratic classifier (i.e., based on Quadratic Discriminant Analysis, QDA); and test set, used to evaluate the performance of the protection method. In order to generate unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set).

The task in *all* the scenarios and experiments described in the next sections is to automatically distinguish between real and fake fingerprints. Therefore, in all cases, results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; and the False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as HTER $=$ $(\text{FGR} + \text{FFR})/2$.

Table 1.3 Results obtained in the ATVS-FFp DB by the two biometric protection methods described in Sects. 1.5 and 1.6

	Results: ATVS-FFp DB								
	Biometrika			Precise			Yubee		
	FFR	FGR	HTER	FFR	FGR	HTER	FFR	FGR	HTER
IQF-based	4.9	7.6	5.8	1.8	7.0	4.4	2.2	9.7	5.9
IQA-based	9.2	4.0	6.6	6.8	1.5	4.2	7.9	1.9	4.9

1.7.1 Results: ATVS-FFp DB

Both the development and the test set of the ATVS-FFp DB contain half of the fingerprint images acquired with and without the cooperation of the user, following a twofold cross validation protocol. In Table 1.3, we show the detection results of the two systems described in Sects. 1.5 (top row) and 1.6 (bottom row).

The performance of both algorithms is similar, although in the overall, the method based on general image quality assessment is slightly better in two of the three datasets (Precise and Yubee). In addition, thanks to its simplicity and lack of image preprocessing steps, the IQA-based method is around 30 times faster than the one using fingerprint-specific quality features (tested on the same Windows-based platform). This gives the IQA-based scheme the advantage of being usable in practical real-time applications, without losing any accuracy.

1.7.2 Results: LivDet 2009 DB

The train and test sets selected for the evaluation experiments on this database are the same as the ones used in the LivDet 2009 competition, so that the results obtained by the two described methods based on quality assessment may be directly compared to the participants of the contest. Results are shown in the first two rows of Table 1.4. For comparison, the best results achieved in LivDet 2009 for each of the individual datasets are given in the third row.

Rows four to seven show post-competition results over the same dataset and protocol. In [55], a novel fingerprint liveness detection method combining perspiration and morphological features was presented and evaluated on the LivDet 2009 DB following the same protocol (training and test sets) used in the competition. In that work, comparative results were reported with particular implementations of the techniques proposed in: [66], based on wavelet analysis; [69], based on curvelet analysis; and [53], based on the combination of local ridge frequencies and multiresolution texture analysis. In the last four rows of Table 1.4, we also present those results so that they can be compared with the two quality-based methods described in Sects. 1.5 (first row) and 1.6 (second row).

Table 1.4 Results obtained in the LivDet 2009 DB by: the two biometric protection methods described in Sects. 1.5 and 1.6 (IQF-based and IQA-based, top two rows); each of the best approaches participating in LivDet 2009 [21] (third row); the method proposed in [55] which combines perspiration and morphological features (fourth row); the method proposed in [66] based on wavelet analysis, according to an implementation from [55] (fifth row); the method proposed in [69] based on curvelet analysis, according to an implementation from [55] (sixth row); and the method proposed in [53] based on the combination of local ridge frequencies and multiresolution texture analysis, according to an implementation from [55] (bottom row)

	Results: LivDet 2009 DB								
	Biometrika			CrossMatch			Identix		
	FFR	FGR	HTER	FFR	FGR	HTER	FFR	FGR	HTER
IQF-based	3.1	71.8	37.4	8.8	20.8	13.2	4.8	5.0	6.7
IQA-based	14.0	11.6	12.8	8.6	12.8	10.7	1.1	1.4	1.2
LivDet 2009	15.6	20.7	18.2	7.4	11.4	9.4	2.7	2.8	2.8
Marasco et al.	12.2	13.0	12.6	17.4	12.9	15.2	8.3	11.0	9.7
Moon et al.	20.8	25.0	23.0	27.4	19.6	23.5	74.7	1.6	38.2
Nikam et al.	14.3	42.3	28.3	19.0	18.4	18.7	23.7	37.0	30.3
Abhyankar et al.	24.2	39.2	31.7	39.7	23.3	31.5	48.4	46.0	47.2

The results given in Table 1.4 show that the method based on general image quality assessment outperforms all the contestants in LivDet 2009 in two of the datasets (Biometrika and Identix), while its classification error is just slightly worse than the best of the participants for the Crossmatch data. Although the results are not as good for the case of the IQF-based method, its performance is still competitive compared to that of the best LivDet 2009 participants.

The classification rates of the two quality-based approaches are also clearly lower than those reported in [55] for the different liveness detection solutions tested.

1.8 Conclusions

The study of the vulnerabilities of biometric systems against presentation attacks has been a very active field of research in recent years [36, 37, 135]. This interest has led to big advances in the field of security-enhancing technologies for fingerprint-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats (usually based on some type of self-manufactured gummy finger) has proven to be a challenging task.

Simple visual inspection of an image of a real fingerprint and its corresponding fake sample shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that fingerprints, as 3-D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (silicone, gelatin, glycerin) or synthetically produced samples do not possess. Furthermore, fingerprint acquisition devices are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3-D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact, the characteristics of the captured image may significantly vary.

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this "*quality difference*" hypothesis, in this chapter, after an overview of early works and main research lines in fingerprint PAD methods, we have explored the potential of quality assessment as a protection tool against fingerprint direct attacks.

For this purpose, we have considered two different feature sets which we have combined with simple classifiers to detect real and fake access attempts: (i) a set of 10 fingerprint-specific quality measures which requires of some preprocessing steps (e.g., fingerprint segmentation); (ii) a set of 25 complementary general image quality measures which may be computed without any image preprocessing.

The two PAD methods have been evaluated on two large publicly available databases following their associated protocols. This way, the results are reproducible and may be fairly compared with other past or future fingerprint PAD solutions.

Several conclusions can be extracted from the evaluation results presented in the experimental sections of the chapter: (i) The proposed methods, especially the one based on general image quality assessment, are able to generalize well performing consistently well for different databases, acquisition conditions, and spoofing scenarios. (ii) The error rates achieved by the described protection schemes are in many cases lower than those reported by other related fingerprint PAD systems which have been tested in the framework of different independent competitions. (iii) In addition to its very competitive performance, the IQA-based approach presents some other very attractive features such as: its simple, fast, nonintrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.

All the previous results validate the "different-quality" hypothesis formulated in Sect. 1.4, and show the great potential of quality assessment as a PAD tool to secure fingerprint recognition systems.

Overall, the chapter has tried to give an introduction to fingerprint PAD, including an overview of early works, main research lines, and selected results. For more recent and advanced developments occurred in the last 5 years we refer the reader to [36, 37]. In addition, the experimental evaluation carried out in the chapter has been performed following a clear and standard methodology [33] based on common protocols, metrics, and benchmarks, which may serve as a good baseline starting point for the validation of future fingerprint PAD methods.

Acknowledgements This work was done in the context of the TABULA RASA and BEAT projects funded under the 7th Framework Programme of EU. This work was supported by project Cogni-Metrics from MINECO/FEDER under Grant TEC2015-70627-R, and the COST Action CA16101 (Multi-Foresee).

References

1. van der Putte T, Keuning J (2000) Biometrical fingerprint recognition: don't get your fingers burned. In: Proceedings of the IFIP conference on smart card research and advanced applications, pp 289–303
2. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial gummy fingers on fingerprint systems. In: Proceedings of the SPIE optical security and counterfeit deterrence techniques IV, vol 4677, pp 275–289
3. Thalheim L, Krissler J (2002) Body check: biometric access protection devices and their programs put to the test. ct magazine, pp 114–121
4. Sousedik C, Busch C (2014) Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biom 3(14):219–233. http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2013.0020
5. Derakhshani R, Schuckers S, Hornak L, O'Gorman L (2003) Determination of vitality from non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognit 36:383–396
6. Antonelli A, Capelli R, Maio D, Maltoni D (2006) Fake finger detection by skin distortion analysis. IEEE Trans Inf Forensics Secur 1:360–373
7. Galbally J, Alonso-Fernandez F, Fierrez J, Ortega-Garcia J (2012) A high performance fingerprint liveness detection method based on quality related features. Future Gener Comput Syst 28:311–321
8. Franco A, Maltoni D (2008) Advances in biometrics: sensors, algorithms and systems, chap. fingerprint synthesis and spoof detection. Springer, Berlin, pp 385–406
9. Li SZ (ed) (2009) Encyclopedia of biometrics. Springer, Berlin
10. Coli P (2008) Vitality detection in personal authentication systems using fingerprints. PhD thesis, Universita di Cagliari
11. Sandstrom M (2004) Liveness detection in fingerprint recognition systems. Master's thesis, Linkoping University
12. Lane M, Lordan L (2005) Practical techniques for defeating biometric devices. Master's thesis, Dublin City University
13. Blomme J (2003) Evaluation of biometric security systems against artificial fingers. Master's thesis, Linkoping University
14. Lapsley P, Less J, Pare D, Hoffman N (1998) Anti-fraud biometric sensor that accurately detects blood flow
15. Setlak DR (1999) Fingerprint sensor having spoof reduction features and related methods
16. Kallo I, Kiss A, Podmaniczky JT (2001) Detector for recognizing the living character of a finger in a fingerprint recognizing apparatus
17. Diaz-Santana E, Parziale G (2008) Liveness detection method
18. Kim J, Choi H, Lee W (2011) Spoof detection method for touchless fingerprint acquisition apparatus
19. Centro Criptologico Nacional (CCN) (2011) Characterizing attacks to fingerprint verification mechanisms CAFVM v3.0. Common Criteria Portal
20. Bundesamt fur Sicherheit in der Informationstechnik (BSI) (2008) Fingerprint spoof detection protection profile FSDPP v1.8. Common Criteria Portal
21. Marcialis GL, Lewicke A, Tan B, Coli P, Grimberg D, Congiu A, Tidu A, Roli F, Schuckers S (2009) First international fingerprint liveness detection competition – livdet 2009. In: Proceedings of the IAPR international conference on image analysis and processing (ICIAP). LNCS, vol 5716, pp 12–23
22. Ghiani L, Yambay DA, Mura V, Marcialis GL, Roli F, Schuckers SA (2017) Review of the fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. Image Vis Comput 58:110–128
23. Galbally J, Fierrez J, Alonso-Fernandez F, Martinez-Diaz M (2011) Evaluation of direct attacks to fingerprint verification systems. J Telecommun Syst Special Issue Biom Syst Appl 47:243–254

24. Abhyankar A, Schuckers S (2009) Integrating a wavelet based perspiration liveness check with fingerprint recognition. Pattern Recognit 42:452–464
25. Biometrics Institute: Biometric Vulnerability Assessment Expert Group (2011). http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group-bvaeg.html
26. NPL: National Physical Laboratory: Biometrics (2010). http://www.npl.co.uk/biometrics
27. CESG: Communications-Electronics Security Group - Biometric Working Group (BWG) (2001). https://www.cesg.gov.uk/policyguidance/biometrics/Pages/index.aspx
28. BEAT: Biometrics Evaluation and Testing (2016). http://www.beat-eu.org/
29. TABULA RASA: Trusted biometrics under spoofing attacks (2014). http://www.tabularasa-euproject.org/
30. Maltoni D, Maio D, Jain A, Prabhakar S (2009) Handbook of fingerprint recognition. Springer, Berlin
31. Cappelli R, Maio D, Lumini A, Maltoni D (2007) Fingerprint image reconstruction from standard templates. IEEE Trans Pattern Anal Mach Intell 29:1489–1503
32. Cappelli R (2009) Handbook of fingerprint recognition, chapter, synthetic fingerprint generation. Springer, Berlin, pp 270–302
33. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag 32(5):20–30
34. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. IEEE Trans on Image Process 23(2):710–724
35. Sousedik C, Busch C (2014) Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics 3(4):219–233
36. Marasco E, Ross A (2015) A survey on anti-spoofing schemes for fingerprint recognition systems. ACM Comput Surv 47(2):1–36
37. Pinto A, Pedrini H, Krumdick M, Becker B, Czajka A, Bowyer KW, Rocha A (2018) Counteracting presentation attacks in face, fingerprint, and iris recognition. In: Vatsa M, Singh R, Majumdar A (eds) Deep learning in biometrics. CRC Press
38. Wehde A, Beffel JN (1924) Fingerprints can be forged. Tremonia Publish Co, Chicago
39. de Water MV (1936) Can fingerprints be forged? Sci News-Lett 29:90–92
40. Sengottuvelan P, Wahi A (2007) Analysis of living and dead finger impressions identification for biometric applications. In: Proceedings of the international conference on computational intelligence and multimedia applications
41. Yoon S, Feng J, Jain AK (2012) Altered fingerprints: analysis and detection. IEEE Trans Pattern Anal Mach Intell 34:451–464
42. Willis D, Lee M (1998) Biometrics under our thumb. Netw Comput http://www.networkcomputing.com/
43. Sten A, Kaseva A, Virtanen T (2003) Fooling fingerprint scanners - biometric vulnerabilities of the precise biometrics 100 SC scanner. In: Proceedings of the australian information warfare and IT security conference
44. Wiehe A, Sondrol T, Olsen K, Skarderud F (2004) Attacking fingerprint sensors. Technical report NISlab, Gjovik University College
45. Galbally J, Cappelli R, Lumini A, de Rivera GG, Maltoni D, Fierrez J, Ortega-Garcia J, Maio D (2010) An evaluation of direct and indirect attacks using fake fingers generated from ISO templates. Pattern Recognit Lett 31:725–732
46. Barral C, Tria A (2009) Fake fingers in fingerprint recognition: glycerin supersedes gelatin. In: Formal to Practical Security. LNCS, vol 5458, pp 57–69
47. Parthasaradhi S, Derakhshani R, Hornak L, Schuckers S (2005) Time-series detection of perspiration as a liveness test in fingerprint devices. IEEE Trans Syst Man Cybern - Part C: Appl Rev 35:335–343
48. Schuckers S, Abhyankar A (2004) A wavelet based approach to detecting liveness in fingerprint scanners. In: Proceeding of the biometric authentication workshop (BioAW). LNCS, vol 5404. Springer, Berlin, pp 278–386

49. Tan B, Schuckers S (2006) Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. In: Proceeding of the SPIE biometric technology for human identification III (BTHI III), vol 6202, p 62020A
50. Tan B, Schuckers S (2009) A new approach for liveness detection in fingerprint scanners based on valley noise analysis. J Electron Imaging 17:011,009
51. DeCann B, Tan B, Schuckers S (2009) A novel region based liveness detection approach for fingerprint scanners. In: Proceeding of the IAPR/IEEE international conference on biometrics. LNCS, vol 5558. Springer, Berlin, pp 627–636
52. NexIDBiometrics: (2012). http://nexidbiometrics.com/
53. Abhyankar A, Schuckers S (2006) Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In: Proceedings of the IEEE international conference on image processing (ICIP)
54. Marasco E, Sansone C (2010) An anti-spoofing technique using multiple textural features in fingerprint scanners. In: Proceeding of the IEEE workshop on biometric measurements and systems for security and medical applications (BIOMS), pp 8–14
55. Marasco E, Sansone C (2012) Combining perspiration- and morphology-based static features for fingerprint liveness detection. Pattern Recognit Lett 33:1148–1156
56. Cappelli R, Maio D, Maltoni D (2001) Modelling plastic distortion in fingerprint images. In: Proceedings of the international conference on advances in pattern recognition (ICAPR). LNCS, vol 2013. Springer, Berlin, pp 369–376
57. Bazen AM, Gerez SH (2003) Fingerprint matching by thin-plate spline modelling of elastic deformations. Pattern Recognit 36:1859–1867
58. Chen Y, Dass S, Ross A, Jain AK (2005) Fingerprint deformation models using minutiae locations and orientations. In: Proceeding of the IEEE workshop on applications of computer vision (WACV), pp 150–156
59. Chen Y, Jain AK (2005) Fingerprint deformation for spoof detection. In: Proceeding of the IEEE biometric symposium (BSym), pp 19–21
60. Zhang Y, Tian J, Chen X, Yang X, Shi P (2007) Fake finger detection based on thin-plate spline distortion model. In: Proceeding of the IAPR international conference on biometrics. LNCS, vol 4642. Springer, Berlin, pp 742–749
61. Yau WY, Tran HT, Teoh EK, Wang JG (2007) Fake finger detection by finger color change analysis. In: Proceedings of the international conference on biometrics (ICB). LNCS, vol 4642. Springer, Berlin, pp 888–896
62. Jia J, Cai L (2007) Fake finger detection based on time-series fingerprint image analysis. In: Proceedings of the IEEE international conference on intelligent computing (ICIC). LNCS, vol 4681. Springer, Berlin, pp 1140–1150
63. Marcialis GL, Roli F, Tidu A (2010) Analysis of fingerprint pores for vitality detection. In: Proceedings of the IEEE international conference on pattern recognition (ICPR), pp 1289–1292
64. Memon S, Manivannan N, Balachandran W (2011) Active pore detection for liveness in fingerprint identification system. In: Proceeding of the IEEE Telecommuncations Forum (TelFor), pp 619–622
65. Martinsen OG, Clausen S, Nysather JB, Grimmes S (2007) Utilizing characteristic electrical properties of the epidermal skin layers to detect fake fingers in biometric fingerprint systems-a pilot study. IEEE Trans Biomed Eng 54:891–894
66. Moon YS, Chen JS, Chan KC, So K, Woo KC (2005) Wavelet based fingerprint liveness detection. Electron Lett 41
67. Nikam SB, Agarwal S (2009) Feature fusion using gabor filters and cooccrrence probabilities for fingerprint antispoofing. Int J Intell Syst Technol Appl 7:296–315
68. Nikam SB, Argawal S (2009) Ridgelet-based fake fingerprint detection. Neurocomputing 72:2491–2506
69. Nikam S, Argawal S (2010) Curvelet-based fingerprint anti-spoofing. Signal Image Video Process 4:75–87

70. Coli P, Marcialis GL, Roli F (2007) Power spectrum-based fingerprint vitality detection. In: Proceedings of the IEEE workshop on automatic identification advanced technologies (AutoID), pp 169–173
71. Jin C, Kim, H, Elliott S (2007) Liveness detection of fingerprint based on band-selective Fourier spectrum. In: Proceedings of the international conference on information security and cryptology (ICISC). LNCS, vol 4817. Springer, Berlin, pp 168–179
72. Jin S, Bae Y, Maeng H, Lee H (2010) Fake fingerprint detection based on image analysis. In: Proceedings of the SPIE, Sensors, cameras, and systems for industrial/scientific applications XI, vol 7536, p 75360C
73. Lee H, Maeng H, Bae Y (2009) Fake finger detection using the fractional Fourier transform. In: Proceedings of the biometric ID management and multimodal communication (BioID). LNCS, vol 5707. Springer, Berlin, pp 318–324
74. Marcialis GL, Coli P, Roli F (2012) Fingerprint liveness detection based on fake finger characteristics. Int J Digit Crime Forensics 4
75. Coli P, Marcialis GL, Roli F (2007) Vitality detection from fingerprint images: a critical survey. In: Proceedings of the international conference on biometrics (ICB). LNCS, vol 4642. Springer, Berlin, pp 722–731
76. Coli P, Marcialis GL, Roli F (2008) Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device. Int J Image Graph, pp 495–512
77. Marcialis GL, Coli P, Roli F (2012) Fingerprint liveness detection based on fake finger characteristics. Int J Digit Crime Forensics 4:1–19
78. Choi H, Kang R, Choi K, Jin ATB, Kim J (2009) Fake-fingerprint detection using multiple static features. Optic Eng 48:047, 202
79. Nixon KA, Rowe RK (2005) Multispectral fingerprint imaging for spoof detection. In: Proceedings of the SPIE, biometric technology for human identification II (BTHI), vol 5779, pp 214–225
80. Rowe RK, Nixon KA, Butler PW (2008) Advances in biometrics: Sensors, algorithms and systems, Chapter, multispectral fingerprint image acquisition. Springer, Berlin, pp 3–23
81. Yau WY, Tran HL, Teoh EK (2008) Fake finger detection using an electrotactile display system. In: Proceedings of the international conference on control, automation, robotics and vision (ICARCV), pp 17–20
82. Reddy PV, Kumar A, Rahman SM, Mundra TS (2008) A new antispoofing approach for biometric devices. IEEE Trans Biomed Circuits Syst 2:328–337
83. Baldiserra D, Franco A, Maio D, Maltoni D (2006) Fake fingerprint detection by odor analysis. In: Proceedings of the IAPR international conference on biometrics (ICB). LNCS, vol 3832. Springer, Berlin, pp 265–272
84. Cheng Y, Larin KV (2006) Artificial fingerprint recognition using optical coherence tomography with autocorrelation analysis. Appl Opt 45:9238–9245
85. Manapuram RK, Ghosn M, Larin KV (2006) Identification of artificial fingerprints using optical coherence tomography technique. Asian J Phys 15:15–27
86. Cheng Y, Larin KV (2007) In vivo two- and three-dimensional imaging of artificial and real fingerprints with optical coherence tomography. IEEE Photonics Technol Lett 19:1634–1636
87. Larin KV, Cheng Y (2008) Three-dimensional imaging of artificial fingerprint by optical coherence tomography. In: Proceedings of the SPIE biometric technology for human identification (BTHI), vol 6944, p 69440M
88. Chang S, Larin KV, Mao Y, Almuhtadi W, Flueraru C (2011) State of the art in biometrics, chap. fingerprint spoof detection using near infrared optical analysis, Intechopen, pp 57–84
89. Nasiri-Avanaki MR, Meadway A, Bradu A, Khoshki RM, Hojjatoleslami A, Podoleanu AG (2011) Anti-spoof reliable biometry of fingerprints using en-face optical coherence tomography. Opt Photonics J 1:91–96
90. Rattani A, Poh N, Ross A (2012) Analysis of user-specific score characteristics for spoof biometric attacks. In: Proceedings of the IEEE computer society workshop on biometrics at the international conference on computer vision and pattern recognition (CVPR), pp 124–129

91. Marasco E, Ding Y, Ross A (2012) Combining match scores with liveness values in a fingerprint verification system. In: Proceedings of the IEEE international conference on biometrics: theory, applications and systems (BTAS), pp 418–425
92. Hariri M, Shokouhi SB (2011) Possibility of spoof attack against robustness of multibiometric authentication systems. SPIE J Opt Eng 50:079, 001
93. Akhtar Z, Fumera G, Marcialis GL, Roli F (2011) Robustness analysis of likelihood ratio score fusion rule for multi-modal biometric systems under spoof attacks. In: Proceedings of the IEEE international carnahan conference on security technology (ICSST), pp 237–244
94. Akhtar Z, Fumera G, Marcialis GL, Roli F (2012) Evaluation of serial and parallel multi-biometric systems under spoofing attacks. In: Proceedings of the international conference on biometrics: theory, applications and systems (BTAS)
95. Ultra-Scan: (2012). http://www.ultra-scan.com/
96. Optel: (2012). http://www.optel.pl/
97. PosID: (2012). http://www.posid.co.uk/
98. VirdiTech: (2012). http://www.virditech.com/
99. Kang H, Lee B, Kim H, Shin D, Kim J (2003) A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In: Proceedings of the international conference on knowledge-based intelligent information and engineering systems (KES). LNAI, vol 2774. Springer, Berlin, pp 1245–1253
100. Wang L, El-Maksoud RA, Sasian JM, William Kuhn P, Gee K, 2009, V.S.V (2009) A novel contactless aliveness-testing fingerprint sensor. In: Proceedings of the SPIE novel optical systems design and optimization XII, vol 7429, pp 742–915
101. Bayram S, Avcibas I, Sankur B, Memon N (2006) Image manipulation detection. J Electron Imaging 15:041,102
102. Stamm MC, Liu KJR (2010) Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Trans Inf Forensics Secur 5:492–496
103. Avcibas I, Memon N, Sankur B (2003) Steganalysis using image quality metrics. IEEE Trans Image Process 12:221–229
104. Avcibas I, Kharrazi M, Memon N, Sankur B (2005) Image steganalysis with binary similarity measures. EURASIP J Appl Signal Process 1:2749–2757
105. Lyu S, Farid H (2006) Steganalysis using higher-order image statistics. IEEE Trans Inf Forensics Secur 1:111–119
106. Lim E, Jiang X, Yau W (2002) Fingerprint quality and validity analysis. In: Proceeding of the IEEE international conference on image processing (ICIP), vol 1, pp 469–472
107. Chen Y, Dass S, Jain A (2005) Fingerprint quality indices for predicting authentication performance. In: Proceedings of the IAPR audio- and video-based biometric person authentication (AVBPA). LNCS, vol 3546. Springer, Berlin, pp 160–170
108. Chen T, Jiang X, Yau W (2004) Fingerprint image quality analysis. In: Proceeding of the IEEE international conference on image processing (ICIP), vol 2, pp 1253–1256
109. Hong L, Wan Y, Jain AK (1998) Fingerprint image enhancement: algorithm and performance evaluation. IEEE Trans Pattern Anal Mach Intell 20(8):777–789
110. Alonso-Fernandez F, Fierrez J, Ortega-Garcia J, Gonzalez-Rodriguez J, Fronthaler H, Kollreider K, Bigun, J (2008) A comparative study of fingerprint image quality estimation methods. IEEE Trans Inf Forensics Secur 2(4):734–743
111. Bigun J (2006) Vision with direction. Springer, Berlin
112. Shen L, Kot A, Koo W (2001) Quality measures of fingerprint images. In: Proceedings of the IAPR audio- and video-based biometric person authentication (AVBPA). LNCS, vol 2091. Springer, Berlin, pp 266–271
113. Wong PW, Pappas TN, Safranek RJ, Chen J, Wang Z, Bovik AC, Simoncelli EP, Sheikh HR (2005) Handbook of image and video processing, Chapter, Sect. VIII: image and video rendering and assessment. Academic Press, New York, pp 925–989
114. Sheikh HRS, Sabir MF, Bovik AC (2006) A statistical evaluation of recent full reference image quality assessment algorithms. IEEE Trans Image Process 15:3440–3451

115. Saad MA, Bovik AC, Charrier C (2012) Blind image quality assessment: a natural scene statatistics approach in the DCT domain. IEEE Trans Image Process 21:3339–3352
116. Wang Z, Bovik AC (2009) Mean squared error: love it or leave it? IEEE Signal Process Mag 26:98–117
117. Teo PC, Heeger DJ (1994) Perceptual image distortion. In: Proceedings of the international conference on image processing, pp 982–986
118. Avcibas I, Sankur B, Sayood K (2002) Statistical evaluation of image quality measures. J Electron Imaging 11:206–223
119. Huynh-Thu Q, Ghanbari M (2008) Scope of validity of PSNR in image/video quality assessment. Electron Lett 44:800–801
120. Yao S, Lin W, Ong E, Lu Z (2005) Contrast signal-to-noise ratio for image quality assessment. In: Proceedings of the international conference on image processing (ICIP), pp 397–400
121. Eskicioglu AM, Fisher PS (1995) Image quality measures and their performance. IEEE Trans Commun 43:2959–2965
122. Martini MG, Hewage CT, Villarini B (2012) Image quality assessment based on edge preservation. Signal Process Image Commun 27:875–882
123. Nill NB, Bouzas B (1992) Objective image quality measure derived from digital image power spectra. Opt Eng 31:813–825
124. Liu A, Lin W, Narwaria M (2012) Image quality assessment based on gradient similarity. IEEE Trans Image Process 21:1500–1511
125. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13:600–612
126. LIVE: (2012). http://live.ece.utexas.edu/research/Quality/index.htm
127. Sheikh HR, Bovik AC (2006) Image information and visual quality. IEEE Trans Image Process 15:430–444
128. Soundararajan R, Bovik AC (2012) RRED indices: reduced reference entropic differencing for image quality assessment. IEEE Trans Image Process 21:517–526
129. Wang Z, Sheikh HR, Bovik AC (2002) No-reference perceptual quality assessment of JPEG compressed images. In: Proceedings of the IEEE international conference on image processing (ICIP), pp 477–480
130. Zhu X, Milanfar P (2009) A no-reference sharpness metric sensitive to blur and noise. In: Proceedings of the international workshop on quality of multimedia experience (QoMEx), pp 64–69
131. Moorthy AK, Bovik AC (2010) A two-step framework for constructing blind image quality indices. IEEE Signal Process Lett 17:513–516
132. Mittal A, Soundararajan R, Bovik AC (2012) Making a completely blind image quality analyzer. IEEE Signal Process Lett. https://doi.org/10.1109/LSP.2012.2227726
133. Harris C, Stephens M (1988) A combined corner and edge detector. In: Proceeding of the alvey vision conference (AVC), pp 147–151
134. Brunet D, Vrscay ER, Wang Z (2012) On the mathematical properties of the structural similarity index. IEEE Trans Image Process 21:1488–1499
135. Nixon KA, Aimale V, Rowe RK (2008) Handbook of biometrics, Chapter, Spoof detection schemes. Springer, Berlin, pp 403–423