Chapter 15
Introduction to Voice Presentation Attack Detection and Recent Advances

Md Sahidullah, Héctor Delgado, Massimiliano Todisco, Tomi Kinnunen, Nicholas Evans, Junichi Yamagishi and Kong-Aik Lee

Abstract Over the past few years, significant progress has been made in the field of presentation attack detection (PAD) for automatic speaker recognition (ASV). This includes the development of new speech corpora, standard evaluation protocols and advancements in front-end feature extraction and back-end classifiers. The use of standard databases and evaluation protocols has enabled for the first time the meaningful benchmarking of different PAD solutions. This chapter summarises the progress, with a focus on studies completed in the last 3 years. The article presents a summary of findings and lessons learned from two ASVspoof challenges, the first community-led benchmarking efforts. These show that ASV PAD remains an unsolved problem and that further attention is required to develop generalised PAD solutions which have potential to detect diverse and previously unseen spoofing attacks.

M. Sahidullah (✉) · T. Kinnunen
School of Computing, University of Eastern Finland, Kuopio, Finland
e-mail: sahid@cs.uef.fi

T. Kinnunen
e-mail: tkinnu@cs.uef.fi

H. Delgado · M. Todisco · N. Evans
Department of Digital Security, EURECOM, Biot Sophia Antipolis, France
e-mail: hector.delgado@eurecom.fr

M. Todisco
e-mail: massimiliano.todisco@eurecom.fr

N. Evans
e-mail: evans@eurecom.fr

J. Yamagishi
National Institute of Informatics, Tokyo, Japan
e-mail: jyamagis@nii.ac.jp

J. Yamagishi
University of Edinburgh, Edinburgh, Scotland

K.-A. Lee
Data Science Research Laboratories, NEC Corporation (Japan), Tokyo, Japan
e-mail: k-lee@ax.jp.nec.com

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_15

15.1 Introduction

Automatic speaker verification (ASV) technology aims to recognise individuals using samples of the human voice signal [1, 2]. Most ASV systems operate on estimates of the spectral characteristics of voice in order to recognise individual speakers. ASV technology has matured in recent years and now finds application in a growing variety of real-world authentication scenarios involving both *logical* and *physical* access. In logical access scenarios, ASV technology can be used for remote person authentication via the Internet or traditional telephony. In many cases, ASV serves as a convenient and efficient alternative to more conventional password-based solutions, one prevalent example being person authentication for Internet and mobile banking. Physical access scenarios include the use of ASV to protect personal or secure/sensitive facilities, such as domestic and office environments. With the growing, widespread adoption of smartphones and voice-enabled smart devices, such as intelligent personal assistants all equipped with at least one microphone, ASV technology stands to become even more ubiquitous in the future.

Despite its appeal, the now-well-recognised vulnerability to manipulation through presentation attacks (PAs), also known as spoofing, has dented confidence in ASV technology. As identified in ISO/IEC 30107-1 standard [3], the possible locations of presentation attack points in a typical ASV system are illustrated in Fig. 15.1. Two of the most vulnerable places in an ASV system are marked by 1 and 2, corresponding to physical access and logical access. This work is related to these two types of attacks.

Unfortunately, ASV is arguably more prone to PAs than other biometric systems based on traits or characteristics that are less easily acquired; samples of a given person's voice can be collected readily by fraudsters through face-to-face or telephone conversations and then replayed in order to manipulate an ASV system. Replay attacks are furthermore only one example of ASV PAs. More advanced voice

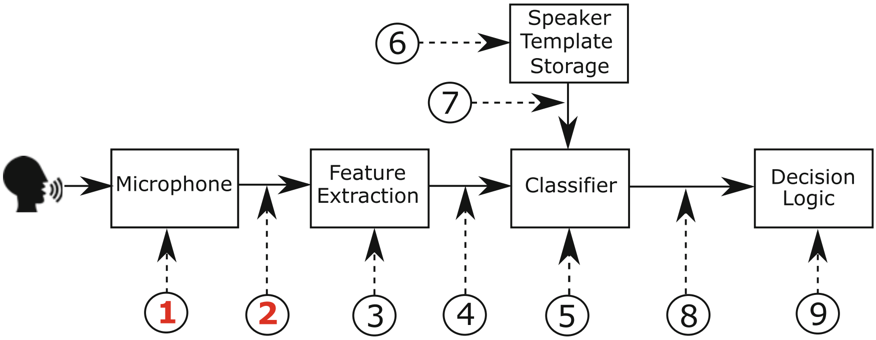

Fig. 15.1 Possible attack locations in a typical ASV system. 1: microphone point, 2: transmission point, 3: override feature extractor, 4: modify probe to features, 5: override classifier, 6: modify speaker database, 7: modify biometric reference, 8: modify score and 9: override decision

conversion or speech synthesis algorithms can be used to generate particularly effective PAs using only modest amounts of voice data collected from a target person.

There are a number of ways to prevent PA problems. The first one is based on a text-prompted system which uses an utterance verification process [4]. The user needs to utter a specific text prompted for authentication by the system which requires a text-verification system. Second, as human can never reproduce an identical speech signal, some countermeasures use template matching or audio fingerprinting to verify whether the speech utterance was presented to the system earlier [5]. Third, some work looks into statistical acoustic characterisation of authentic speech and speech created with presentation attack methods or spoofing techniques [6]. Our focus is on the last category, which is more convenient in a practical scenario for both text-dependent and text-independent ASV. In this case, given a speech signal, S, PA detection here, the determination of whether S is a natural or PA speech can be formulated as a hypothesis test:

- H_0: S is natural speech.
- H_1: S is created with PA methods.

A likelihood ratio test can be applied to decide between H_0 and H_1. Suppose that $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_N\}$ are the acoustic feature vectors of N speech frames extracted from S, then the logarithmic likelihood ratio score is given by

$$\Lambda(\mathbf{X}) = \log p(\mathbf{X}|\lambda_{H_0}) - \log p(\mathbf{X}|\lambda_{H_1}) \tag{15.1}$$

In (15.1), λ_{H_0} and λ_{H_1} are the acoustic models to characterise the hypotheses correspondingly for natural speech and PA speech. The parameters of these models are estimated using training data for natural and PA speech. A typical PAD system is shown in Fig. 15.2. A test speech can be accepted as natural or rejected as PA speech with help of a threshold, θ computed on some development data. If the score is greater than or equal to the threshold, it is accepted; otherwise, rejected. The performance of the PA system is assessed by computing the *Equal Error Rate* (EER) metric. This is the error rate for a specific value of a threshold where two error rates, i.e. the probability of a PA speech detected as being natural speech (known as false acceptance rate or FAR) and the probability of a natural speech being misclassified as a PA speech (known as false rejection rate or FRR), are equal. Sometimes *Half Total Error Rate* (HTER) is also computed [7]. This is the average of FAR and FRR which are computed using a decision threshold obtained with the help of the development data.

Awareness and acceptance of the vulnerability to PAs have generated a growing interest in developing solutions to presentation attack detection (PAD), also referred to as spoofing countermeasures. These are typically dedicated auxiliary systems which function in tandem to ASV in order to detect and deflect PAs. The research in this direction has progressed rapidly in the last three years, due partly to the release of several public speech corpora and the organisation of PAD challenges for ASV. This article, a continuation of the chapter [8] in the first edition of the

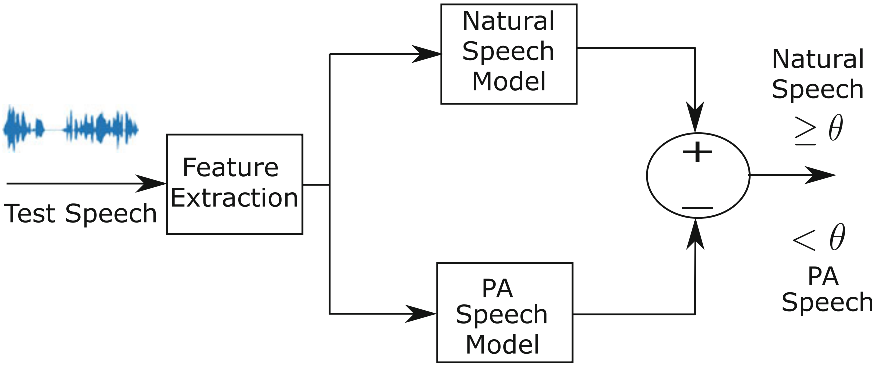

Fig. 15.2 Block diagram of a typical presentation attack detection system

Handbook for Biometrics [9] presents an up-to-date review of the different forms of voice presentation attacks, broadly classified in terms of impersonation, replay, speech synthesis and voice conversion. The primary focus is nonetheless on the progress in PAD. The chapter reviews the most recent work involving a variety of different features and classifiers. Most of the work covered in the chapter relates to that conducted using the two most popular and publicly available databases, which were used for the two ASVspoof challenges co-organised by the authors. The chapter concludes with a discussion of research challenges and future directions in PAD for ASV.

15.2 Basics of ASV Spoofing and Countermeasures

Spoofing or presentation attacks are performed on a biometric system at the sensor or acquisition level to bias score distributions towards those of genuine clients, thus provoking increases in the false acceptance rate (FAR). This section reviews four well-known ASV spoofing techniques and their respective countermeasures: impersonation, replay, speech synthesis and voice conversion. Here, we mostly review the work in the pre-ASVspoof period, as well as some very recent studies on presentation attacks.

15.2.1 Impersonation

In speech impersonation or mimicry attacks, an intruder speaker intentionally modifies his or her speech to sound like the target speaker. Impersonators are likely to copy lexical, prosodic and idiosyncratic behaviour of their target speakers presenting a potential point of vulnerability concerning speaker recognition systems.

15.2.1.1 Spoofing

There are several studies about the consequences of mimicry on ASV. Some studies concern attention to the voice modifications performed by professional impersonators. It has been reported that impersonators are often particularly able to adapt the fundamental frequency (F0) and occasionally also the formant frequencies towards those of the target speakers [10–12]. In studies, the focus has been on analysing the vulnerability of speaker verification systems in the presence of voice mimicry. The studies by Lau et al. [13, 14] suggest that if the target of impersonation is known in advance and his or her voice is "similar" to the impersonator's voice (in the sense of automatic speaker recognition score), then the chance of spoofing an automatic recognizer is increased. In [15], the experiments indicated that professional impersonators are potentially better impostors than amateur or naive ones. Nevertheless, the voice impersonation was not able to spoof the ASV system. In [10], the authors attempted to quantify how much a speaker is able to approximate other speakers' voices by selecting a set of prosodic and voice source features. Their prosodic and acoustic-based ASV results showed that two professional impersonators imitating known politicians increased the identification error rates.

More recently, a fundamentally different study was carried out by Panjwani et al. [16] using crowdsourcing to recruit both amateur and more professional impersonators. The results showed that impersonators succeed in increasing their average score, but not in exceeding the target speaker score. All of the above studies analysed the effects of speech impersonation either at the acoustic or speaker recognition score level, but none proposed any countermeasures against impersonation. In a recent study [17], the experiments aimed to evaluate the vulnerability of three modern speaker verification systems against impersonation attacks and to further compare these results to the performance of non-expert human listeners. It is observed that, on average, the mimicry attacks lead to increased error rates. The increase in error rates depends on the impersonator and the ASV system.

The main challenge, however, is that no large speech corpora of impersonated speech exists for the quantitative study of impersonation effects on the same scale as for other attacks, such as text-to-speech synthesis and voice conversion, where generation of simulated spoofing attacks as well as developing appropriate countermeasures are more convenient.

15.2.1.2 Countermeasures

While the threat of impersonation is not fully understood due to limited studies involving small datasets, it is perhaps not surprising that there is no prior work investigating countermeasures against impersonation. If the threat is proven to be genuine, then the design of appropriate countermeasures might be challenging. Unlike the spoofing attacks discussed below, all of which can be assumed to leave traces of the physical properties of the recording and playback devices, or signal processing artefacts from synthesis or conversion systems, impersonators are live human beings who produce entirely natural speech.

15.2.2 Replay

Replay attacks refer to the use of pre-recorded speech from a target speaker, which is then replayed through some playback device to feed the system microphone. These attacks require no specific expertise nor sophisticated equipment, thus they are easy to implement. Replay is a relatively low-technology attack within the grasp of any potential attacker even without specialised knowledge in speech processing. Several works in the earlier literature report significant increases in error rates when using replayed speech. Even if replay attacks may present a genuine risk to ASV systems, the use of prompted-phrase has the potential to mitigate the impact.

15.2.2.1 Spoofing

The study on the impact of replay attack on ASV performance was very limited until recently before the release of AVspoof [18] and ASVspoof 2017 corpus. The earlier studies were conducted either on simulated or on real replay recording from far-field.

The vulnerability of ASV systems to replay attacks was first investigated in a text-dependent scenario [19], where the concatenation of recorded digits was tested against a hidden Markov model (HMM)-based ASV system. Results showed an increase in the FAR from 1 to 89% for male speakers and from 5 to 100% for female speakers.

The work in [20] investigated text-independent ASV vulnerabilities through the replaying of far-field recorded speech in a mobile telephony scenario where signals were transmitted by analogue and digital telephone channels. Using a baseline ASV system based on *joint factor analysis* (JFA), the work showed an increase in the EER of 1% to almost 70% when impostor accesses were replaced by replayed spoof attacks.

A physical access scenario was considered in [21]. While the baseline performance of the Gaussian mixture model-universal background model (GMM-UBM) ASV system was not reported, experiments showed that replay attacks produced a FAR of 93%.

The work in [18] introduced audio-visual spoofing (AVspoof) database for replay attack detection where the replayed signals are collected and played back using different low-quality (phones and laptop) and high-quality (laptop with loudspeakers) devices. The study reported that FARs for replayed speech was 77.4 and 69.4% for male and female, respectively, using a total variability system speaker recognition system. In this study, the EER for bona fide trials was 6.9 and 17.5% for those conditions. This study also includes presentation attack where speech signals created with voice conversion and speech synthesis were used in playback attack. In that case, higher FAR was observed, particularly when high-quality device is used for playback.

15.2.2.2 Countermeasures

A countermeasure for replay attack detection in the case of text-dependent ASV was reported in [5]. The approach is based upon the comparison of new access samples with stored instances of past accesses. New accesses which are deemed too similar to previous access attempts are identified as replay attacks. A large number of different experiments, all relating to a telephony scenario, showed that the countermeasures succeeded in lowering the EER in most of the experiments performed. While some form of text-dependent or challenge response countermeasure is usually used to prevent replay attacks, text-independent solutions have also been investigated. The same authors in [20] showed that it is possible to detect replay attacks by measuring the channel differences caused by far-field recording [22]. While they show spoof detection error rates of less than 10% it is feasible that today's state-of-the-art approaches to channel compensation will render some ASV systems still vulnerable.

Two different replay attack countermeasures are compared in [21]. Both are based on the detection of differences in channel characteristics expected between licit and spoofed access attempts. Replay attacks incur channel noise from both the recording device and the loudspeaker used for replay and thus the detection of channel effects beyond those introduced by the recording device of the ASV system thus serves as an indicator of replay. The performance of a baseline GMM-UBM system with an EER of 40% under spoofing attack falls to 29% with the first countermeasure and a more respectable EER of 10% with the second countermeasure.

In another study [23], a speech database of 175 subjects have been collected for different kinds of replay attack. Other than the use of genuine voice samples for the legitimate speakers in playback, the voice samples recorded over the telephone channel was also used for unauthorised access. Further, a far-field microphone is used to collect the voice samples as eavesdropped (covert) recording. The authors proposed an algorithm motivated from music recognition system used for comparing recordings on the basis of the similarity of the local configuration of maxima pairs extracted from spectrograms of verified and reference recordings. The experimental results show the EER of playback attack detection to be as low as 1.0% on the collected data.

15.2.3 Speech Synthesis

Speech synthesis, commonly referred to as text-to-speech (TTS), is a technique for generating intelligible, natural sounding artificial speech for any arbitrary text. Speech synthesis is used widely in various applications including in-car navigation systems, e-book readers, voice-over for the visually impaired and communication aids for the speech impaired. More recent applications include spoken dialogue systems, communicative robots, singing speech synthesisers and speech-to-speech translation systems.

Typical speech synthesis systems have two main components [24]: text analysis followed by speech waveform generation, which is sometimes referred to as the front-end and back-end, respectively. In the text analysis component, input text is converted into a linguistic specification consisting of elements such as phonemes. In the speech waveform generation component, speech waveforms are generated from the produced linguistic specification. There are emerging end-to-end frameworks that generate speech waveforms directly from text inputs without using any additional modules.

Many approaches have been investigated, but there have been major paradigm shifts every ten years. In the early 1970s, the speech waveform generation component used very low-dimensional acoustic parameters for each phoneme, such as formants, corresponding to vocal tract resonances with hand-crafted acoustic rules [25]. In the 1980s, the speech waveform generation component used a small database of phoneme units called *diphones* (the second half of one phoneme plus the first half of the following) and concatenated them according to the given phoneme sequence by applying signal processing such as linear predictive (LP) analysis, to the units [26]. In the 1990s, larger speech databases were collected and used to select more appropriate speech units that matched both phonemes and other linguistic contexts such as lexical stress and pitch accent in order to generate high-quality natural sounding synthetic speech with the appropriate prosody. This approach is generally referred to as *unit selection*, and is nowadays used in many speech synthesis systems [27–31].

In the late 2000s, several machine learning based data-driven approaches emerged. ‘Statistical parametric speech synthesis’ was one of the more popular machine learning approaches [32–35]. In this approach, several acoustic parameters are modelled using a time-series stochastic generative model, typically an HMM. HMMs represent not only the phoneme sequences but also various contexts of the linguistic specification. Acoustic parameters generated from HMMs and selected according to the linguistic specification are then used to drive a vocoder, a simplified speech production model in which speech is represented by vocal tract parameters and excitation parameters in order to generate a speech waveform. HMM-based speech synthesisers [36, 37] can also learn speech models from relatively small amounts of speaker-specific data by adapting background models derived from other speakers based on the standard model adaptation techniques drawn from speech recognition, i.e. maximum likelihood linear regression (MLLR) [38, 39].

In the 2010s, deep learning has significantly improved the performance of speech synthesis and led to a significant breakthrough. First, various types of deep neural networks are used to improve the prediction accuracy of the acoustic parameters [40, 41]. Investigated architectures include recurrent neural network [42–44], residual/highway network [45, 46], autoregressive network [47, 48] and generative adversarial networks (GAN) [49–51]. Furthermore, in the late 2010s, conventional waveform generation modules that typically used signal processing and text analysis modules that used natural language processing were substituted by neural networks. This allows for neural networks capable of directly outputting the desired speech waveform samples from the desired text inputs. Successful architectures for direct waveform modelling include dilated convolutional autoregressive neural network, known as ‘Wavenet’ [52] and hierarchical recurrent neural network, called ‘SampleRNN’ [53]. Finally, we have also seen successful architectures that totally remove the hand-crafted linguistic features obtained through text analysis by relying in sequence-to-sequence systems. This system is called Tacotron [54]. As expected, the combination of these advanced models results in a very high-quality end-to-end TTS synthesis system [55, 56] and recent results reveal that the generated synthetic speech sounds as natural as human speech [56].

For more details and technical comparisons, please see the results of Blizzard Challenge, which annually compares the performance of speech synthesis systems built on the common database over decades [57, 58].

15.2.3.1 Spoofing

There is a considerable volume of research in the literature which has demonstrated the vulnerability of ASV to synthetic voices generated with a variety of approaches to speech synthesis. Experiments using formant, diphone, and unit selection based synthetic speech in addition to the simple cut-and-paste of speech waveforms have been reported [19, 20, 59].

ASV vulnerabilities to HMM-based synthetic speech were first demonstrated over a decade ago [60] using an HMM-based, text-prompted ASV system [61] and an HMM-based synthesiser where acoustic models were adapted to specific human speakers [62, 63]. The ASV system scored feature vectors against speaker and background models composed of concatenated phoneme models. When tested with human speech, the ASV system achieved a FAR of 0% and a false rejection rate (FRR) of 7%. When subjected to spoofing attacks with synthetic speech, the FAR increased to over 70%, however, this work involved only 20 speakers.

Larger scale experiments using the Wall Street Journal corpus containing in the order of 300 speakers and 2 different ASV systems (GMM-UBM and SVM using Gaussian supervectors) was reported in [64]. Using an HMM-based speech synthesiser, the FAR was shown to rise to 86 and 81% for the GMM-UBM and SVM systems, respectively, representing a genuine threat to ASV. Spoofing experiments using HMM-based synthetic speech against a forensics speaker verification tool *BATVOX* was also reported in [65] with similar findings. Therefore, the above speech synthesisers were chosen as one of spoofing methods in the ASVspoof 2015 database.

Spoofing experiments using the above advanced DNNs or using spoofing-specific strategies such as GAN have not yet been properly investigated. Only a relatively small-scale spoofing experiment against a speaker recognition system using Wavenet, SampleRNN and GAN is reported in [66].

15.2.3.2 Countermeasures

Only a small number of attempts to discriminate synthetic speech from natural speech had been investigated before the ASVspoof challenge started. Previous work has demonstrated the successful detection of synthetic speech based on prior knowledge of the acoustic differences of specific speech synthesisers such as the dynamic ranges of spectral parameters at the utterance level [67] and variance of higher order parts of mel-cepstral coefficients [68].

There are some attempts which focus on acoustic differences between vocoders and natural speech. Since the human auditory system is known to be relatively insensitive to phase [69], vocoders are typically based on a minimum-phase vocal tract model. This simplification leads to differences in the phase spectra between human and synthetic speech, differences which can be utilised for discrimination [64, 70].

Based on the difficulty in reliable prosody modelling in both unit selection and statistical parametric speech synthesis, other approaches to synthetic speech detection use F0 statistics [71, 72]. F0 patterns generated for the statistical parametric speech synthesis approach tend to be oversmoothed and the unit selection approach frequently exhibits ‘F0 jumps’ at concatenation points of speech units.

After the ASVspoof challenges took place, various types of countermeasures that work for both speech synthesis and voice conversion have been proposed. Please read the next section for the details of the recently developed countermeasures.

15.2.4 Voice Conversion

Voice conversion, in short, VC, is a spoofing attack against automatic speaker verification using an attacker’s natural voice which is converted towards that of the target. It aims to convert one speaker’s voice towards that of another and is a sub-domain of voice transformation [73]. Unlike TTS, which requires text input, voice conversion operates directly on speech inputs. However, speech waveform generation modules such as vocoders may be the same as or similar to those for TTS.

A major application of VC is to personalise and create new voices for TTS synthesis systems and spoken dialogue systems. Other applications include speaking aid devices that generate more intelligible voice sounds to help people with speech disorders, movie dubbing, language learning, and singing voice conversion. The field has also attracted increasing interest in the context of ASV vulnerabilities for almost two decades [74].

Most voice conversion approaches require a parallel corpus where source and target speakers read out identical utterances and adopt a training phase which typically requires frame- or phone-aligned audio pairs of the source and target utterances and estimates transformation functions that convert acoustic parameters of the source speaker to those of the target speaker. This is called ‘parallel voice conversion’. Frame alignment is traditionally achieved using dynamic time warping (DTW) on the source target training audio files. Phone alignment is traditionally achieved using *automatic* *speech recognition* (ASR) and phone-level forth alignment. The estimated conversion function is then applied to any new audio files uttered by the source speaker [75].

A large number of estimation methods for the transformation functions have been reported starting in the late 1980s. In the late 1980s and 90s, simple techniques employing vector quantisation (VQ) with codebooks [76] or segmental codebooks [77] of paired source-target frame vectors were proposed to represent the transformation functions. However, these VQ methods introduced frame-to-frame discontinuity problems.

In the late 1990 and 2000s, *joint density Gaussian mixture model* (JDGMM) based transformation methods [78, 79] were proposed and have since then been actively improved by many researchers [80, 81]. This method still remains popular even now. Although this method achieves smooth feature transformations using a locally linear transformation, this method also has several critical problems such as oversmoothing [82–84] and overfitting [85, 86] which leads to muffled quality of speech and degraded speaker similarity.

Therefore, in the early 2010, several alternative linear transformation methods were developed. Examples are partial least square (PLS) regression [85], tensor representation [87], a trajectory HMM [88], mixture of factor analysers [89], local linear transformation [82] or noisy channel models [90].

In parallel to the linear-based approaches, there have been studies on nonlinear transformation functions such as support vector regression [91], kernel partial least square [92] and conditional restricted Boltzmann machines [93], neural networks [94, 95], highway network [96] and RNN [97, 98]. Data-driven frequency warping techniques [99–101] have also been studied.

Recently, deep learning has changed the above standard procedures for voice conversion and we can see many different solutions now. For instance, variational auto-encoder or sequence-to-sequence neural networks enable us to build VC systems without using frame level alignment [102, 103]. It has also been shown that a cycle-consistent adversarial network called ‘CycleGAN’ [104] is one possible solution for building VC systems without using a parallel corpus. Wavenet can also be used as a replacement for the purpose of generating speech waveforms from converted acoustic features [105].

The approaches to voice conversion considered above are usually applied to the transformation of spectral envelope features, though the conversion of prosodic features such as fundamental frequency [106–109] and duration [107, 110] has also been studied.

For more details and technical comparisons, please see results of Voice Conversion Challenges that compare the performance of VC systems built on a common database [111, 112].

15.2.4.1 Spoofing

When applied to spoofing, the aim with voice conversion is to synthesise a new speech signal such that the extracted ASV features are close in some sense to the target speaker. Some of the first works relevant to text-independent ASV spoofing were reported in [113, 114]. The work in [113] showed that baseline EER increased from 16 to 26% thanks to a voice conversion system which also converted prosodic aspects not modelled in typical ASV systems. This work targeted the conversion of spectral-slope parameters and showed that the baseline EER of 10% increased to over 60% when all impostor test samples were replaced with converted voices. Moreover, signals subjected to voice conversion did not exhibit any perceivable artefacts indicative of manipulation.

The work in [115] investigated ASV vulnerabilities to voice conversion based on JDGMMs [78] which requires a parallel training corpus for both source and target speakers. Even if the converted speech could be easily detectable by human listeners, experiments involving five different ASV systems showed their universal susceptibility to spoofing. The FAR of the most robust, JFA system increased from 3% to over 17%. Instead of vocoder-based waveform generation, unit selection approaches can be applied directly to feature vectors coming from the target speaker to synthesise converted speech [116]. Since they use target speaker data directly, unit selection approaches arguably pose a greater risk to ASV than statistical approaches [117]. In the ASVspoof 2015 challenge, we therefore had chosen these popular VC methods as spoofing methods.

Other work relevant to voice conversion includes attacks referred to as artificial signals. It was noted in [118] that certain short intervals of converted speech yield extremely high scores or likelihoods. Such intervals are not representative of intelligible speech but they are nonetheless effective in overcoming typical ASV systems which lack any form of speech quality assessment. The work in [118] showed that artificial signals optimised with a genetic algorithm provoke increases in the EER from 10% to almost 80% for a GMM-UBM system and from 5% to almost 65% for a factor analysis (FA) system.

15.2.4.2 Countermeasures

Here, we provide an overview of countermeasure methods developed for the VC attacks before the ASVspoof challenge began.

Some of the first works to detect converted voice draws on related work in synthetic speech detection [119]. In [70, 120], cosine phase and modified group delay function (MGDF) based countermeasures were proposed. These are effective in detecting converted speech using vocoders based on minimum phase. In VC, it is, however, possible to use natural phase information extracted from a source speaker [114]. In this case, they are unlikely to detect converted voice.

Two approaches to artificial signal detection are reported in [121]. Experimental work shows that supervector-based SVM classifiers are naturally robust to such attacks, and that all the spoofing attacks they used could be detected by using an utterance-level variability feature, which detected the absence of the natural and dynamic variabilities characteristic of genuine speech. A related approach to detect converted voice is proposed in [122]. Probabilistic mappings between source and target speaker models are shown to typically yield converted speech with less short-term variability than genuine speech. Therefore, the thresholded, average pair-wise distance between consecutive feature vectors was used to detect converted voice with an EER of under 3%.

Due to the fact that majority of VC techniques operate at the short-term frame level, more sophisticated long-term features such as temporal magnitude and phase modulation feature can also detect converted speech [123]. Another experiment reported in [124] showed that local binary pattern analysis of sequences of acoustic vectors can also be used for successfully detecting frame-wise JDGMM-based converted voice. However, it is unclear whether these features are effective in detecting recent VC systems that consider long-term dependency such as recurrent or autoregressive neural network models.

After the ASVspoof challenges took place, new countermeasures that works for both speech synthesis and voice conversion were proposed and evaluated. See the next section for a detailed review of the recently developed countermeasures.

15.3 Summary of the Spoofing Challenges

A number of independent studies confirm the vulnerability of ASV technology to spoofed voice created using voice conversion, speech synthesis and playback [6]. Early studies on speaker anti-spoofing were mostly conducted on in-house speech corpora created using a limited number of spoofing attacks. The development of countermeasures using only a small number of spoofing attacks may not offer the generalisation ability in the presence of different or unseen attacks. There was a lack of publicly available corpora and evaluation protocol to help with comparing the results obtained by different researchers.

The ASVspoof[1] initiative aims to overcome this bottleneck by making available standard speech corpora consisting of a large number of spoofing attacks, evaluation protocols and metrics to support a common evaluation and the benchmarking of different systems. The speech corpora were initially distributed by organising an evaluation challenge. In order to make the challenge simple and to maximise participation, the ASVspoof challenges so far involved only the detection of spoofed speech; in effect, to determine whether a speech sample is genuine or spoofed. A training set and development set consisting of several spoofing attacks were first shared with the challenge participants to help them develop and tune their anti-spoofing algorithm. Next, the evaluation set without any label indicating genuine or spoofed speech was distributed, and the organisers asked the participants to submit scores within a specific deadline. Participants were allowed to submit scores of multiple systems. One of these systems was designated as the primary submission. Spoofing detectors for all primary submissions were trained using only the training data in the challenge corpus. Finally, the organisers evaluated the scores for benchmarks and ranking.

[1] http://www.asvspoof.org/.

Table 15.1 Summary of the datasets used in ASVspoof challenges

	ASVspoof 2015 [125]	ASVspoof 2017 [126]
Theme	Detection of artificially generated speech	Detection of replay speech
Speech format	$F_s = 16$ kHz, 16 bit PCM	$F_s = 16$ kHz, 16 bit PCM
Natural speech	Recorded using high-quality microphone	Recorded using different smart phones
Spoofed speech	Created with seven VC and three SS methods	Collected 'in the wild' by crowdsourcing using different microphone and playback devices from diverse environments
Spoofing types in train/dev/eval	5/5/10	3/10/57
No of speakers in train/dev/eval	25/35/46	10/8/24
No of genuine speech files in train/dev/eval	3750/3497/9404	1508/760/1298
No of spoofed speech files in train/dev/eval	12625/49875/184000	1508/950/12008

The evaluation keys were subsequently released to the challenge participants. The challenge results were discussed with the participants in a special session in INTERSPEECH conferences, which also involved sharing knowledge and receiving useful feedback. To promote further research and technological advancements, the datasets used in the challenge are made publicly available.

The ASVspoof challenges have been organised twice so far. The first was held in 2015 and the second in 2017. A summary of the speech corpora used in the two challenges are shown in Table 15.1. In both the challenges, EER metric was used to evaluate the performance of spoofing detector. The EER is computed by considering the scores of genuine files as positive scores and those of spoofed files as negative scores. A lower EER means more accurate spoofing countermeasures. In practice, the EER is estimated using a specific *receiver operating characteristics convex hull* (ROCCH) technique with an open-source implementation[2] originating from outside the ASVspoof consortium. In the following subsections, we briefly discuss the two challenges. For more interested readers, [125] contains details of the 2015 edition while [126] discusses the results of the 2017 edition.

[2] https://sites.google.com/site/bosaristoolkit/.

15.3.1 ASVspoof 2015

The first ASVspoof challenge involved detection of artificial speech created using a mixture of voice conversion and speech synthesis techniques [125]. The dataset was generated with ten different artificial speech generation algorithms. The ASVspoof 2015 was based upon a larger collection spoofing and anti-spoofing (SAS) corpus (v1.0) [127] that consists of both natural and artificial speech. Natural speech was recorded from 106 human speakers using a high-quality microphone and without significant channel or background noise effects. In a speaker disjoint manner, the full database was divided into three subsets called the training, development, and evaluation set. Five of the attacks (S1–S5), named as *known attacks*, were used in the training and development set. The other five attacks, S6-S10, called *unknown attacks*, were used only in the evaluation set, along with the known attacks. Thus, this provides the possibility of assessing the generalisability of the spoofing detectors. The detailed evaluation plan is available in [128], describing the speech corpora and challenge rules.

Ten different spoofing attacks used in the ASVspoof 2015 are listed below:

- **S1**: a simplified frame selection (FS) based voice conversion algorithm, in which the converted speech is generated by selecting target speech frames.
- **S2**: the simplest voice conversion algorithm which adjusts only the first mel-cepstral coefficient (C1) in order to shift the slope of the source spectrum to the target.
- **S3**: a speech synthesis algorithm implemented with the HMM-based speech synthesis system (HTS3) using speaker adaptation techniques and only 20 adaptation utterances.
- **S4**: the same algorithm as S3, but using 40 adaptation utterances.
- **S5**: a voice conversion algorithm implemented with the voice conversion toolkit and with the Festvox system.[3]
- **S6**: a VC algorithm based on joint density Gaussian mixture models (GMMs) and maximum likelihood parameter generation considering global variance.
- **S7**: a VC algorithm similar to S6, but using line spectrum pair (LSP) rather than mel-cepstral coefficients for spectrum representation.
- **S8**: a tensor-based approach to VC, for which a Japanese dataset was used to construct the speaker space.
- **S9**: a VC algorithm which uses kernel-based partial least square (KPLS) to implement a nonlinear transformation function.
- **S10**: an SS algorithm implemented with the open-source MARY text-to-tpeech system (MaryTTS).[4]

More details of how the SAS corpus was generated can be found in [127].

The organisers also confirmed the vulnerability to spoofing by conducting speaker verification experiments with this data and demonstrating considerable performance

[3] http://www.festvox.org/.

[4] http://mary.dfki.de/.

degradation in the presence of spoofing. With a state-of-the-art probabilistic linear discriminant analysis (PLDA) based ASV system, it is shown that in presence of spoofing, the average EER for ASV increases from 2.30 to 36.00% for male and 2.08 to 39.53% for female [125]. This motivates the development of the anti-spoofing algorithm.

For ASVspoof 2015, the challenge evaluation metric was the average EER. It is computed by calculating EERs for each attack and then taking average. The dataset was requested by 28 teams from 16 countries, 16 teams returned primary submissions by the deadline. A total of 27 additional submissions were also received. Anonymous results were subsequently returned to each team, who were then invited to submit their work to the ASVspoof special session for INTERSPEECH 2015.

Table 15.2 shows the performance of the top five systems in the ASVspoof 2015 challenge. The best performing system [129] uses a combination of *mel cesptral* and *cochlear filter cepstral coefficients plus instantaneous frequency* features with GMM back-end. In most cases, the participants have used fusion of multiple feature based systems to get better recognition accuracy. Variants of cepstral features computed from the magnitude and phase of short-term speech are widely used for the detection of spoofing attacks. As a back-end, GMM was found to outperform

Table 15.2 Performance of top five systems in ASVspoof 2015 challenge (ranked according to the average % EER for all attacks) with respective features and classifiers

System	Avg. EER for			System
Identifier	Known	Unknown	All	Description
A [129]	0.408	2.013	1.211	*Features*: mel-frequency cepstral coefficients (MFCC), Cochlear filter cepstral coefficients plus instantaneous frequency (CFCCIF). *Classifier*: GMM
B [130]	0.008	3.922	1.965	*Features*: MFCC, MFPC, cosine phase principal coefficients (CosPhasePCs). *Classifier*: Support vector machine (SVM) with i-vectors
C [131]	0.058	4.998	2.528	*Feature*: DNN-based with filterbank output and their deltas as input. *Classifier*: Mahalanobis distance on s-vectors
D [132]	0.003	5.231	2.617	*Features*: log magnitude spectrum (LMS), residual log magnitude spectrum (RLMS), group delay (GD), modified group delay (MGD), instantaneous frequency derivative (IF), baseband phase difference (BPD), and pitch synchronous phase (PSP), *Classifier*: Multilayer perceptron (MLP)
E [133]	0.041	5.347	2.694	*Features*: MFCC, product spectrum MFCC (PS-MFCC), MGD with and without energy, weighted linear prediction group delay, cepstral coefficients (WLP-GDCCs), and MFCC cosine-normalised phase-based cepstral coefficients (MFCC-CNPCCs) *Classifier*: GMM

more advanced classifiers like i-vectors, possibly due to the use of short segments of high-quality speech not requiring treatment for channel compensation and background noise reduction. All the systems submitted in the challenge are reviewed in more detail [134].

15.3.2 ASVspoof 2017

The ASVspoof 2017 is the second automatic speaker verification anti-spoofing and countermeasures challenge. Unlike the 2015 edition that used very high-quality speech material, the 2017 edition aims to assess spoofing attack detection with 'out in the wild' conditions. It focuses exclusively on replay attacks. The corpus originates from the recent *text-dependent RedDots* corpus,[5] whose purpose was to collect speech data over mobile devices, in the form of smartphones and tablet computers, by volunteers from across the globe.

The replayed version of the original *RedDots* corpus was collected through a crowdsourcing exercise using various replay configurations consisting of varied devices, loudspeakers, and recording devices, under a variety of different environments across four European countries within the EU Horizon 2020-funded OCTAVE project,[6] (see [126]). Instead of covert recording, we made a "short-cut" and took the digital copy of the target speakers' voice to create the playback versions. The collected corpus is divided into three subsets: for training, development and evaluation. Details of each are presented in Table 15.1. All three subsets are disjoint in terms of speakers and data collection sites. The training and development subsets were collected at three different sites. The evaluation subset was collected at the same three sites and also included data from two new sites. Data from the same site include different recordings and replaying devices and from different acoustic environments. The evaluation subset contains data collected from 161 replay sessions in 62 unique replay configurations.[7] More details regarding replay configurations can be found in [126, 135].

The primary evaluation metric is 'pooled' EER. In contrast to the ASVspoof 2015 challenge, the EER is computed from scores pooled across all the trial segments rather than condition averaging. A baseline[8] system based on common GMM backend classifier with constant-Q cepstral coefficient (CQCC) [136, 137] features were provided to the participants. This configuration is chosen as baseline as it has shown best recognition performance on ASVspoof 2015. The baseline is trained using either combined training and development data (B01) or training data (B02) alone. The baseline system does not involve any kind of optimisation or tuning with respect

[5] https://sites.google.com/site/thereddotsproject/.

[6] https://www.octave-project.eu/.

[7] A **replay configuration** refers to a unique combination of room, replay device and recording device while a **session** refers to a set of source files, which share the same replay configuration.

[8] See *Appendix A.2. Software packages*.

Table 15.3 Summary of top 10 primary submissions to ASVspoof 2017. Systems' IDs are the same received by participants in the evaluation. The column 'Training' refers to the part of data used for training: train (T) and/or development (D)

ID	Features	Post-proc.	Classifiers	Fusion	#Subs.	Training	Performances on eval subset (EER%)
S01 [138]	Log-power Spectrum, LPCC	MVN	CNN, GMM, TV, RNN	Score	3	T	6.73
S02 [139]	CQCC, MFCC, PLP	WMVN	GMM-UBM, TV-PLDA, GSV-SVM, GSV-GBDT, GSV-RF	Score	–	T	12.34
S03	MFCC, IMFCC, RFCC, LFCC, PLP, CQCC, SCMC, SSFC	–	GMM, FF-ANN	Score	18	T+D	14.03
S04	RFCC, MFCC, IMFCC, LFCC, SSFC, SCMC	–	GMM	Score	12	T+D	14.66
S05 [140]	Linear filterbank feature	MN	GMM, CT-DNN	Score	2	T	15.97
S06	CQCC, IMFCC, SCMC, Phrase one-hot encoding	MN	GMM	Score	4	T+D	17.62
S07	HPCC, CQCC	MVN	GMM, CNN, SVM	Score	2	T+D	18.14
S08 [141]	IFCC, CFCCIF, Prosody	–	GMM	Score	3	T	18.32
S09	SFFCC	No	GMM	None	1	T	20.57
S10 [142]	CQCC	–	ResNet	None	1	T	20.32

to [136]. The dataset was requested by 113 teams, of which 49 returned primary submissions by the deadline. The results of the challenge were disseminated at a special session consisting of two slots at INTERSPEECH 2017.

Most of the systems are based on standard spectral features, such as CQCCs, MFCCs and *perceptual linear prediction* (PLP). As a back-end, in addition to the classical GMM to model the replay and non-replay classes, it has also exploited the power of deep classifiers, such as *convolutional neural network* (CNN) or *recurrent neural network* (RNN). A fusion of multiple features and classifiers is also widely adopted by the participants. A summary of the top-10 primary systems is provided in Table 15.3. Results in terms of EER of the 49 primary systems and the baseline B01 and B02 are shown in Fig. 15.3.

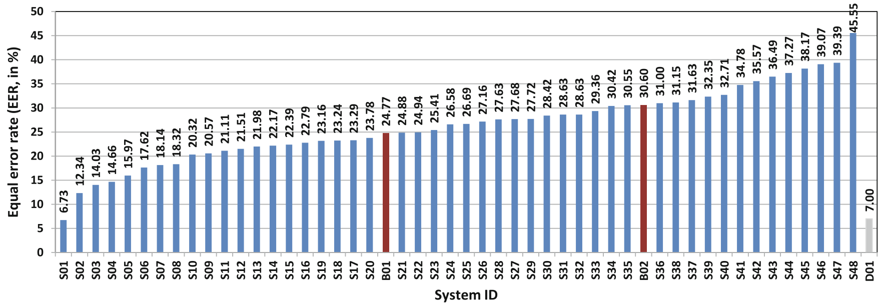

Fig. 15.3 Performance of the two baseline systems (B01 and B02) and the 49 primary systems (S01–S48 in addition to late submission D01) for the ASVspoof 2017 challenge. Results are in terms of the replay/non-replay EER (%)

15.4 Advances in Front-End Features

The selection of appropriate features for a given classification problem is an important task. Even if the classic boundary to think between a feature extractor (front-end) and a classifier (back-end) as separate components is getting increasingly blurred with the use of end-to-end deep learning and other similar techniques, research on the 'early' components in a pipeline remains important. In the context of anti-spoofing for ASV, this allows the utilisation of one's domain knowledge to guide the design of new discriminative features. For instance, earlier experience suggests that lack of spectral [70] and temporal [123] detail is characteristic of synthetic or voice-coded (vocoded) speech, and that low-quality replayed signals tend to experience loss of spectral details [143]. These initial findings sparked further research into developing advanced front-end features with improved robustness, generalisation across datasets, and other desideratum. As a matter of fact, in contrast to classic ASV (without spoofing attacks) where the most significant advancements have been in the back-end modelling [2], in ASV anti-spoofing, the features seem to make the difference. In this section, we take a brief look at a few such methods emerging from the ASVspoof evaluations. The list is by no means exhaustive and the interested reader is referred to [134] for further discussion.

15.4.1 Front-Ends for Detection of Voice Conversion and Speech Synthesis Spoofing

The front-ends described below have been shown to provide good performance on the ASVspoof 2015 database of spoofing attacks based on voice conversion and speech synthesis. The first front-end was used in the ASVspoof 2015 challenge, while the rest were proposed later after the evaluation.

Cochlear Filter Cepstral Coefficients with Instantaneous Frequency (CFCCIF). These features were introduced in [129] and successfully used as part of the top-ranked system in the ASVspoof 2015 evaluation. They combine cochlear filter cepstral coefficients (CFCC), proposed in [144], with instantaneous frequency [69]. CFCC is based on wavelet transform-like auditory transform and on some mechanisms of the cochlea of the human ear such as hair cells and nerve spike density. To compute CFCC with instantaneous frequency (CFCCIF), the output of the nerve spike density envelope is multiplied by the instantaneous frequency, followed by the derivative operation and logarithm nonlinearity. Finally, the Discrete Cosine Transform (DCT) is applied to decorrelate the features and obtain a set of cepstral coefficients.

Linear Frequency Cepstral Coefficients (LFCC). LFCCs are very similar to the widely used mel-frequency cepstral coefficients (MFCCs) [145], though the filters are placed in equal sizes for linear scale. This front-end is widely used in speaker recognition and has been shown to perform well in spoofing detection [146]. This technique performs a windowing on the signal, computes the magnitude spectrum using the short-time Fourier transform (STFT), followed by logarithm nonlinearity and the application of a filterbank of linearly spaced N triangular filters to obtain a set of N log-density values. Finally, the DCT is applied to obtain a set of cepstral coefficients.

Constant-Q Cepstral Coefficients (CQCC). This feature was proposed in [136, 137] for spoofing detection and it is based on the Constant-Q Transform (CQT) [147]. The CQT is an alternative time–frequency analysis tool to the STFT that provides variable time and frequency resolution. It provides greater frequency resolution at lower frequencies but greater time resolution at higher frequencies. Figure 15.4 illustrates the CQCC extraction process. The CQT spectrum is obtained, followed by logarithm nonlinearity and by a linearisation of the CQT geometric scale. Finally, cepstral coefficients are obtained through the DCT.

As an alternative to CQCC, infinite impulse response constant-Q transform cepstrum (ICQC) features [148] use the infinite impulse response—constant-Q transform [149], an efficient constant-Q transform based on the IIR filtering of the fast Fourier transform (FFT) spectrum. It delivers multiresolution time–frequency analysis in a linear scale spectrum which is ready to be coupled with traditional cepstral analysis. The IIR-CQT spectrum is followed by the logarithm and decorrelation, either through the DCT or principal component analysis.

Deep Features for Spoofing Detection. All of the above three features sets are handcrafted and consist of a fixed sequence of standard digital signal processing

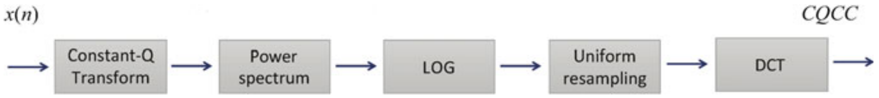

Fig. 15.4 Block diagram of CQCC feature extraction process

operations. An alternative approach, seeing increased popularity across different machine learning problems, is to learn the feature extractor from a given data by using deep learning techniques [150, 151]. In speech-related applications, these features are widely employed for improving recognition accuracy [152–154]. The work in [155] uses deep neural network to generate bottleneck features for spoofing detection; that is, the activations of a hidden layer with a relatively small number of nodes compared to the size of other layers. The study in [156] investigates various features based on deep learning techniques. Different feed-forward DNNs are used to obtain frame level deep features. Input acoustic features consisting of filterbank outputs with their first derivatives are used to train the network to discriminate between the natural and spoofed speech classes, and output of hidden layers are taken as deep features which are then averaged to obtain an utterance-level descriptor. RNNs are also proposed to estimate utterance-level features from input sequences of acoustic features. In another recent work [157], the authors have investigated deep features based on filterbank trained with the natural and artificial speech data. A feed-forward neural network architecture called here as filter bank neural network (FBNN) is used here that includes a linear hidden layer, a sigmoid hidden layer and a softmax output layer. The number of nodes in the output is six; and of them, five are for the number of spoofed classes in the training set, and the remaining one is for natural speech. The filter banks are learned using the stochastic gradient descent algorithm. The cepstral features extracted using these DNN-based features are shown to be better than the hand-crafted cepstral coefficients.

Scattering Cepstral Coefficients. This feature for spoofing detection was proposed in [158]. It relies upon *scattering spectral decomposition* [159, 160]. This transform is a hierarchical spectral decomposition of a signal based on wavelet filter banks (constant-Q filters), modulus operator, and averaging. Each level of decomposition processes the input signal (either the input signal for the first level of decomposition, or the output of a previous level of decomposition) through the wavelet filterbank and takes the absolute value of filter outputs, producing a scalogram. The scattering coefficients at a certain level are estimated by windowing the scalogram signals and computing the average value within these windows. A two-level scattering decomposition has been shown to be effective for spoofing detection [158]. The final feature vector is computed by taking the DCT of the vector obtained by concatenating the logarithms of the scattering coefficients from all levels and retaining the first a few coefficients. The 'interesting' thing about scattering transform is its stability to small signal deformation and more details of the temporal envelopes than MFCCs [158, 159].

Fundamental Frequency Variation Features. The prosodic features are not as successful as cepstral features in detecting artificial speech on ASVspoof 2015, though some earlier results on PAs indicate that pitch contours are useful for such tasks [6]. In a recent work [161], the author uses fundamental frequency variation (FFV) for this. The FFV captures pitch variation at the frame level and provides complementary information on cepstral features [162]. The combined system gives a very promising performance for both known and unknown conditions on ASVspoof evaluation data.

Phase-based Features. The phase-based features are also successfully used in PAD systems for ASVspoof 2015. For example, relative phase shift (RPS) and modified group delay (MGD) based features are explored in [163]. The authors in [164] have investigated relative phase information (RPI) features. Though the performances on seen attacks are promising with these phase-based features, the performances noticeably degrade for unseen attacks, particularly for S10.

General Observations Regarding Front-Ends for Artificial Speech Setection. Beyond the feature extraction method used, there are two general findings common to any front- end [129, 137, 146, 148]. The first refers to the use of dynamic coefficients. The first and second derivatives of the static coefficients, also known as velocity and acceleration coefficients, respectively, are found important to achieve good spoofing detection performance. In some cases, the use of only dynamic features is superior to the use of static plus dynamic coefficients [146]. This is not entirely surprising, since voice conversion and speech synthesis techniques may fail to model the dynamic properties of the speech signals, introducing artefacts that help the discrimination of spoofed signals. The second finding refers to the use of speech activity detection. In experiments with ASVspoof 2015 corpus, it appears that the silence regions also contain useful information for discriminating between natural and synthetic speech. Thus, retaining non-speech frames turns out to be a better choice for this corpus [146]. This is likely due to the fact that non-speech regions are usually replaced with noise during the voice conversion or speech synthesis operation. However, this could be a database-dependent observation, thus detailed investigations are required.

15.4.2 Front-Ends for Replay Attack Detection

The following front-ends have been proposed for the task of replay spoofing detection, and evaluated in replayed speech databases such as the BTAS 2016 and ASVspoof 2017. Many standard front-ends, such as MFCC, LFCC and PLP, have been combined to improve the performance of replay attack detection. Other front-ends proposed for synthetic and converted speech detection (CFCCIF, CQCC) have been successfully used for the replay detection task. In general, and in opposition to the trend for synthetic and converted speech detection, the use of static coefficients has been shown to be crucial for achieving good performance. This may be explained by the nature of the replayed speech detection task, where detecting changes in the channel captured by static coefficients help with the discrimination of natural and replayed speech. Two additional front-ends are described next.

Inverted Mel-Frequency Cepstral Coefficients (IMFCC). This front-end is relatively simple and similar to the standard MFCC. The only difference is that the filterbank follows an inverted mel scale; that is, it provides an increasing frequency resolution (narrower filters) when frequency increases, and a decreased frequency resolution (wider filters) for decreasing frequency, unlike the mel scale [165]. This front-end was used as part of the top-ranked system of the Biometrics: Theory, Applications, and Systems (BTAS) 2016 speaker anti-spoofing competition [7].

Features Based on Convolutional Neural Networks. In the recent ASVspoof 2017 challenge, the use of deep learning frameworks for feature learning was proven to be key in achieving good replay detection performance. In particular, convolutional neural networks have been successfully used to learn high-level utterance-level features which can later be classified with simple classifiers. As part of the top-ranked system [138] in the ASVspoof 2017 challenge, a light convolutional neural network architecture [166] is fed with truncated normalised FFT spectrograms (to force fixed data dimensions). The network consists of a set of convolutional layers, followed by a fully connected layer. The last layer contains two outputs with softmax activation corresponding to the two classes. All layers use the max-feature-map activation function [166], which acts as a feature selector and reduces the number of feature maps by half on each layer. The network is then trained to discriminate between the natural and spoofed speech classes. Once the network is trained, it is used to extract a high-level feature vector which is the output of the fully connected layer. All the test utterances are processed to obtain high-level representations, which are later classified with an external classifier.

Other Hand-Crafted Features. Many other features have also been used for replayed speech detection in the context of the ASVspoof 2017 database. Even if the performances of single systems using such features are not always high, they are shown to be complementary when fused at the score level [167], similar to conventional ASV research outside of the spoofing detection. These features include MFCC, IMFCC, rectangular filter cepstral coefficients (RFCCs), PLP, CQCC, spectral centroid magnitude coefficients (SCMC), subband spectral flux coefficient (SSFC) and variable length Teager energy operator energy separation algorithm-instantaneous frequency cosine coefficients (VESA-IFCC). Though, of course, one usually then has to further train the fusion system, which makes the system more involved concerning practical applications.

15.5 Advances in Back-End Classifiers

In the natural versus spoof classification problem, two main families of approaches have been adopted, namely generative and discriminative. Generative approaches include those of GMM-based classifiers and i-vector representations combined with support vector machines (SVMs). As for discriminative approaches, deep learning-based techniques have become more popular. Finally, new deep learning end-to-end solutions are emerging. Such techniques perform the typical pipeline entirely through deep learning, from feature representation learning and extraction to the final classification. While including such approaches into the traditional classifiers category may not be the most precise, they are included in this classifiers section for simplicity.

15.5.1 Generative Approaches

Gaussian Mixture Model (GMM) Classifiers. Considering two classes, namely natural and spoofed speech, one GMM can be learned for each class using appropriate training data. In the classification stage, an input utterance is processed to obtain its likelihoods with respect to the natural and spoofed models. The resulting classification score is the log-likelihood ratio between the two competing hypotheses; in effect, those of the input utterance belonging to the natural and to the spoofed classes. A high score supports the former hypothesis, while a low score supports the latter. Finally, given a test utterance, classification can be performed by thresholding the obtained score. If the score is above the threshold, the test utterance is classified as natural, and otherwise, it is classified as spoof. Many proposed anti-spoofing systems use GMM classifiers [129, 136, 146, 148, 155, 158, 168].

I-vector. The state-of-the-art i-vector paradigm for speaker verification [169] has been explored for spoofing detection [170, 171]. Typically, an i-vector is extracted from an entire speech utterance and used as a low-dimensional, high-level feature which is later classified by means of a binary classifier, commonly cosine distance measure or support vector machine (SVM). Different amplitude- and phase-based front-ends [130, 138] can be employed for the estimation of i-vectors. A recent work shows that data selection for i-vector extractor training (also known as **T** matrix) is an important factor for achieving completive recognition accuracy [172].

15.5.2 Discriminative Approaches

DNN Classifiers. Deep learning-based classifiers have been explored for use in the task of natural and spoofed speech discrimination. In [155, 173], several front-ends are evaluated with neural network classifier consisting of several hidden layers with sigmoid nodes and softmax output, which is used to calculate utterance posteriors. However, the implementation detail of the DNNs—such the number of nodes, the cost function, the optimization algorithm and the activation functions—is not precisely mentioned in those work and the lack of this very relevant information makes it difficult to reproduce the results.

In a recent work [174], a five-layer DNN spoofing detection system is investigated for ASVspoof 2015 which uses a novel scoring method, termed in the paper as *human log-likelihoods* (HLLs). Each of the hidden layers has 2048 nodes with a sigmoid activation function. The network has six softmax output layers. The DNN is implemented using a computational network toolkit[9] and trained with stochastic gradient descent methods with dynamics information of acoustic features, such as spectrum-based cepstral coefficients (SBCC) and CQCC as input. The cross entropy function is selected as the cost function and the maximum training epoch is chosen as 120. The mini-batch size is set to 128. The proposed method shows considerable PAD detection performance. The author obtain an EER for S10 of 0.255% and average EER for all attacks of 0.045- when used with CQCC acoustic features. These are the best reported performance in ASVspoof 2015 so far.

DNN-Based End-to-End Approaches. End-to-end systems aim to perform all the stages of a typical spoofing detection pipeline, from feature extraction to classification, by learning the network parameters involved in the process as a whole. The advantage of such approaches is that they do not explicitly require prior knowledge of the spoofing attacks as required for the development of acoustic features. Instead, the parameters are learned and optimised from the training data. In [175], a convolutional long short-term memory (LSTM) deep neural network (CLDNN) [176] is used as an end-to-end solution for spoofing detection. This model receives input in the form of a sequence of raw speech frames and outputs a likelihood for the whole sequence. The CLDNN performs time–frequency convolution through CNN to reduce spectral variance, long-term temporal modelling by using a LSTM, and classification using a DNN. Therefore, it is entirely an end-to-end solution which does not rely on any external feature representation. The works in [138, 177] propose other end-to-end solutions by combining convolutional and recurrent layers, where the first act as a feature extractor and the second models the long-term dependencies and acts as a classifier. Unlike the work in [175], the input data is the FFT spectrogram of the speech utterance and not the raw speech signal. In [178], the authors have investigated CNN-based end-to-end system for PAD where the raw speech is used to jointly learn the feature extractor and classifier. Score level combination of this CNN system with standard long-term spectral statistics based system shows considerable overall improvement.

15.6 Other PAD Approaches

While most of the studies in voice PAD detection research focus on algorithmic improvements for discriminating natural and artificial speech signals, some recent studies have explored utilising additional information collected using special additional hardware to protect ASV system from presentation attacks [179–182]. Since an intruder can easily collect voice samples for the target speakers using covert recording; the idea here is to detect and recognise supplementary information related to the speech production process. Moreover, by its nature, that supplementary information is difficult, if not impossible, to mimic using spoofing methods in the practical

[9] https://github.com/Microsoft/CNTK.

scenario. These PAD techniques have shown excellent recognition accuracy in the spoofed condition, at the cost of additional setup in the data acquisition step.

The work presented in [180, 181] utilises the phenomenon of *pop noise*, which is a distortion in human breath when it reaches a microphone [183]. During natural speech production, the interactions between the airflow and the vocal cavities may result in a sort of plosive burst, commonly know as pop noise, which can be captured via a microphone. In the context of professional audio and music production, pop noise is unwanted and is eliminated during the recording or mastering process. In the context of ASV, however, it can help in the process of PAD. The basic principle is that a replay sound from a loudspeaker does not involve the turbulent airflow generating the pop noise as in the natural speech. The authors in [180, 181] have developed a pop noise detector which eventually distinguishes natural speech from playback recording as well as synthetic speech generated using VC and SS methods. In experiments with 17 female speakers, a tandem detection system that combines both single- and double-channel pop noise detection gives the lowest ASV error rates in the PA condition.

The authors in [179] have introduced the use of a smartphone-based *magnetometer* to detect voice presentation attack. The conventional loudspeakers, which are used for playback during access of the ASV systems, generate sound using acoustic transducer and generate a magnetic field. The idea, therefore, is to capture the use of loudspeaker by sensing the magnetic field which would be absent from human vocals. Experiments were conducted using playback from 25 different conventional loudspeakers, ranging from low-end to high-end and placed in different distances from the smartphone that contains the ASV system. A speech corpus of five speakers was collected for the ASV experiments executed using an open-source ASV toolkit, SPEAR.[10] Experiments were conducted with other datasets, using a similarly limited number of speakers. The authors demonstrated that the magnetic field based detection can be reliable for the detection of playback within 6–8 cm from the smartphone. They further developed a mechanism to detect the size of the sound source to prevent the use of small speakers such as earphones.

The authors in [184, 185] utilise certain acoustics concepts to prevent ASV systems from PAs. They first introduced a method [184] that estimates dynamic sound source position (articulation position within mouth) of some speech sounds using a small array using *microelectromechanical systems* (MEMS) microphones embedded in mobile devices and compare it with loudspeakers, which have a flat sound source. In particular, the idea is to capture the dynamics of *time-difference-of-arrival* (TDOA) in a sequence of speech sounds to the microphones of the smartphone. Such unique TDOA changes, which do not exist under replay conditions, are used for detecting replay attacks. The similarities between the TDOAs of test speech and user templates are measured using probability function under Gaussian assumption and correlation measure as well as their combinations. Experiments involving 12 speakers and 3 different types of smartphone demonstrate a low EER and high PAD accuracy. The

[10] https://www.idiap.ch/software/bob/docs/bob/bob.bio.spear/stable/index.html.

proposed method is seen to remain robust despite the change of smartphones during the test and the displacements.

In [185], the same research group has used the idea of the *Doppler effect* to detect the replay attack. The idea here is to capture the *articulatory gestures* of the speakers when they speak a passphrase. The smartphone acts as a Doppler radar and transmits a high-frequency tone at 20 kHz from the built-in speaker and senses the reflections using the microphone during authentication process. The movement of the speaker's articulators during vocalisation creates a speaker-dependent Doppler frequency shift at around 20 kHz, which is stored along with the speech signal during the speaker-enrolment process. During a playback attack, the Doppler frequency shift will be different due to the lack of articulatory movements. Energy-based frequency features and frequency-based energy features are computed from a band of 19.8 and 20.2 kHz. These features are used to discriminate between the natural and replayed voice, and the similarity scores are measured in terms of Pearson correlation coefficient. Experiments are conducted with a dataset of 21 speakers and using three different smartphones. The data also includes test speech for replay attack with different loudspeakers and for impersonation attack with four different impersonators. The proposed system was demonstrated to be effective in achieving low EER for both types of attacks. Similar to [184], the proposed method indicated robustness to the phone placement.

The work in [182] introduces the use of a specific non-acoustic sensor, *throat microphone* (TM), or laryngophone, to enhance the performance of the voice PAD system. An example of such microphones is shown in Fig. 15.5. The TM is used with a conventional acoustic microphone (AM) in a dual-channel framework for robust speaker recognition and PAD. Since this type of microphone is attached to the speaker's neck, it would be difficult for the attacker to obtain a covert recording

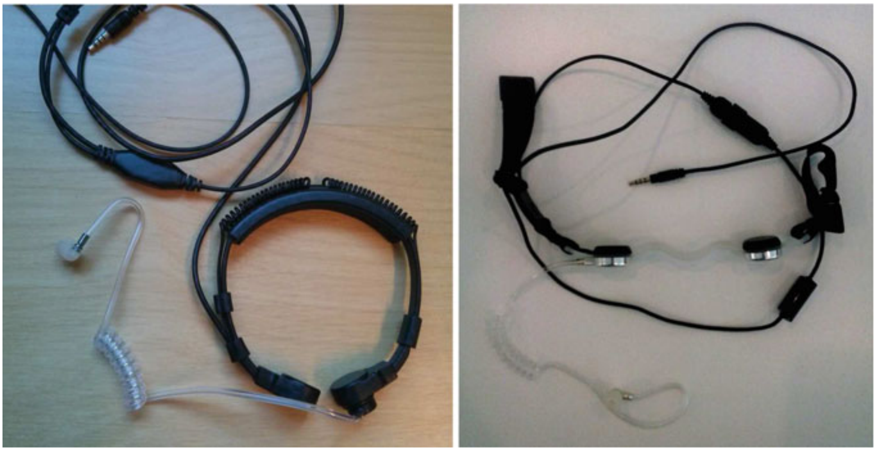

Fig. 15.5 Throat-microphones used in [182]. (Reprinted with permission from IEEEACM Transactions on (T-ASL) Audio, Speech, and Language Processing)

of the target speaker's voice. Therefore, one possibility for the intruder is to use the stolen recording from an AM and to try to record it back using a TM for accessing the ASV system. A speech corpus of 38 speakers were collected for the ASV experiments. The dual-channel setup yielded considerable ASV for both licit and spoofed conditions. The performance is further improved when this ASV system is integrated with the dual-channel based PAD. The authors show zero FAR for replay imposters by decision fusion of ASV and PAD.

All of the above new PAD methods deviating from the 'mainstream' of PAD research in ASV are reported to be reliable and useful in specific application scenarios for identifying presentation attacks. The methods are also fundamentally different and difficult to compare in the same settings. Since the authors focus on the methodological aspects, experiments are mostly conducted on a dataset of limited number of speakers. Extensive experiments with more subjects from diverse environmental conditions should be performed to assess their suitability for real-world deployment.

15.7 Future Directions of Anti-spoofing Research

The research in ASV anti-spoofing is becoming popular and well recognised in the speech processing and voice biometric community. The state-of-the-art spoofing detector gives promising accuracy in the benchmarking of spoofing countermeasures. Further work is needed to address a number of specific issues regarding its practical use. A number of potential topics for consideration in further work are now discussed.

- **Noise, reverberation and channel effect**. Recent studies indicate that spoofing countermeasures offer little resistance to additive noise [186, 187], reverberation [188] and channel effect [189] even though their performances on 'clean' speech corpus is highly promising. The relative degradation of performance is actually much worse than the degradation of a typical ASV system under the similar mismatch condition. One reason could be that, at least until the ASVspoof 2017 evaluation, the methodology developed has been driven in clean, high-quality speech. In other words, the community might have developed its methods implicitly for laboratory testing. The commonly used speech enhancement algorithms also fail to reduce the mismatch due to environmental differences, though multi-condition training [187] and more advanced training methods [190] have been found useful. The study presented in [189] shows considerable degradation of PAD performance even in *matched* acoustic conditions. The feature settings used for the original corpus gives lower accuracy when both training and test data are digitally processed with the telephone channel effect. These are probably because the spoofing artefacts themselves act as extrinsic variabilities which degrade the speech quality in some way. Since the task of spoofing detection is related to detecting those artefacts, the problem becomes more difficult in the presence of small external effects due to variation in environment and channel. These suggest further investigations need to be carried out for the development of robust spoofing countermeasures.

- **Generalisation of spoofing Countermeasures**. The generalisation property of spoofing countermeasures for detecting new kinds of speech presentation attack is an important requirement for their application in the wild. Study explores that countermeasure methods trained with a class of spoofing attacks fail to generalise this for other classes of spoofing attack [167, 191]. For example, PAD systems trained with VC- and SS-based spoofed speech give a very poor performance for playback detection [192]. The results of the first two ASVspoof challenges also reveal that detecting the converted speech created with an "unknown" method or the playback voice recording in a new replay session are difficult to detect. These clearly indicate the overfitting of PAD systems with available training data. Therefore, further investigation should be conducted to develop attack-independent universal spoofing detector. Other than the unknown attack issue, generalisation is also an important concern for cross-corpora evaluation of the PAD system [193]. This specific topic is discussed in chapter 19 of this book.
- **Investigations with new spoofing methods**. The studies of converted spoof speech mostly focused on methods based on classical signal processing and machine learning techniques. Recent advancements in VC and SS research with deep learning technology show significant improvements in creating high-quality synthetic speech [52]. The GAN [194] can be used to create (generator) spoofed voices with relevant feedback from the spoofing countermeasures (discriminator). Some preliminary studies demonstrate that the GAN-based approach can make speaker verification systems more vulnerable to presentation attacks [66, 195]. More detailed investigations should be conducted on this direction for the development of countermeasure technology to guard against this type of advanced attack.
- **Joint operations of PAD and ASV**. The ultimate goal of developing PAD system is to protect the recogniser, the ASV system from imposters with spoofed speech. So far, the majority of the studies focused on the evaluation of standalone countermeasures. The integration of these two systems is not trivial number of reasons. First, standard linear output score fusion techniques, being extensively used to combine homogenous ASV system, are not appropriate since the ASV and its countermeasures are trained to solve two different tasks. Second, an imperfect PAD can increase the false alarm rate by rejecting genuine access trials [196]. Third, and more fundamentally, it is not obvious whether improvements in standalone spoofing countermeasures should improve the overall system as a whole: a nearly perfect PAD system with close to zero EER may fail to protect ASV system in practice if not properly calibrated [197]. In a recent work [198], the authors propose a modification in a GMM-UBM based ASV system to make it suitable for both licit and spoofed conditions. The joint evaluation of PAD and ASV, as well as their combination techniques, certainly deserves further attention. Among other feedback received from the attendees of the ASVspoof 2017 special session organised during INTERSPEECH 2017, it was proposed that the authors of this chapter consider shifting the focus from standalone spoofing to more ASV-centric solutions in future. We tend to agree. In our recent work [199], we propose a new

cost function for joint assessment of PAD and ASV system. In another work [200], we propose a new fusion method for combining scores of countermeasures and recognisers. This work also explores speech features which can be used both for PAD and ASV.

15.8 Conclusion

This contribution provides an introduction to the different voice presentation attacks and their detection methods. It then reviews previous works with a focus on recent progress in assessing the performance of PAD systems. We have also briefly reviewed two recent ASVspoof challenges organised for the detection of voice PAs. This study includes discussion of recently developed features and the classifiers which are predominantly used in ASVspoof evaluations. We further include an extensive survey on alternative PAD methods. Apart from the conventional voice-based systems that use statistical properties of natural and spoofed speech for their discrimination, these recently developed methods utilise a separate hardware for the acquisition of other signals such as pop noise, throat signal and extrasensory signals with smartphones for PAD. The current status of these non-mainstream approaches to PAD detection are somewhat similar to the status of the now more-or-less standard methods for artificial speech and replay PAD detection some 3–4 years ago: they are innovative and show promising results, but the pilot experiments have been carried out on relatively small and/or proprietary datasets, leaving an open question as to how scalable or generalisable these solutions are in practice. Nonetheless, in the long run and noting especially the rapid development of speech synthesis technology, it is likely that the quality of artificial/synthetic speech will eventually be indistinguishable from that of natural human speech. Such future spoofing attacks therefore could not be detected using the current mainstream techniques that focus on spectral or temporal details of the speech signal, but will require novel ideas that benefit from auxiliary information, rather than just the acoustic waveform.

In the past three years, the progress in voice PAD research has been accelerated by the development and free availability of speech corpus such as the ASVspoof series, SAS, BTAS 2016, AVSpoof. The work discussed several open challenges which show that this problem requires further attention to improving robustness due to mismatch condition, generalisation to a new type of presentation attacks, and so on. Results from joint evaluations with integrated ASV system are also an important requirement for practical applications of PAD research. We think, however, that this extensive review will be of interest not only to those involved in voice PAD research but also to voice biometrics researchers in general.

Appendix A. Action Towards Reproducible Research

A.1. Speech Corpora

1. Spoofing and Anti-Spoofing (SAS) database v1.0: This database presents the first version of a speaker verification spoofing and anti-spoofing database, named SAS corpus [201]. The corpus includes nine spoofing techniques, two of which are speech synthesis, and seven are voice conversion.
   Download link: http://dx.doi.org/10.7488/ds/252
2. ASVspoof 2015 database: This database has been used in the first Automatic Speaker Verification Spoofing and Countermeasures Challenge (ASVspoof 2015). Genuine speech is collected from 106 speakers (45 male, 61 female) and with no significant channel or background noise effects. Spoofed speech is generated from the genuine data using a number of different spoofing algorithms. The full dataset is partitioned into three subsets, the first for training, the second for development and the third for evaluation.
   Download link: http://dx.doi.org/10.7488/ds/298
3. ASVspoof 2017 database: This database has been used in the Second Automatic Speaker Verification Spoofing and Countermeasuers Challenge: ASVspoof 2017. This database makes an extensive use of the recent text-dependent RedDots corpus, as well as a replayed version of the same data. It contains a large amount of speech data from 42 speakers collected from 179 replay sessions in 62 unique replay configurations.
   Download link: http://dx.doi.org/10.7488/ds/2313

A.2. Software Packages

1. Feature extraction techniques for anti-spoofing: This package contains the MATLAB implementation of different acoustic feature extraction schemes as evaluated in [146].
   Download link: http://cs.joensuu.fi/~sahid/codes/AntiSpoofing_Features.zip
2. Baseline spoofing detection package for ASVspoof 2017 corpus: This package contains the MATLAB implementations of two spoofing detectors employed as baseline in the official ASVspoof 2017 evaluation. They are based on constant-Q cepstral coefficients (CQCC) [137] and Gaussian mixture model classifiers.
   Download link: http://audio.eurecom.fr/software/ASVspoof2017_baseline_countermeasures.zip

References

1. Kinnunen T, Li H (2010) An overview of text-independent speaker recognition: From features to supervectors. Speech Commun 52(1):12–40. https://doi.org/10.1016/j.specom.2009.08.009. http://www.sciencedirect.com/science/article/pii/S0167639309001289
2. Hansen J, Hasan T (2015) Speaker recognition by machines and humans: a tutorial review. IEEE Signal Process Mag 32(6):74–99
3. ISO/IEC 30107: Information technology—biometric presentation attack detection. International Organization for Standardization (2016)
4. Kinnunen T, Sahidullah M, Kukanov I, Delgado H, Todisco M, Sarkar A, Thomsen N, Hautamäki V, Evans N, Tan ZH (2016) Utterance verification for text-dependent speaker recognition: a comparative assessment using the reddots corpus. In: Proceedings of Interspeech, pp 430–434
5. Shang, W, Stevenson, M. (2010). Score normalization in playback attack detection. In: Proceedings of ICASSP. IEEE, pp 1678–1681
6. Wu Z, Evans N, Kinnunen T, Yamagishi J, Alegre F, Li H (2015) Spoofing and countermeasures for speaker verification: a survey. Speech Commun 66:130–153
7. Korshunov P, Marcel S, Muckenhirn H, Gonçalves A, Mello A, Violato R, Simoes F, Neto M, de Angeloni AM, Stuchi J, Dinkel H, Chen N, Qian Y, Paul D, Saha G, Sahidullah M. (2016). Overview of BTAS 2016 speaker anti-spoofing competition. In: 2016 IEEE 8th international conference on biometrics theory, applications and systems (BTAS), pp 1–6 (2016)
8. Evans N, Kinnunen T, Yamagishi J, Wu Z, Alegre F, DeLeon P (2014) Speaker recognition anti-spoofing. In: Marcel S, Li, SZ, Nixon M (eds) Handbook of biometric anti-spoofing. Springer
9. Marcel S, Li SZ, Nixon M (eds) Handbook of biometric anti-spoofing: trusted biometrics under spoofing attacks. Springer (2014)
10. Farrús Cabeceran M, Wagner M, Erro D, Pericás H (2010) Automatic speaker recognition as a measurement of voice imitation and conversion. The Int J Speech Lang Law 1(17):119–142
11. Perrot P, Aversano G, Chollet G (2007) Voice disguise and automatic detection: review and perspectives. Progress in nonlinear speech processing, pp. 101–117
12. Zetterholm E (2007) Detection of speaker characteristics using voice imitation. In: Speaker Classification II. Springer, pp 192–205
13. Lau Y, Wagner M, Tran D (2004) Vulnerability of speaker verification to voice mimicking. In: Proceedings of 2004 international symposium on intelligent multimedia, video and speech processing, 2004. IEEE, pp 145–148
14. Lau Y, Tran D, Wagner M (2005) Testing voice mimicry with the YOHO speaker verification corpus. In: International conference on knowledge-based and intelligent information and engineering systems. Springer, pp 15–21
15. Mariéthoz J, Bengio S (2005) Can a professional imitator fool a GMM-based speaker verification system? Technical report, Idiap Research Institute
16. Panjwani S, Prakash A (2014) Crowdsourcing attacks on biometric systems. In: Symposium on usable privacy and security (SOUPS 2014), pp 257–269
17. Hautamäki R, Kinnunen T, Hautamäki V, Laukkanen AM (2015) Automatic versus human speaker verification: the case of voice mimicry. Speech Commun 72:13–31
18. Ergunay S, Khoury E, Lazaridis A, Marcel S (2015) On the vulnerability of speaker verification to realistic voice spoofing. In: IEEE international conference on biometrics: theory, applications and systems, pp 1–8
19. Lindberg J, Blomberg M (1999) Vulnerability in speaker verification-a study of technical impostor techniques. Proceedings of the European conference on speech communication and technology 3:1211–1214
20. Villalba J, Lleida E (2010) Speaker verification performance degradation against spoofing and tampering attacks. In: FALA 10 workshop, pp 131–134

21. Wang ZF, Wei G, He QH (2011) Channel pattern noise based playback attack detection algorithm for speaker recognition. In: 2011 International conference on machine learning and cybernetics, vol 4, pp 1708–1713
22. Villalba J, Lleida E (2011) Preventing replay attacks on speaker verification systems. In: 2011 IEEE International Carnahan Conference on Security Technology (ICCST). IEEE, pp 1–8
23. Gałka J, Grzywacz M, Samborski R (2015) Playback attack detection for text-dependent speaker verification over telephone channels. Speech Commun 67:143–153
24. Taylor P (2009) Text-to-speech synthesis. Cambridge University Press
25. Klatt DH (1980) Software for a cascade/parallel formant synthesizer. J Acoust Soc Am 67:971–995
26. Moulines E, Charpentier F (1990) Pitch-synchronous waveform processing techniques for text-to-speech synthesis using diphones. Speech Commun 9:453–467
27. Hunt A, Black AW (1996) Unit selection in a concatenative speech synthesis system using a large speech database. In: Proceedings ICASSP, pp 373–376
28. Breen A, Jackson P (1998) A phonologically motivated method of selecting nonuniform units. In: Proceedings of ICSLP, pp 2735–2738
29. Donovan RE, Eide EM (1998) The IBM trainable speech synthesis system. In: Proceedings of ICSLP, pp 1703–1706
30. Beutnagel B, Conkie A, Schroeter J, Stylianou Y, Syrdal A (1999) The AT&T Next-Gen TTS system. In: Proceedigns of joint ASA, EAA and DAEA meeting, pp 15–19
31. Coorman G, Fackrell J, Rutten P, Coile B (2000) Segment selection in the L & H realspeak laboratory TTS system. In: Proceedings of ICSLP, pp 395–398
32. Yoshimura T, Tokuda K, Masuko T, Kobayashi T, Kitamura T (1999) Simultaneous modeling of spectrum, pitch and duration in HMM-based speech synthesis. In: Proceedings of Eurospeech, pp 2347–2350
33. Ling ZH, Wu YJ, Wang YP, Qin L, Wang RH (2006) USTC system for Blizzard Challenge 2006 an improved HMM-based speech synthesis method. In: Proceedings of the Blizzard challenge workshop
34. Black A (2006) CLUSTERGEN: a statistical parametric synthesizer using trajectory modeling. In: Proceedings of Interspeech, pp 1762–1765
35. Zen H, Toda T, Nakamura M, Tokuda K (2007) Details of the Nitech HMM-based speech synthesis system for the Blizzard challenge 2005. IEICE Trans Inf Syst E90-D(1):325–333
36. Zen H, Tokuda K, Black AW (2009) Statistical parametric speech synthesis. Speech Commun 51(11):1039–1064
37. Yamagishi J, Kobayashi T, Nakano Y, Ogata K, Isogai J (2009) Analysis of speaker adaptation algorithms for HMM-based speech synthesis and a constrained SMAPLR adaptation algorithm. IEEE Trans Speech Audio Lang Process **17**(1), 66–83 (2009)
38. Leggetter CJ, Woodland PC (1995) Maximum likelihood linear regression for speaker adaptation of continuous density hidden Markov models. Comput Speech Lang 9:171–185
39. Woodland PC (2001) Speaker adaptation for continuous density HMMs: a review. In: Proceedings of ISCA workshop on adaptation methods for speech recognition, p 119
40. Ze H, Senior A, Schuster M (2013) Statistical parametric speech synthesis using deep neural networks. In: Proceedings of ICASSP, pp 7962–7966
41. Ling ZH, Deng L, Yu D (2013) Modeling spectral envelopes using restricted boltzmann machines and deep belief networks for statistical parametric speech synthesis. IEEE Trans Audio Speech Lang Process 21(10):2129–2139
42. Fan Y, Qian Y, Xie FL, Soong F (2014) TTS synthesis with bidirectional LSTM based recurrent neural networks. In: Proceedings of Interspeech, pp 1964–1968
43. Zen H, Sak H (2015) Unidirectional long short-term memory recurrent neural network with recurrent output layer for low-latency speech synthesis. In: Proceedings of ICASSP, pp 4470–4474
44. Wu Z, King S (2016) Investigating gated recurrent networks for speech synthesis. In: Proceedings of ICASSP, pp 5140–5144 (2016)

45. Wang X, Takaki S, Yamagishi J (2016) Investigating very deep highway networks for parametric speech synthesis. In: 9th ISCA speech synthesis workshop, pp 166–171
46. Wang X, Takaki S, Yamagishi J (2018) Investigating very deep highway networks for parametric speech synthesis. Speech Commun 96:1–9
47. Wang X, Takaki S, Yamagishi J (2017) An autoregressive recurrent mixture density network for parametric speech synthesis. In: Proceedings of ICASSP, pp 4895–4899
48. Wang X, Takaki S, Yamagishi J (2017) An RNN-based quantized F0 model with multi-tier feedback links for text-to-speech synthesis. In: Proceedings of Interspeech, pp 1059–1063 (2017)
49. Saito, Y., Takamichi, S., Saruwatari, H.: Training algorithm to deceive anti-spoofing verification for DNN-based speech synthesis. In: Proc. ICASSP, pp 4900–4904 (2017)
50. Saito Y, Takamichi S, Saruwatari H (2018) Statistical parametric speech synthesis incorporating generative adversarial networks. IEEE/ACM Trans Audio Speech Lang Process 26(1):84–96
51. Kaneko T, Kameoka H, Hojo N, Ijima Y, Hiramatsu K, Kashino K (2017) Generative adversarial network-based postfilter for statistical parametric speech synthesis. In: Proceedings of ICASSP, pp 4910–4914
52. Van Oord D, Dieleman A, Zen S, Simonyan H, Vinyals K, Graves O, Kalchbrenner A, Senior N, Kavukcuoglu AK (2016) Wavenet: a generative model for raw audio. arXiv:1609.03499
53. Mehri S, Kumar K, Gulrajani I, Kumar R, Jain S, Sotelo J, Courville A, Bengio Y (2016) Samplernn: an unconditional end-to-end neural audio generation model. arXiv:1612.07837
54. Wang Y, Skerry-Ryan R, Stanton D, Wu Y, Weiss R, Jaitly N, Yang Z, Xiao Y, Chen Z, Bengio S, Le Q, Agiomyrgiannakis Y, Clark R, Saurous R (2017) Tacotron: towards end-to-end speech synthesis. In: Proceedings of Interspeech, pp 4006–4010
55. Gibiansky A, Arik S, Diamos G, Miller J, Peng K, Ping W, Raiman J, Zhou Y (2017) Deep voice 2: multi-speaker neural text-to-speech. In: Advances in neural information processing systems, pp 2966–2974
56. Shen J, Schuster M, Jaitly N, Skerry-Ryan R, Saurous R, Weiss R, Pang R, Agiomyrgiannakis Y, Wu Y, Zhang Y, Wang Y, Chen Z, Yang Z (2018) Natural tts synthesis by conditioning wavenet on mel spectrogram predictions. In: Proceedigns of ICASSP
57. King S (2014) Measuring a decade of progress in text-to-speech. Loquens 1(1):006
58. King S, Wihlborg L, Guo W (2017) The blizzard challenge 2017. In: Proceedings of Blizzard Challenge Workshop, Stockholm, Sweden
59. Foomany F, Hirschfield A, Ingleby M (2009) Toward a dynamic framework for security evaluation of voice verification systems. In: 2009 IEEE toronto international conference science and technology for humanity (TIC-STH), pp 22–27
60. Masuko T, Hitotsumatsu T, Tokuda K, Kobayashi T (1999) On the security of HMM-based speaker verification systems against imposture using synthetic speech. In: Proceedings of EUROSPEECH
61. Matsui T, Furui S (1995) Likelihood normalization for speaker verification using a phoneme- and speaker-independent model. Speech Commun 17(1–2):109–116
62. Masuko T, Tokuda K, Kobayashi T, Imai S (1996) Speech synthesis using HMMs with dynamic features. In: Proceedings of ICASSP
63. Masuko T, Tokuda K, Kobayashi T, Imai S (1997) Voice characteristics conversion for HMM-based speech synthesis system. In: Proceedings of ICASSP
64. De Leon PL, Pucher M, Yamagishi J, Hernaez I, Saratxaga I (2012) Evaluation of speaker verification security and detection of HMM-based synthetic speech. IEEE Trans Audio Speech Lang Process 20(8):2280–2290
65. Galou G (2011) Synthetic voice forgery in the forensic context: a short tutorial. In: Forensic speech and audio analysis working group (ENFSI-FSAAWG), pp 1–3
66. Cai W, Doshi A, Valle R (2018) Attacking speaker recognition with deep generative models. arXiv:1801.02384
67. Satoh T, Masuko T, Kobayashi T, Tokuda K (2001) A robust speaker verification system against imposture using an HMM-based speech synthesis system. In: Proceedings of Eurospeech (2001)

68. Chen LW, Guo W, Dai LR (2010) Speaker verification against synthetic speech. In: 2010 7th International symposium on Chinese spoken language processing (ISCSLP), pp 309–312
69. Quatieri TF (2002) Discrete-time speech signal processing: principles and practice. Prentice-Hall, Inc
70. Wu Z, Chng E, Li H (2012) Detecting converted speech and natural speech for anti-spoofing attack in speaker recognition. In: Proceedings of Interspeech
71. Ogihara A, Unno H, Shiozakai A (2005) Discrimination method of synthetic speech using pitch frequency against synthetic speech falsification. IEICE Trans Fund Electron Commun Comput Sci 88(1):280–286
72. De Leon P, Stewart B, Yamagishi J (2012) Synthetic speech discrimination using pitch pattern statistics derived from image analysis. In: Proceedings of Interspeech 2012. Portland, Oregon, USA
73. Stylianou Y (2009) Voice transformation: a survey. In: Proceedings of ICASSP, pp 3585–3588
74. Pellom B, Hansen J (1999) An experimental study of speaker verification sensitivity to computer voice-altered imposters. In: Proceedings of ICASSP, vol 2, pp 837–840
75. Mohammadi S, Kain A (2017) An overview of voice conversion systems. Speech Commun 88:65–82
76. Abe M, Nakamura S, Shikano K, Kuwabara H (1988) Voice conversion through vector quantization. In: Proceedigns of ICASSP, pp 655–658
77. Arslan L (1999) Speaker transformation algorithm using segmental codebooks (STASC). Speech Commun 28(3):211–226
78. Kain A, Macon M (1998) Spectral voice conversion for text-to-speech synthesis. In: Proceedings of ICASSP vol 1, pp 285–288
79. Stylianou Y, Cappé O, Moulines E (1998) Continuous probabilistic transform for voice conversion. IEEE Trans Speech Audio Process 6(2):131–142
80. Toda T, Black A, Tokuda K (2007) Voice conversion based on maximum-likelihood estimation of spectral parameter trajectory. IEEE Trans Audio Speech Lang Process 15(8):2222–2235
81. Kobayashi K, Toda T, Neubig G, Sakti S, Nakamura S (2014) Statistical singing voice conversion with direct waveform modification based on the spectrum differential. In: Proceedings of Interspeech
82. Popa V, Silen H, Nurminen J, Gabbouj M (2012) Local linear transformation for voice conversion. In: Proceedigns of ICASSP. IEEE, pp 4517–4520
83. Chen Y, Chu M, Chang E, Liu J, Liu R (2003) Voice conversion with smoothed GMM and MAP adaptation. In: Proceedings of EUROSPEECH, pp 2413–2416
84. Hwang HT, Tsao Y, Wang HM, Wang YR, Chen SH (2012) A study of mutual information for GMM-based spectral conversion. In: Proceedigns of Interspeech
85. Helander E, Virtanen T, Nurminen J, Gabbouj M (2010) Voice conversion using partial least squares regression. IEEE Trans Audio Speech Lang Process 18(5):912–921
86. Pilkington N, Zen H, Gales M (2011) Gaussian process experts for voice conversion. In: Proceedings of Interspeech
87. Saito D, Yamamoto K, Minematsu N, Hirose K (2011) One-to-many voice conversion based on tensor representation of speaker space. In: Proceedings of Interspeech, pp 653–656
88. Zen H, Nankaku Y, Tokuda K (2011) Continuous stochastic feature mapping based on trajectory HMMs. IEEE Trans Audio Speech Lang Process 19(2):417–430
89. Wu Z, Kinnunen T, Chng E, Li H (2012) Mixture of factor analyzers using priors from non-parallel speech for voice conversion. IEEE Signal Process Lett 19(12)
90. Saito D, Watanabe S, Nakamura A, Minematsu N (2012) Statistical voice conversion based on noisy channel model. IEEE Trans Audio Speech Lang Process 20(6):1784–1794
91. Song P, Bao Y, Zhao L, Zou C (2011) Voice conversion using support vector regression. Electron Lett 47(18):1045–1046
92. Helander E, Silén H, Virtanen T, Gabbouj M (2012) Voice conversion using dynamic kernel partial least squares regression. IEEE Trans Audio Speech Lang Process 20(3):806–817
93. Wu Z, Chng E, Li H (2013) Conditional restricted boltzmann machine for voice conversion. In: The first IEEE China summit and international conference on signal and information processing (ChinaSIP). IEEE

94. Narendranath M, Murthy H, Rajendran S, Yegnanarayana B (1995) Transformation of formants for voice conversion using artificial neural networks. Speech Commun 16(2):207–216
95. Desai S, Raghavendra E, Yegnanarayana B, Black A, Prahallad K (2009) Voice conversion using artificial neural networks. In: Proceedings of ICASSP. IEEE, pp 3893–3896
96. Saito Y, Takamichi S, Saruwatari H (2017) Voice conversion using input-to-output highway networks. IEICE Transactions on Inf Syst E100.D(8):1925–1928
97. Nakashika T, Takiguchi T, Ariki Y (2015) Voice conversion using RNN pre-trained by recurrent temporal restricted boltzmann machines. IEEE/ACM Trans Audio Speech Lang Process (TASLP) 23(3):580–587
98. Sun L, Kang S, Li K, Meng H (2015) Voice conversion using deep bidirectional long short-term memory based recurrent neural networks. In: Proceedings of ICASSP, pp 4869–4873
99. Sundermann D, Ney H (2003) VTLN-based voice conversion. In: Proceedings of the 3rd IEEE international symposium on signal processing and information technology, 2003. ISSPIT 2003. IEEE
100. Erro D, Moreno A, Bonafonte A (2010) Voice conversion based on weighted frequency warping. IEEE Trans Audio Speech Lang Process 18(5):922–931
101. Erro D, Navas E, Hernaez I (2013) Parametric voice conversion based on bilinear frequency warping plus amplitude scaling. IEEE Trans Audio Speech Lang Process 21(3):556–566
102. Hsu CC, Hwang HT, Wu YC, Tsao Y, Wang HM (2017) Voice conversion from unaligned corpora using variational autoencoding wasserstein generative adversarial networks. In: Proceedings of Interspeech, vol 2017, pp 3364–3368
103. Miyoshi H, Saito Y, Takamichi S, Saruwatari H (2017) Voice conversion using sequence-to-sequence learning of context posterior probabilities. Proceedings of Interspeech, vol 2017, pp 1268–1272
104. Fang F, Yamagishi J, Echizen I, Lorenzo-Trueba J (2018) High-quality nonparallel voice conversion based on cycle-consistent adversarial network. In: Proceedings of ICASSP 2018
105. Kobayashi K, Hayashi T, Tamamori A, Toda T (2017) Statistical voice conversion with wavenet-based waveform generation. In: Proceedings of Interspeech, pp 1138–1142
106. Gillet B, King S (2003) Transforming F0 contours. In: Proceedings of EUROSPEECH, pp 101–104 (2003)
107. Wu CH, Hsia CC, Liu TH, Wang JF (2006) Voice conversion using duration-embedded bi-HMMs for expressive speech synthesis. IEEE Trans Audio Speech Lang Process 14(4):1109–1116
108. Helander E, Nurminen J (2007) A novel method for prosody prediction in voice conversion. In: Proceedings of ICASSP, vol 4. IEEE, pp IV–509
109. Wu Z, Kinnunen T, Chng E, Li H (2010) Text-independent F0 transformation with non-parallel data for voice conversion. In: Proceedings of Interspeech
110. Lolive D, Barbot N, Boeffard O (2008) Pitch and duration transformation with non-parallel data. Speech Prosody 2008:111–114
111. Toda T, Chen LH, Saito D, Villavicencio F, Wester M, Wu Z, Yamagishi J (2016) The voice conversion challenge 2016. In: Proceedings of Interspeech, pp 1632–1636
112. Wester M, Wu Z, Yamagishi J (2016) Analysis of the voice conversion challenge 2016 evaluation results. In: Proceedings of Interspeech, pp 1637–1641
113. Perrot P, Aversano G, Blouet R, Charbit M, Chollet G (2005) Voice forgery using ALISP: indexation in a client memory. In: Proceedings of ICASSP, vol 1. IEEE, pp 17–20
114. Matrouf D, Bonastre JF, Fredouille C (2006) Effect of speech transformation on impostor acceptance. In: Proceedings of ICASSP, vol 1. IEEE, pp I–I
115. Kinnunen T, Wu Z, Lee K, Sedlak F, Chng E, Li H (2012) Vulnerability of speaker verification systems against voice conversion spoofing attacks: the case of telephone speech. In: Proceedings of ICASSP. IEEE, pp 4401–4404
116. Sundermann D, Hoge H, Bonafonte A, Ney H, Black A, Narayanan S (2006) Text-independent voice conversion based on unit selection. In: Proceedings of ICASSP, vol 1, pp I–I
117. Wu Z, Larcher A, Lee K, Chng E, Kinnunen T, Li H (2013) Vulnerability evaluation of speaker verification under voice conversion spoofing: the effect of text constraints. In: Proceedings of Interspeech, Lyon, France (2013)

118. Alegre F, Vipperla R, Evans N, Fauve B (2012) On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals. In: 2012 EURASIP conference on european conference on signal processing (EUSIPCO)
119. De Leon PL, Hernaez I, Saratxaga I, Pucher M, Yamagishi J (2011) Detection of synthetic speech for the problem of imposture. In: Proceedings of ICASSP, Dallas, USA, pp 4844–4847
120. Wu Z, Kinnunen T, Chng E, Li H, Ambikairajah E (2012) A study on spoofing attack in state-of-the-art speaker verification: the telephone speech case. In: Proceedings of Asia-Pacific signal information processing association annual summit and conference (APSIPA ASC). IEEE, pp 1–5
121. Alegre F, Vipperla R, Evans,N (2012) Spoofing countermeasures for the protection of automatic speaker recognition systems against attacks with artificial signals. In: Proceedings of Interspeech
122. Alegre F, Amehraye A, Evans N (2013) Spoofing countermeasures to protect automatic speaker verification from voice conversion. In: Proceedings of ICASSP
123. Wu Z, Xiao X, Chng E, Li H (2013) Synthetic speech detection using temporal modulation feature. In: Proceedings of ICASSP
124. Alegre F, Vipperla R, Amehraye A, Evans N (2013) A new speaker verification spoofing countermeasure based on local binary patterns. In: Proceedings of Interspeech, Lyon, France
125. Wu Z, Kinnunen T, Evans N, Yamagishi J, Hanilçi C, Sahidullah M, Sizov A (2015) ASVspoof 2015: the first automatic speaker verification spoofing and countermeasures challenge. In: Proceedings of Interspeech
126. Kinnunen T, Sahidullah M, Delgado H, Todisco M, Evans N, Yamagishi J, Lee K (2017) The ASVspoof 2017 challenge: assessing the limits of replay spoofing attack detection. In: INTERSPEECH
127. Wu Z, Khodabakhsh A, Demiroglu C, Yamagishi J, Saito D, Toda T, King S (2015) SAS: a speaker verification spoofing database containing diverse attacks. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)
128. Wu Z, Kinnunen T, Evans N, Yamagishi J (2014) ASVspoof 2015: automatic speaker verification spoofing and countermeasures challenge evaluation plan. http://www.spoofingchallenge.org/asvSpoof.pdf
129. Patel T, Patil H (2015) Combining evidences from mel cepstral, cochlear filter cepstral and instantaneous frequency features for detection of natural vs. spoofed speech. In: Proceedings of Interspeech
130. Novoselov S, Kozlov A, Lavrentyeva G, Simonchik K, Shchemelinin V (2016) STC anti-spoofing systems for the ASVspoof 2015 challenge. In: Proceedings of IEEE international conference on acoustics, speech, and signal processing (ICASSP), pp 5475–5479
131. Chen N, Qian Y, Dinkel H, Chen B, Yu K (2015) Robust deep feature for spoofing detection-the SJTU system for ASVspoof 2015 challenge. In: Proceedings of Interspeech
132. Xiao X, Tian X, Du S, Xu H, Chng E, Li H (2015) Spoofing speech detection using high dimensional magnitude and phase features: the NTU approach for ASVspoof 2015 challenge. In: Proceedings of Interspeech
133. Alam M, Kenny P, Bhattacharya G, Stafylakis T (2015) Development of CRIM system for the automatic speaker verification spoofing and countermeasures challenge 2015. In: Proceedings of Interspeech
134. Wu Z, Yamagishi J, Kinnunen T, Hanilçi C, Sahidullah M, Sizov A, Evans N, Todisco M, Delgado H (2017) Asvspoof: the automatic speaker verification spoofing and countermeasures challenge. IEEE J Sel Top Signal Process 11(4):588–604
135. Delgado H, Todisco M, Sahidullah M, Evans N, Kinnunen T, Lee K, Yamagishi J (2018) ASVspoof 2017 version 2.0: meta-data analysis and baseline enhancements. In: Proceedings of Odyssey 2018 the speaker and language recognition workshop, pp 296–303
136. Todisco M, Delgado H, Evans N (2016) A new feature for automatic speaker verification anti-spoofing: constant Q cepstral coefficients. In: Proceedings of Odyssey: the speaker and language recognition workshop, Bilbao, Spain, pp 283–290

137. Todisco M, Delgado H, Evans N (2017) Constant Q cepstral coefficients: a spoofing countermeasure for automatic speaker verification. Comput Speech Lang 45:516–535
138. Lavrentyeva G, Novoselov S, Malykh E, Kozlov A, Kudashev O, Shchemelinin V (2017) Audio replay attack detection with deep learning frameworks. In: Proceedings of Interspeech, pp 82–86
139. Ji Z, Li Z, Li P, An M, Gao S, Wu D, Zhao F (2017) Ensemble learning for countermeasure of audio replay spoofing attack in ASVspoof2017. In: Proceedings of Interspeech, pp 87–91
140. Li L, Chen Y, Wang D, Zheng T (2017) A study on replay attack and anti-spoofing for automatic speaker verification. In: Proceedings of Interspeech, pp 92–96
141. Patil H, Kamble M, Patel T, Soni M (2017) Novel variable length teager energy separation based instantaneous frequency features for replay detection. In: Proceedings of Interspeech, pp 12–16
142. Chen Z, Xie Z, Zhang W, Xu X (2017) ResNet and model fusion for automatic spoofing detection. In: Proceedings of Interspeech, pp 102–106
143. Wu Z, Gao S, Cling E, Li H (2014) A study on replay attack and anti-spoofing for text-dependent speaker verification. In: Proceedings of Asia-Pacific signal information processing association annual summit and conference (APSIPA ASC). IEEE, pp 1–5
144. Li Q (2009) An auditory-based transform for audio signal processing. In: 2009 IEEE workshop on applications of signal processing to audio and acoustics. IEEE, pp 181–184
145. Davis S, Mermelstein P (1980) Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences. IEEE Trans Acoust Speech Signal Process 28(4):357–366
146. Sahidullah M, Kinnunen T, Hanilçi C (2015) A comparison of features for synthetic speech detection. In: Proceedings of Interspeech. ISCA, pp 2087–2091
147. Brown J (1991) Calculation of a constant Q spectral transform. J Acoust Soc Am 89(1):425–434
148. Alam M, Kenny P (2017) Spoofing detection employing infinite impulse response—constant Q transform-based feature representations. In: Proceedings of European signal processing conference (EUSIPCO)
149. Cancela P, Rocamora M, López E (2009) An efficient multi-resolution spectral transform for music analysis. In: Proceedings of international society for music information retrieval conference, pp 309–314
150. Bengio Y (2009) Learning deep architectures for AI. Found Trends Mach Learn 2(1):1–127
151. Goodfellow I, Bengio Y, Courville A, Bengio Y (2016) Deep learning. MIT Press, Cambridge
152. Tian Y, Cai M, He L, Liu J (2015) Investigation of bottleneck features and multilingual deep neural networks for speaker verification. In: Proceedings of Interspeech, pp 1151–1155
153. Richardson F, Reynolds D, Dehak N (2015) Deep neural network approaches to speaker and language recognition. IEEE Signal Process Lett 22(10):1671–1675
154. Hinton G, Deng L, Yu D, Dahl GE, Mohamed RA, Jaitly N, Senior A, Vanhoucke V, Nguyen P, Sainath TN, Kingsbury B (2012) Deep neural networks for acoustic modeling in speech recognition: the shared views of four research groups. IEEE Signal Process Mag 29(6):82–97
155. Alam M, Kenny P, Gupta V, Stafylakis T (2016) Spoofing detection on the ASVspoof2015 challenge corpus employing deep neural networks. In: Proceedings of Odyssey: the Speaker and Language Recognition Workshop, Bilbao, Spain, pp 270–276
156. Qian Y, Chen N, Yu K (2016) Deep features for automatic spoofing detection. Speech Commun 85:43–52
157. Yu H, Tan ZH, Zhang Y, Ma Z, Guo J (2017) DNN filter bank cepstral coefficients for spoofing detection. IEEE Access 5:4779–4787
158. Sriskandaraja K, Sethu V, Ambikairajah E, Li H (2017) Front-end for antispoofing countermeasures in speaker verification: scattering spectral decomposition. IEEE J Sel Top Signal Process 11(4):632–643. https://doi.org/10.1109/JSTSP.2016.2647202
159. Andén J, Mallat S (2014) Deep scattering spectrum. IEEE Trans Signal Process 62(16):4114–4128
160. Mallat S (2012) Group invariant scattering. Commun Pure Appl Math 65:1331–1398

161. Pal M, Paul D, Saha G (2018) Synthetic speech detection using fundamental frequency variation and spectral features. Comput Speech Lang 48:31–50
162. Laskowski K, Heldner M, Edlund J (2008) The fundamental frequency variation spectrum. Proc FONETIK 2008:29–32
163. Saratxaga I, Sanchez J, Wu Z, Hernaez I, Navas E (2016) Synthetic speech detection using phase information. Speech Commun 81:30–41
164. Wang L, Nakagawa S, Zhang Z, Yoshida Y, Kawakami Y (2017) Spoofing speech detection using modified relative phase information. IEEE J Sel Top Signal Process 11(4):660–670
165. Chakroborty S, Saha G (2009) Improved text-independent speaker identification using fused MFCC & IMFCC feature sets based on Gaussian filter. Int J Signal Process 5(1):11–19
166. Wu X, He R, Sun Z, Tan T (2018) A light CNN for deep face representation with noisy labels. IEEE Trans Inf Forensics Secur 13(11):2884–2896
167. Goncalves AR, Violato RPV, Korshunov P, Marcel S, Simoes FO (2017) On the generalization of fused systems in voice presentation attack detection. In: 2017 International conference of the biometrics special interest group (BIOSIG), pp 1–5. https://doi.org/10.23919/BIOSIG.2017.8053516
168. Paul D, Pal M, Saha G (2016) Novel speech features for improved detection of spoofing attacks. In: Proceedings of annual IEEE India conference (INDICON)
169. Dehak N, Kenny P, Dehak R, Dumouchel P, Ouellet P (2011) Front-end factor analysis for speaker verification. IEEE Trans Audio Speech Lang Process 19(4):788–798
170. Khoury E, Kinnunen T, Sizov A, Wu Z, Marcel S (2014) Introducing i-vectors for joint anti-spoofing and speaker verification. In: Proceedings of Interspeech
171. Sizov A, Khoury E, Kinnunen T, Wu Z, Marcel S (2015) Joint speaker verification and antispoofing in the i-vector space. IEEE Trans Inf Forensics Secur 10(4):821–832
172. Hanilçi C (2018) Data selection for i-vector based automatic speaker verification anti-spoofing. Digit Signal Process 72:171–180
173. Tian X, Wu Z, Xiao X, Chng E, Li H (2016) Spoofing detection from a feature representation perspective. In: Proceedings of IEEE international conference on acoustics, speech, and signal processing (ICASSP), pp 2119–2123
174. Yu H, Tan ZH, Ma Z, Martin R, Guo J (2018) Spoofing detection in automatic speaker verification systems using dnn classifiers and dynamic acoustic features. IEEE Trans Neural Netw Learn Syst PP(99):1–12
175. Dinkel H, Chen N, Qian Y, Yu K (2017) End-to-end spoofing detection with raw waveform cldnns. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), pp 4860–4864
176. Sainath T, Weiss R, Senior A, Wilson K, Vinyals O (2015) Learning the speech front-end with raw waveform CLDNNs. In: Proceedigns of Interspeech
177. Zhang C, Yu C, Hansen JHL (2017) An investigation of deep-learning frameworks for speaker verification antispoofing. IEEE J Sel Top Signal Process 11(4):684–694
178. Muckenhirn H, Magimai-Doss M, Marcel S (2017) End-to-end convolutional neural network-based voice presentation attack detection. In: 2017 IEEE international joint conference on biometrics (IJCB), pp 335–341
179. Chen S, Ren K, Piao S, Wang C, Wang Q, Weng J, Su L, Mohaisen A (2017) You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones. In: 2017 IEEE 37th international conference on distributed computing systems (ICDCS). IEEE, pp 183–195
180. Shiota S, Villavicencio F, Yamagishi J, Ono N, Echizen I, Matsui T (2015) Voice liveness detection algorithms based on pop noise caused by human breath for automatic speaker verification. In: Proceedings of Interspeech
181. Shiota S, Villavicencio F, Yamagishi J, Ono N, Echizen I, Matsui T (2016) Voice liveness detection for speaker verification based on a tandem single/double-channel pop noise detector. In: ODYSSEY
182. Sahidullah M, Thomsen D, Hautamäki R, Kinnunen T, Tan ZH, Parts R, Pitkänen M (2018) Robust voice liveness detection and speaker verification using throat microphones. IEEE/ACM Trans Audio Speech Lang Process 26(1):44–56

183. Elko G, Meyer J, Backer S, Peissig J (2007) Electronic pop protection for microphones. In: 2007 IEEE workshop on applications of signal processing to audio and acoustics. IEEE, pp 46–49

184. Zhang L, Tan S, Yang J, Chen Y (2016) Voicelive: a phoneme localization based liveness detection for voice authentication on smartphones. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, pp 1080–1091

185. Zhang L, Tan S, Yang J (2017) Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. ACM, pp 57–71

186. Hanilçi C, Kinnunen T, Sahidullah M, Sizov A (2016) Spoofing detection goes noisy: an analysis of synthetic speech detection in the presence of additive noise. Speech Commun 85:83–97

187. Yu H, Sarkar A, Thomsen D, Tan ZH, Ma Z, Guo J (2016) Effect of multi-condition training and speech enhancement methods on spoofing detection. In: Proceedings of international workshop on sensing, processing and learning for intelligent machines (SPLINE)

188. Tian X, Wu Z, Xiao X, Chng E, Li H (2016) An investigation of spoofing speech detection under additive noise and reverberant conditions. In: Proceedings of Interspeech (2016)

189. Delgado H, Todisco M, Evans N, Sahidullah M, Liu W, Alegre F, Kinnunen T, Fauve B (2017) Impact of bandwidth and channel variation on presentation attack detection for speaker verification. In: 2017 International conference of the biometrics special interest group (BIOSIG), pp 1–6

190. Qian Y, Chen N, Dinkel H, Wu Z (2017) Deep feature engineering for noise robust spoofing detection. IEEE/ACM Trans Audio Speech Lang Process 25(10):1942–1955

191. Korshunov P, Marcel S (2016) Cross-database evaluation of audio-based spoofing detection systems. In: Proceedings of Interspeech

192. Paul D, Sahidullah M, Saha G (2017) Generalization of spoofing countermeasures: a case study with ASVspoof 2015 and BTAS 2016 corpora. In: Proceedigns of IEEE international conference on acoustics, speech, and signal processing (ICASSP). IEEE pp 2047–2051

193. Lorenzo-Trueba J, Fang F, Wang X, Echizen I, Yamagishi J, Kinnunen T (2018) Can we steal your vocal identity from the Internet?: Initial investigation of cloning Obama's voice using GAN, WaveNet and low-quality found data. In: Proceedings of Odyssey: the speaker and language recognition workshop

194. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial nets. In: Advances in neural information processing systems, pp 2672–2680

195. Kreuk F, Adi Y, Cisse M, Keshet J (2018) Fooling end-to-end speaker verification by adversarial examples. arXiv:1801.03339

196. Sahidullah M, Delgado H, Todisco M, Yu H, Kinnunen T, Evans N, Tan ZH (2016) Integrated spoofing countermeasures and automatic speaker verification: an evaluation on ASVspoof 2015. In: Proceedings of Interspeech

197. Muckenhirn H, Korshunov P, Magimai-Doss M, Marcel S (2017) Long-term spectral statistics for voice presentation attack detection. IEEE/ACM Trans Audio Speech Lang Process 25(11):2098–2111

198. Sarkar A, Sahidullah M, Tan ZH, Kinnunen T (2017) Improving speaker verification performance in presence of spoofing attacks using out-of-domain spoofed data. In: Proceedings of Interspeech

199. Kinnunen T, Lee K, Delgado H, Evans N, Todisco M, Sahidullah M, Yamagishi J, Reynolds D (2018) t-DCF: a detection cost function for the tandem assessment of spoofing countermeasures and automatic speaker verification. In: Proceedings of Odyssey: the speaker and language recognition workshop

200. Todisco M, Delgado H, Lee K, Sahidullah M, Evans N, Kinnunen T, Yamagishi J (2018) Integrated presentation attack detection and automatic speaker verification: common features and Gaussian back-end fusion. In: Proceedings of Interspeech

201. Wu Z, De Leon P, Demiroglu C, Khodabakhsh A, King S, Ling ZH, Saito D, Stewart B, Toda T, Wester M, Yamagishi Y (2016) Anti-spoofing for text-independent speaker verification: an initial database, comparison of countermeasures, and human performance. IEEE/ACM Trans Audio Speech Lang Process 24(4):768–783