JOURNAL OF APPLIED INTELLIGENT SYSTEMS & INFORMATION SCIENCES
VOL. 2, ISSUE 2, PP. 33-46, DECEMBER 2021.
Available at: www.journal.research.fanap.com
DOI: https://doi.org/10.22034/JAISIS.2021.311114.1036

A REVIEW ON BIOMETRIC AUTHENTICATION AND PRESENTATION ATTACK DETECTION IN BIOMETRIC SYSTEMS

Fereshteh Shabany Moghadam [1,*], Abbas Ahmadi [1]

[1]*Department of Industrial Engineering, Amir-Kabir University of Technology, Tehran, Iran*

ABSTRACT

Biometric authentication has become a topic of interest ever since there appeared to be a movement toward digital life. However, recent issues regarding social distancing and pandemic control have acted like a catalyst for biometric authentication systems. The majority of companies and organizations accelerated their digital transition journey and tried to provide remote services. Meanwhile, high security digital authentication has become a controversial issue. This paper will present an integrated overview on basic to complicated concepts in biometric systems. Different types of biometric systems, information fusion approaches, spoofing and liveness, and performance evaluation in these systems will be discussed. With respect to the significant importance of anti-spoofing approaches on the reliability of biometric systems, a considerable emphasis is placed on this issue. This review represents the fact that despite all progress made in biometric systems development, unseen attack detection is still a vexing issue in this domain. Cutting edge research paths will be introduced in each topic and an interested reader can, hopefully, find interesting research areas for further study.

***KEYWORDS*:** Digital Authentication, Liveness Detection, Multi-modal Biometric system, Multi biometric systems, Anti-Spoofing

1. INTRODUCTION

Biometrics is the branch of science involved with an individual's identification and verification according to her/ his physiological and behavioral identifiers (Dargan & Kumar, 2020). These traits are unique for every individual so can be considered as a fair reference to precisely distinguish people from each other, examples of which are: Face, palm print, iris, retina, fingerprint, voice, signature, gait, hand geometry, handwriting, ECG, and brain print (Dargan & Kumar, 2020; Murillo-Escobar et al., 2015; Venkatraman, 2009). With regard to invasive developments in information technology and the universal movement toward smart life, biometric systems performing identification/ verification have become very popular (Dargan & Kumar, 2020; Salama AbdElminaam et al., 2020). These systems, basically considered as pattern recognition systems, can be very helpful in smart government and can play a shining role in smart cities development (Dargan & Kumar, 2020; Venkatraman, 2009). Global biometric technologies market revenue is envisaged to hit 55 billion dollars in 2027 (Statista, 2021).

Biometric systems can be categorized into unimodal and multimodal biometric systems (Dargan & Kumar, 2020). Unimodal systems use a single biometric trait of the individual for identification and verification, while multimodal biometric systems use or are capable of using a combination of two or more biometric modalities

* *Corresponding Author, Email: f.sh.m@aut.ac.ir*

RECEIVED: 10 OCTOBER, 2021; **ACCEPTED**: 17 NOVEMBER, 2021; **PUBLISHED ONLINE**: 18 NOVEMBER, 2021

to identify an individual. The framework of biometric systems consists of a sequence of actions including: storing input biometric data, pre-processing, finding area of interest, feature extraction, matching module, and decision module (Dargan & Kumar, 2020; Murillo-Escobar et al., 2015). Apart from all points that biometric systems have brought into the technology-focused life, they can be targeted by several attacks including: representing fake biometric, resubmitting the pre-recorded and pre-stored signals, and overriding and compromising (Dargan & Kumar, 2020). Accordingly, the reliability of biometric systems is of immense value and it should safeguard against any spoofing attack or imposter (Dargan & Kumar, 2020; Fernandes & Bala, 2016). Doing so is mainly addressed by liveness detection in the literature(Dargan & Kumar, 2020). Liveness detection refers to the procedure to assess the liveness of the submitting biometric trait in a biometric system to see if an authorized person is using the system or not (Joshi & Singh, 2013). Face spoofing, for instance, occurs when an attacker tries to fool the facial recognition system by submitting a photo, pre-recorded video, or using a mask (Joshi & Singh, 2013). Several ways are applied to protect a biometric system against these attacks which will be discussed later.

With regard to the ever-rising importance of digital authentication systems in digital life, biometric systems have become a topic of interest during recent decades and a considerable amount of research has been dedicated to this field of study. This includes several review papers each of which addressed a special issue in their survey. This work attempts to shed some light on the most important research paths in this area while providing the reader with the basic knowledge and main structure of biometric systems. Hence, not only does this work provide a good resource for being familiar with fundamental issues of biometric authentication. But it also provides a comprehensive review on the most important research trends in information fusion, and presentation attack detection (anti-spoofing). Deep learning approaches, cloud-based and fog computing, as well as Generative Adversarial Networks (GANs) (Wang et al., 2020) are believed to be game changers for ensuring both reliability and applicability of biometric authentication in terms of generalization and unseen attack detection.

Main concepts of biometric systems and their different types, different approaches of information fusion in biometric systems, the concept of spoofing, liveness check approaches, and performance evaluation in these systems will be discussed in the rest of the paper. In each case, the most recent research routes will be introduced to pave the way for further study and research in this domain. Thus, a considerable attention is placed on information fusion and spoof detection, due to their shiny role in any biometric system's reliability. Finally, the discussion and conclusion section, will shed some light on the possible research paths in this domain while wrapping up the discussed issues.

2. BIOMETRIC SYSTEMS OVERVIEW

Fundamental issues about biometric systems necessary to have a good grasp of this field of research, will be presented in this section. Biometric systems' concepts, types, and framework will be discussed first. Then, multi biometric systems and their different types will be elaborated. Playing a significant role in biometric systems' reliability and precision, information fusion would be the forthcoming subject.
In each topic, the most recent research which can best signify the research path in that context will be introduced.

2.1. Biometric systems

Biometrics refers to identifying an individual according to her/ his specific physiological or behavioral characteristics with the ability to precisely differentiate between a genuine person and an imposter (Rubab & Mir, 2011). A biometric system is defined as a system acquiring biometric data, extracting and storing the required feature sets and then comparing and matching it with a predefined authorized dataset (Rubab & Mir, 2011). This procedure can be applied to person verification or person identification with regard to the application context (Rubab & Mir, 2011). Although these concepts may be used interchangeably in some references, the former refers to when a person asks for identification while the latter requires no personal claim (Li et al., 2017; Rubab & Mir, 2011). In fact, verification, normally, provides a matching score between input data and templates stored in the database; this matching score ranges from 0% to almost 100% (El-Abed et al.,2012). However,

what identification does is determine the identity of an unknown individual from a database of individuals through attributing the most similar profile/ profiles or rejecting the individual (El-Abed et al., 2012).

Several types of biometrics have been defined, since the first time this concept was initiated about two decades ago (Rubab & Mir, 2011). Some of which have become a general criterion for digital authentication while others are still in the early development stages. Fingerprint and face are by far the most prevalent biometrics have ever been used and, somehow, have become the part and parcel of smart life in some developed countries (Rubab & Mir, 2011; Venkatraman, 2009). The application can be seen in access control, border security, law enforcement, surveillance systems, and financial gadgets, to name but a few (Abdullakutty et al., 2021). Fingerprint has come out to be a reliable personal verification at the lowest price but recent universal pandemics have worked as a catalyst for face biometrics; since it may well make it easier to control the virus spread rate and observe social distancing rules. As a result, ever since a lion's share of research has been devoted to the face recognition field of study and several algorithms have been proposed to enhance the precision and reliability of this biometric in a wide range of applications (Ltd., 2019; Salama AbdElminaam et al., 2020).

Other biometrics, on the other hand, are: iris, hand geometrics, palmprint, voice, signature, ear shape, knuckle crease, DNA, gait, electroencephalogram (EEG), and electrocardiogram (ECG); among which the four latter are on the edge of research and are not totally applicable, yet (Conti et al., 2007; El-Abed et al., 2012; Rubab & Mir, 2011). Universality, uniqueness, permanency, collectability, and acceptability can best describe required characteristics of an ideal biometric trait (El-Abed et al., 2012). EI-Abed et al. (2012) compared different biometric information in terms of the mentioned properties in (El-Abed et al., 2012). An overall description on how a biometric system generally works, is provided in the next subsection.

2.2. Framework

The basic structure of a biometric system for either verification or identification consists of five primary elements: User Interface/ capture module, Signal processor/ Feature extractor, Database, Matcher, and Decision module (El-Abed et al., 2012; Ltd., 2019); meaning that each biometric-based authentication is carried in four essential levels namely, Enrollment, Preprocessing, Feature Extraction, and Authentication or Matching (Malarvizhi et al., 2020). The following figure depicts the generic architecture of a biometric system (Fig. 1). What happens in a biometric system can be, shortly, narrated as follows (El-Abed et al., 2012; Ltd., 2019; Malarvizhi et al., 2020): raw biometric data is extracted into numerical representation via the capture module. A preprocessing, then, would be performed to reduce the numerical representation and find the area of interest, by the signal processing module. After that, the optimized information would be stored as the biometric templates in the storage module. The matcher compares, next, determines the degree of similarity between

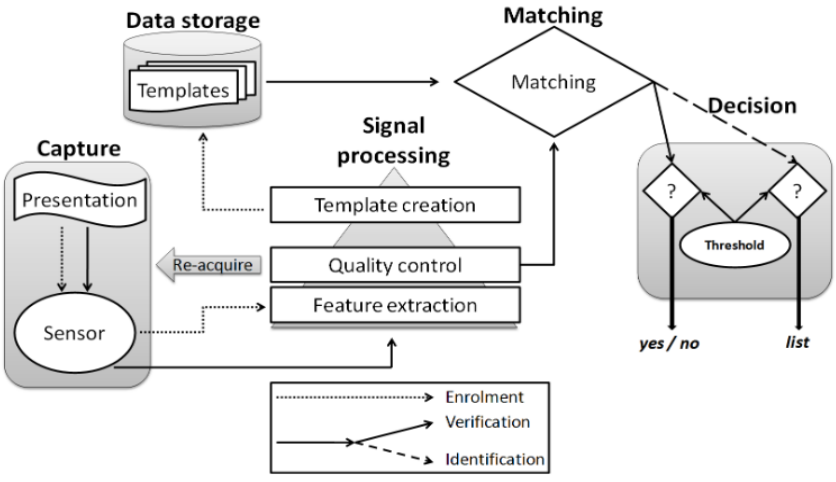

Fig. 1. Generic architecture of a biometric system (El-Abed et al., 2012)

inputs and the stored templates. The final decision on approving the identity of a person or not, would be made based upon the thresholds defined in the decision module.

2.3. Multi biometric systems

Biometric systems are categorized into unimodal and multimodal biometric systems, according to whether they apply a single source of biometric or more than once (Dargan & Kumar, 2020; Rubab & Mir, 2011). Not being dependent to only one source of data, multimodal biometric systems are believed to alleviate concerns like non-universality[1], sensitivity to noise and spoofing, inter-class similarities, and intra-class variations (Conti et al., 2007; Malarvizhi et al., 2020; Rubab & Mir, 2011). Multi biometric systems can be classified into 6 categories according to the nature of the sources of the employed biometric information: multi-sensor, multi-algorithm, multi-instance, multi-sample, multimodal, and hybrid (Ross A., 2008; Rubab & Mir, 2011).

I. Multi-sensor systems

Multiple sensors are employed to capture information of a single type of personal biometric (Ross A., 2008). This can result in higher recognition ability of the biometric system when it is applied correctly (Dargan & Kumar, 2020; Ross A., 2008); successful examples of which can be seen in using an infra-red sensor with a visible-light sensor to provide the face subsurface information or using both 2D and 3D face matching information (Ross A., 2008).

II. Multi-algorithm systems

In some cases, applying more than one algorithm for feature extraction and/ or matching modules can add up to the reliability of the biometric system by providing the system with more information (Dargan & Kumar, 2020; Ross A., 2008). This requires no excessive cost to add other sensors so it can be considered as a cost-efficient way to enhance the system's precision. For instance, according to experimental research, ensemble classifiers are of significant impact in bolstering the identification rate in facial biometric systems (Ross A., 2008).

III. Multi-instance systems

In this case, multiple biometric instances of each individual (for example, both right and left index fingers, to name but a few) will be applied for verification, at the same time (Ross A., 2008). Only when multi-unit/ multi-instance data can be acquired via the same sensor, maywell this approach be cost-effective (Ross A., 2008).

IV. Multi-sample systems

To reduce intra-class variation and complete representation of a trait, a viable solution would be to acquire multiple samples of a biometric trait via the same sensor (Dargan & Kumar, 2020; Ross A., 2008). Multiple dab prints to save images of different areas of fingerprint can best signify this approach (Ross A., 2008). What should be determined in doing so are: number of samples as well as the policy to select the optimal subset best representing the user's biometric; clustering and similarity measurement are believed to be the most popular approaches to find the template which best describes the intra-class variation (Ross A., 2008).

V. Multi-modal systems

Multiple biometric traits will be applied to enhance the reliability and precision of the biometric system, in this case. Clearly, the more uncorrelated traits (for example iris data vs voice, or fingerprint vs face biometric, to name but a few), the more reliable biometric system (Li et al., 2017; Malarvizhi et al., 2020; Ross A., 2008). The cost of adding new sensors, hence, is unavoidable in this approach. Although increasing the number of

[1]Every biometric feature is believed to be universal, but in some people may not own them for some physical invalidity (lack of a finger or the voice) (Conti et al., 2007)

traits may well lead to higher system performance, the curse of dimensionality is an important factor that should be considered, smartly (Ross A., 2008).

VI. Hybrid systems

If any subset of the aforementioned approaches is applied, it is called a hybrid scenario (Ross A., 2008). Both soft and primary biometric traits may be used in this case, with respect to the application context as well as the required accuracy level (Dargan & Kumar, 2020; Ross A., 2008). Soft biometrics refer to biometric traits that are not different enough to be efficient in identifying a person but considering them alongside primary traits can lead to the system becoming more reliable (Dargan & Kumar, 2020; Ross A., 2008). Examples of soft biometrics can be seen in gender, height, weight, and eye color, to name a few (Ross A., 2008). These factors can be also efficient in database filtering/ indexing; for instance, feature "Asian female" can speed up the search engine in finding the matching fingerprint compared to when only finger trait is defined for the system (Ross A., 2008).

The forthcoming subsection will elaborate on how any type of the aforementioned biometric systems can use the provided data to make a decision about the users' identity.

2.4. Information fusion

To efficiently use information provided by biometric traits and improve the system accuracy, it is necessary to apply an effective fusion scheme (Rubab & Mir, 2011). Fusion levels were categorized into two main groups, by Sanderson & Paliwal, (2004); pre-classification and post-classification. The former refers to fusion at raw data and features while the latter refers to fusion at the match score, rank, and decision level occurring after the matcher has been invoked (Sanderson & Paliwal, 2004).Fig. 2 represents both categories and their subset approaches including fusion at the sensor level, feature extraction level, matching score level, ranking level, and decision level (de Luis-García et al., 2003; Ross A., 2008; Rubab & Mir, 2011).

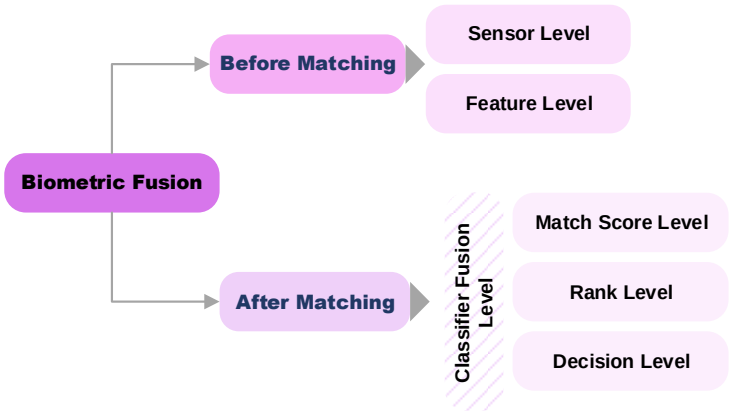

Fig. 2. Levels of fusion in a biometric system

- Sensor level fusion

The input biometric data would be improved by managing any type of noise which degrades the system reliability, like non-uniform illumination, and background clutter, to name a few, in this fusion level (Rubab & Mir, 2011). This input data can be obtained by either multiple sensors or a single sensor (Rubab & Mir, 2011).

- Feature level fusion

In this fusion level, a set of feature normalization, transformation, and reduction schemes will be applied to make an integrated feature set out of all feature sets obtained from different biometrics (Rubab & Mir, 2011). This may well result in detecting correlated features and dimensionality reduction, leading to the accuracy level enhancement. In doing so, incompatibility in feature sets of multi-modality and curse of dimensionality would be main challenges that should be considered intelligently (Li et al., 2017; Rubab & Mir, 2011).

Feature normalization is one of the important tasks that should be covered in this level, referring to alleviate possible diversities among data features in terms of range and type, using a wide range of proper approaches (Rubab & Mir, 2011). For further information about the importance of the normalization in biometric systems and score normalization methods, the interested reader can refer to (Moutafis & Kakadiaris, 2016).

When matching has been accomplished, there are two main approaches to match score fusion (Aizi & Ouslim, 2019): combination approach and classification approach. The former refers to making the final decision based upon a single match score obtained by combining all different match scores generated by the biometric system (Aizi & Ouslim, 2019; Ross A., 2008). The classification approach, on the other hand, deals with this problem as a classification problem. There are three fusion levels in classification approach which will be discussed in the following (Ross A., 2008).

- Classifier-based fusion schemes

After matchers generate related scores for the input data, the verification mode involves a classification task to determine whether the match scores represent a genuine class or a fake one (Abhishek Jana, 2020; Rubab & Mir, 2011). A wide range of classifiers have been applied to biometric domain to facilitate this, ranging from k-Nearest Neighbor to very sophisticated Convolutional Neural Networks (Abhishek Jana, 2020; Rubab & Mir, 2011). To name one of the most recent works in this area, we can refer to Aizi & Ouslim, (2019) that used a combination of a decision tree and fuzzy logic models to classify the interest zones in the score ranges in a multi-modal biometric system (iris and fingerprint). They defined the zones of interest using the K-means clustering approach (Aizi & Ouslim, 2019). Recent research has been gravitated toward using advanced soft computing in techniques such as metaheuristics and fuzzy logic to combine matching scores in the multimodal biometric systems (Alpar, 2015; Malarvizhi et al., 2020). Malarvizhi et al. (2020), as a shiny example of the most recent work in this regard, proposed a hybrid soft computing based optimization approach for fusion enhancement in a multimodal biometric system (Malarvizhi et al., 2020). They applied both genetic algorithm and fuzzy logic to assure high standards of verification in a multimodal biometric system based on iris and fingerprint data (Malarvizhi et al., 2020).

(Jana et al. 2020), also, combined fuzzy logic and Artificial Neural Networks (ANNs) to facilitate using several classification approaches in data fusion to enhance the reliability of biometric systems (Abhishek Jana et al., 2020).

Although using soft computing methods and complicated Machine Learning techniques can surely add value to the precision of biometric systems and digital authentication, there has always been a controversy around the massive CPU they require(Salama AbdElminaam et al., 2020). This, hence, has led to working in a distributed environment becoming an ever-rising topic of interest in this area(Salama AbdElminaam et al., 2020). Edge computing, fog computing, and cloud computing are believed to bring a workable remedy to cope with this challenge(Salama AbdElminaam et al., 2020). (AbdELminaam et al. 2020) presented an interesting work in this line of research that an interested reader may find inspiring(Salama AbdElminaam et al., 2020). They applied Transfer Learning in Fog Computing to develop a highly precise deep face recognition system (Salama AbdElminaam et al., 2020). Their solution has faced several challenges in face recognition, in terms of precision and reliability at a reasonable speed and in near real-time (Salama AbdElminaam et al., 2020).Table 1 provides a brief review of the discussed works regarding classifier-based fusion sechemes.

Posing a real threat to the biometric system's reliability, spoofing attack detection will be elaborated in the following section. Being a significant factor in biometric systems' reliability, precision, and generalization, spoofing and presentation attack detection is the forthcoming subject. Then, to shed some light on how to characterize the performance in authentication systems, biometric systems evaluation will be discussed shortly.

3. Spoofing and Presentation Attack Detection

As mentioned before, Enrollment, Preprocessing, Feature Extraction, and Authentication or Matching are main modules of every biometric system (Malarvizhi et al., 2020). Although each module is of high importance in the system's well-functioning, the latter is believed to be by far the most delicate factor in the biometrics

Table 1. Articles related to classifier-based fusion schemes

Article	Main approach		Detailed approach
	Soft computing	Distributed environment	
(Aizi & Ouslim, 2019)	✓	×	A combination of decision tree and fuzzy logic models
(Malarvizhi et al., 2020)	✓	×	Hybrid soft computing-based optimization approach
(Abhishek Jana, 2020)	✓	×	A combination of fuzzy logic and Artificial Neural Networks
(Salama AbdElminaam et al., 2020)	×	✓	Transfer Learning in Fog Computing

systems' reliability, especially nowadays that these systems are becoming a part and parcel of daily life (Dargan & Kumar, 2020; El-Abed et al., 2012). Since the more such systems become prevalent, the more online crimes would be expected. Almost all biometric systems can be a target of spoof attacks but being the most popular biometrics, fingerprint and face biometrics have been highly prone to this issue (Malarvizhi et al., 2020). Spoofing refers to when an impostor attempts to mimic the traits used to identify/ verify a genuine person in a biometric system and is refered as Presentation Attack (PA) in the literature(Abdullakutty et al., 2021; Ross A., 2008). PAs are classified into 2D and 3D attacks in which the former includes presenting flat printed photos, digital photos, eye-cut photos, wrapped photos, and pre-recorded videos, while the latter includes mask attacks. In fact, 3D masks can be considered as an improved version of photo attacks which can be seen in different types of materials, either rigid or flexible(Abdullakutty et al., 2021). A simple graphical sample of how a facial biometric system can work against different types of PAs is presented in Fig. 3.

Sensor-based methods and feature-based methods are two main categories of PA detection approaches (Abdullakutty et al., 2021); Sensor-based approaches mostly deal with spoofing attacks via applying extra hardware to the digital authentication systems. Examples of which can be seen in using additional sensors like Light Field Camera (LFC), multi spectral sensors, and 3D scanners (Abdullakutty et al., 2021; Ramachandra & Busch, 2017). Feature-based approaches, on the other hand, are considered as software-based methods involving processing additional features of the input data (Abdullakutty et al., 2021). The most effective software-based solution to prevent spoofing is called "liveness detection" meaning that the system would apply some extra process on the input data to deter spoofing via searching for life signs or motion (Abdullakutty et al., 2021; Gang Pan, 2008; Joshi & Singh, 2013).

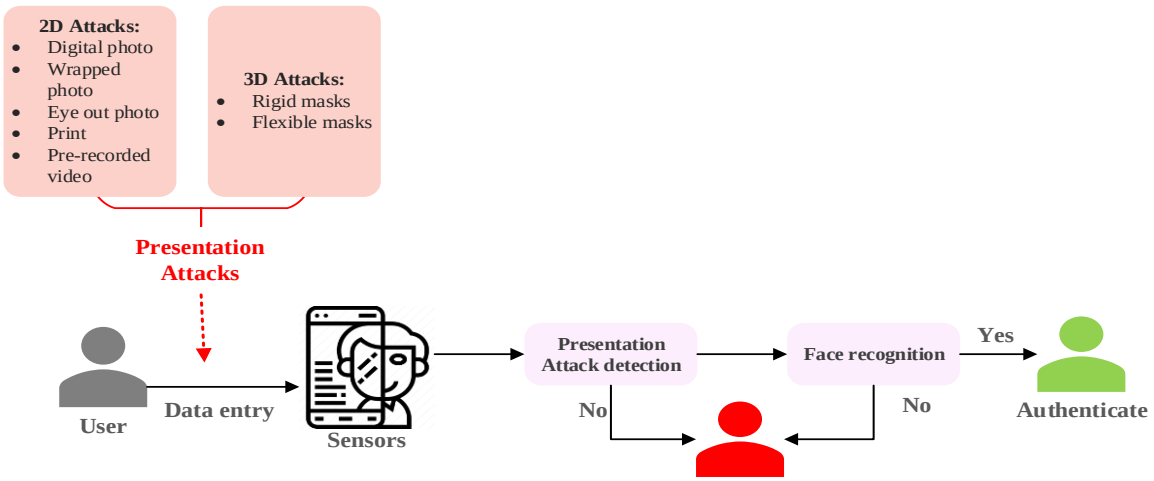

Fig. 3. A sample face detection system with different types of PAs

Fig. 4 provides a good classification of the discussed spoof detection approaches in biometric systems.

As mentioned before, since remote authentication has been the topic of interest in recent years, spoof prevention through liveness check, especially in facial biometric systems, has become a research trend in this research field (Gang Pan, 2008; Joshi & Singh, 2013); because liveness check can be considered as an additional security layer for biometric systems (Fernandes & Bala, 2016). Main liveness detection approaches in facial biometric systems applied in the literature are classified into three main categories by (Singh et al. 2013), including: (1) challenge and response method (2) face texture check (image quality), and (3) joining two or more biometric liveness detection (multi-modal approach) (Fernandes & Bala, 2016; Gang Pan, 2008; Joshi & Singh, 2013). The first method is more prevalent, compared to others, and it is basically used to distinguish a photo from a real user by throwing some challenges in terms of eyes, mouth, and head movement sequences (Gang Pan, 2008; Joshi & Singh, 2013). Since these challenges are defined in a way that can only be performed by a real user, not a photo, the system compares the response sequence and analyzes whether it is related to a real person or not (Joshi & Singh, 2013). To detect imposter, researchers have mostly utilized eye blinking patterns, lips/ head movement sequence, or have applied multimodal approaches like combination of speech and face, in the literature (Joshi & Singh, 2013; Singh et al., 2014). To evaluate the image quality, also, local binary pattern, logistic regression, and low-level feature descriptors have been applied to assess several image quality assessment parameters (Fernandes & Bala, 2016; Singh et al., 2014). Table 2 represents a brief list of the most recent and key works on liveness detection, in the literature. As it can be seen, a wide spectrum of approaches is applied to this domain ranging from combinatory soft computing and fuzzy approaches to neural networks. However, Deep Learning (DL) algorithms are believed to be the game changer approach in PA protection and the majority of research in PA detection have been focused on DL approaches, since 2018 (Abdullakutty et al., 2021).

4. Recent Trends in Presentation Attack Detection

With regard to the important role of digital authentication via biometric systems in the digital era, a lot of work has been done in this topic. There are several review papers which surveyed different approaches in biometric systems and spoof detection in such systems. Table 3 represents a shiny list of which. As it can be seen in this table, every review survey focused on a particular subject. What differentiates this work compared to the others is the fact that this work covers both initial concepts of a biometric system and highly regarded research trends in each aspect of biometric systems, especially in case of PA detection.

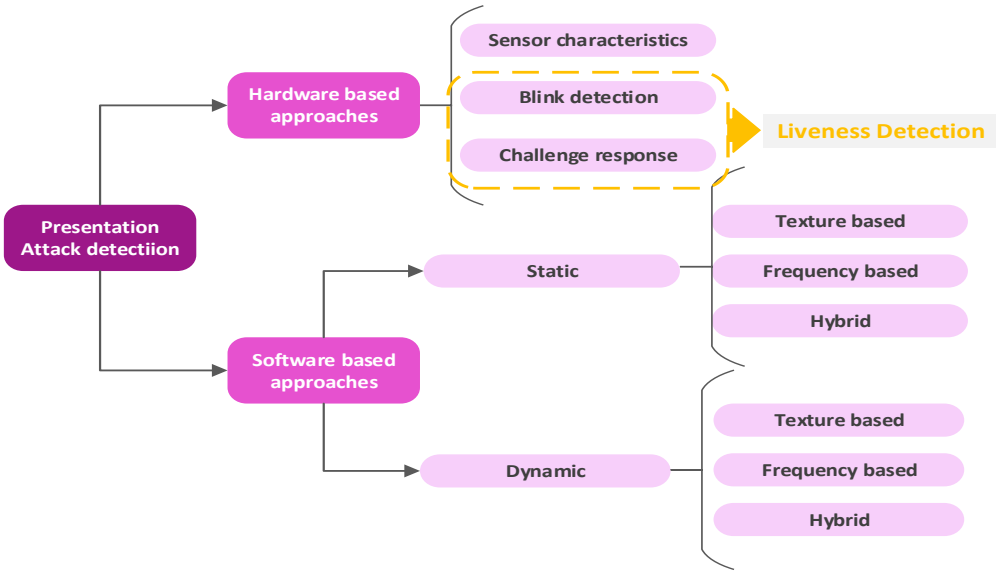

Fig. 4. A summary of main representation attack detection approaches

Table 2. A list of existing approaches on liveness detection in PA detection

Article	Applied approach
(Joshi & Singh, 2013)	Fuzzy expert systems
(Malarvizhi et al., 2020)	Hybrid soft computing optimization based on Adaptive Fuzzy Genetic Algorithm
(Singh et al., 2014)	A combination of eye and mouth movement detection
(Fernandes & Bala, 2016)	Image Quality Assessment (IQA) parameters
(Kundargi & Karandikar, 2018)	A combination of completed local binary pattern with wavelet transform
(Jung & Heo, 2018)	Convolutional neural network
(Yuan C, 2018)	BP neural network
(Xia et al., 2020)	Webber local binary with support vector machines

Table 3. A list of key review surveys on PA detection

Article	Attacks			Generalization	Discussion
	Photo	video	3D mask		
(Galbally et al., 2014)	✓	✓	✓	×	General taxonomy of anti-spoofing methods
(Ramachandra & Busch, 2017)	✓	✓	✓	✓	Generic taxonomy of anti-spoofing methods, evaluationmetrics, and relevant international standardisation
(Ghaffar & Mohd, 2017)	✓	✓	✓	×	General taxonomy of anti-spoofing methods, and evaluationmetrics
(Rattani & Derakhshani, 2018)	✓	✓	✓	×	Anti-spoofing in mobile devices
(Raheem et al., 2019)	✓	✓	✓	×	Generic taxonomy of anti-spoofing methods, and evaluationmetrics
(Bhattacharjee et al., 2019)	Obfuscation attacks			✓	Various approaches in face anti-spoofing, and evaluation metrics,withone class classification perspective
(Jia, Guo, & Xu, 2020)	×	×	✓	✓	A thorough investigation on various methods in 3D anti-spoofing
(Jia, Guo, Xu, et al., 2020)	×	×	×	✓	different aspects of spoof detection in mobile devices includinggeneralization
(Abdullakutty et al., 2021)	✓	✓	✓	✓	The most recent trends of deep learning application in PA detection

Abdullakutty et al. (2021) provided a thorough review on the recent trends in deep learning approaches of PA detection in biometric systems, since 2017. They categorized deep learning trends in spoof detection in four main categories, including: Transfer learning, Auxiliary supervision, Anomaly detection, and Multi spectral methods (Abdullakutty et al., 2021) :

- Transfer learning refers to re-using the learned features in a base network and is considered as an effective approach when data is scarce.
  Generative Adversarial Networks (GANs) are believed to be a game changer in this field of research. Providing an automated optimization-based competitive environment to learn unseen attacks and overcome lack of training data in this issue, such systems can be efficient in enhancing the generalization of biometric systems. The interested reader can refer to (Wang et al., 2020).
- To mitigate poor generalization in anti spoofing systems which is derived from missing some of spoof patterns during feature duplication process, auxiliary supervision is proposed in PA detection rather

than using a binary supervision approach coming out of considering anti-spoofing problems as a binary classification problem.

- Unseen attacks are of high importance in biometric systems so anomaly detection is the approach to handle this issue in PA detection.
- Multi spectral approaches are used to make spoof detection possible in spectral images where PAs does not occur in the visible light.

The popularity of the aforementioned approaches, among 37 papers published during 2017 to 2021, is depicted in Fig. 5. Accordingly, it can be seen that multi spectral methods and anomaly detection approaches are more prevalent in this area. However, it is discussed that transfer learning and anomaly detection approaches will play a significant role in further research due to their being an efficient approach to deal with unseen attacks and model generalization enhancement (Abdullakutty et al., 2021).

As discussed before, transfer learning deals with detering overfitting in case of insufficient training data via re-utilizing learned features. Several transfer learning approaches are applied in spoof detection discussed in(Abdullakutty et al., 2021), completely. The applied approaches are classified by domain generalization and domain adaptation. While both approaches lead to biometric systems' generalization being improved, domain adaptation methods would best suit for feature learning in case of insufficient data(Wang et al., 2019).

Domain generalization, on the other hand, deters the biometric system being biased toward the patterns learned from training dataset(Wang et al., 2019). The most recent works applied these two categories of methods to enhance the biometric system's generalization are reported to use adversarial domain adaptation, multi layer maximum mean discrepancy, multi-channel encoder, domain agnostic model, and unsupervised adversarial domain adaptation (Abdullakutty et al., 2021).Generative Adversarial Networks (GANs), as mentioned before, are believed to revolutions this area of work due to their being a good reference for automate learning (Wang et al., 2020).

Anomaly detection approaches are believed to provide a good opportunity for detecting unseen spoof attacks. These approaches mainly work based on the variance within feature distribution meaning that any sample out of the genuine sample cluster's margine would be considered as a new type of attack (Abdullakutty et al., 2021; Fatemifar et al., 2019). The most recent works in this domain can be seen in(Abdullakutty et al., 2021). (Abdullakutty et al. 2021) reported that the recent works in this area applied Image Quality Measure (IQM), Gaussian Mixture Model (GMM), Deep metric learning, Client specific modeling, Convolutional autoencoder, Hypersphere loss function, and Auxiliary classification model approaches to facilitate unseen attack detection.

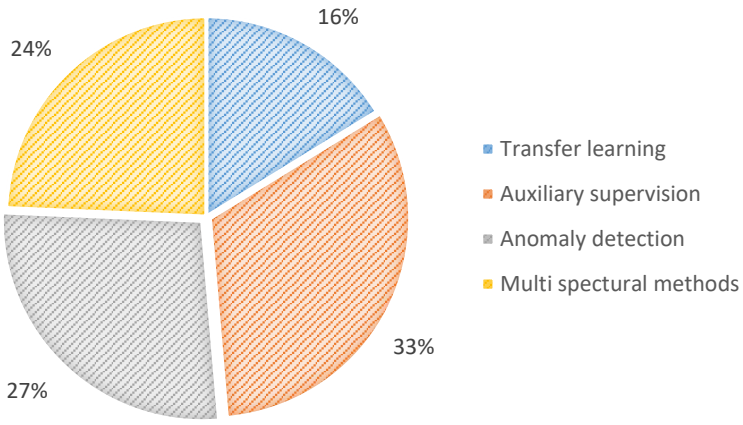

Fig. 5. Popularity of different approaches in deep learning application for spoof detection

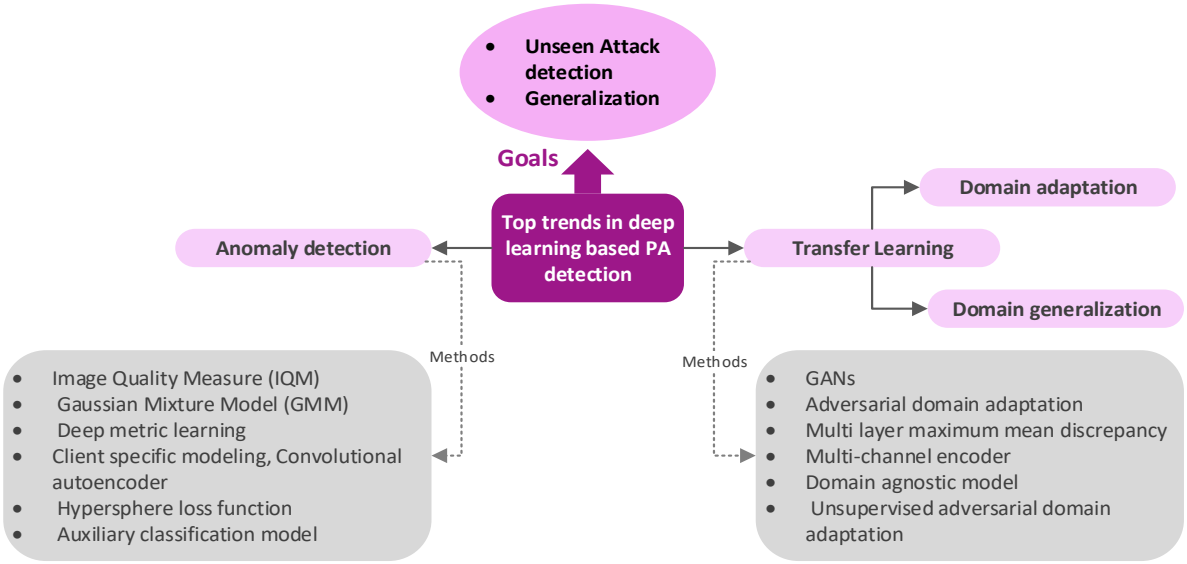

Fig. 6. Recent trends in deep learning-based PA detection

The following figure represents a summarized view of the recent trends in deep learning application in spoof detection discussed before (Fig. 6). To evaluate to what extent the applied approaches were efficient, researchers use system evaluation criteria discussed in the next section.

5. BIOMETRIC SYSTEMS EVALUATION

Performance evaluation in biometric systems is of high importance since these systems are subject to several errors and uncertainties. There are several performance metrics that can be useful to signify the performance of a biometric system, like False-match rate (FMR), False-non-match rate (FNMR), and other criteria elaborated in (El-Abed et al., 2012). However, being more useful to validate a system, verification system performance metrics are what we will focus on, in this section.

Two main metrics to measure the accuracy of a biometric system are: False Rejection Rate (FRR) and False Acceptance Rate (FAR)(de Luis-García et al., 2003; Murillo-Escobar et al., 2015; Sarkar & Singh, 2020).The number of incorrect rejections is reflected by FRR ,normally, ranging from 0.1 % to 20% for a biometric system (Murillo-Escobar et al., 2015). FAR, on the other hand, shows how many times the system accepts an unauthenticated person, normally, ranging from one in 100 to one in 10 million for very high security applications (Murillo-Escobar et al., 2015). When we plot FAR as a function of FRR or its complementary GAR=1-FRR (Genuine Acceptance Rate), it would be possible to well characterize the overall performance of an identity verification system; this plot is called the Receiver Operating Characteristic (ROC) which signifies different tradeoffs between FRR and FAR (de Luis-García et al., 2003; El-Abed et al., 2012). Like other Machine Learning systems, general criteria like accuracy, F-measure, sensitivity, and specificity, as well, can be a good reference to compare biometric systems with each other (Salama AbdElminaam et al., 2020). The most popular evaluation metrics in biometric authentication systems is presented in Table **4**.

One of the most important drivers of a fair system evaluation is having a comprehensive well-organised dataset. There are several standard data sets for both 2D and 3D spoof detection in biometric systems. The interested reader can refer to (Abdullakutty et al. 2021) to access a categorized list of these datasets.

Table 4. Common evaluation criteria for anti-spoofing models

Criteria	Abbreviation	Formulation
False Acceptance Rate	FAR	$FP/Fake\ samples$
False Rejection Rate	FRR	$FN/Genuine\ samples$
Genuine Acceptance Rate	GAR	*1-FRR*
Attack Presentation Classification Error Rate	APCER	$FP/FP+TN$
Bona fide Presentation Classification Error Rate	BPCER	$FN/FN+TP$
Average Classification Error Rate	ACER	$(APCER+BPCER)/2$

6. Discussion and Future Directions

A biometric system is the art of developing an automated verification system working based on biometric traits which are known as permanent, and unique identifiers (Dargan & Kumar, 2020). These systems attempt to enhance security in the digital world and can be applied for a wide spectrum of important applications such as surveillance, defense, law enforcement, access control, border security, personal authentication, and banking, to name a few (Abdullakutty et al., 2021; Dargan & Kumar, 2020). The most important issue in biometric authentication system development is safeguarding its reliability against spoofing and imposter attacks (Dargan & Kumar, 2020). To tackle this, liveness check approaches are proposed, especially in case of face recognition. Type of information fusion, on the other hand, is also of high importance for the system's reliability and accuracy in biometric systems (Sarkar & Singh, 2020). This paper provides an integrated overview on the concept, framework, and different types of biometric systems. In each issue, some recent research works, and novel approaches were introduced to pave the way for further studies. However, due to the significant value of information infusion methods, spoofing, and liveness check for the system's reliability and accuracy, a considerable emphasis is placed on these subjects to shed some light on the research direction in this domain.

According to the discussed research paths, it is clear that soft computing and fuzzy inference systems are expected to be by far more effective than hard computing in this context; due to the obvious ambiguities and uncertainties involved in different phases of a biometric system framework. However, there are a lot of research gaps in this domain of research, especially when it comes to fuzzification of inputs, hybrid inference systems, and defuzzification approaches. Though, the system's complexity and its being applicable in real world scenarios in terms of speed and memory usage are challenges that should be considered intelligently, in doing so.

It is true that soft computing approaches especially fuzzy modeling and combinatory heuristic approaches are recent in this domain and, as discussed before, there is a long path to reach a precise applicable model working based on these approaches. Nevertheless, deep learning approaches are known to be more effective in this regard and this path has received a higher attention during its appearance.

This review authenticates that apart from all progresses obtained in digital authentication via biometric criteria through applying Machine Learning and soft computing approaches, there are obvious setbacks in handling both unseen attacks and the system generalization.

Unseen attacks are one of the most challenging issues in biometric systems development because it is quite impossible to predict different types of spoofing attacks applied in the future due to the ever-rising technology advancements(Abdullakutty et al., 2021; Sarkar & Singh, 2020). This means that compiling a comprehensive dataset which resonates with all possible spoofing attacks would be impractical. This will deter the generalization in biometric systems leading to low reliability. Regarding the surveys performed in this work, anomaly detection and transfer learning are highly recommended for unseen attack detection.

Besides, providing an effective learning environment when data is incomplete, GANs seem to play a shiny role in further research on biometric systems. This approach can provide a good opportunity for automatically enhancing the biometric systems' generalization.

REFERENCES

Abdullakutty, F., Elyan, E., & Johnston, P. (2021). A review of state-of-the-art in Face Presentation Attack Detection: From early development to advanced deep learning and multi-modal fusion methods. *Information Fusion*, *75*, 55-69. https://doi.org/https://doi.org/10.1016/j.inffus.2021.04.015

Abhishek Jana, M. K. S., Monireh Ebrahimi, Pascal Hitzler, George T Amariucai. (2020). *Neural Fuzzy Extractors: A Secure Way to Use Artificial Neural Networks for Biometric User Authentication*https://doi.org/arxiv-2003.08433

Aizi, K., & Ouslim, M. (2019). Score level fusion in multi-biometric identification based on zones of interest. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/https://doi.org/10.1016/j.jksuci.2019.09.003

Alpar, O. (2015). Intelligent biometric pattern password authentication systems for touchscreens. *Expert Systems with Applications*, *42*(17), 6286-6294. https://doi.org/https://doi.org/10.1016/j.eswa.2015.04.052

Bhattacharjee, S., Mohammadi, A., Anjos, A., & Marcel, S. (2019). Recent advances in face presentation attack detection. In (pp. 207-228). https://doi.org/10.1007/978-3-319-92627-8_10

Conti, V., Milici, G., Ribino, P., Sorbello, F., & Vitabile, S. (2007). *Fuzzy Fusion in Multimodal Biometric Systems*. https://doi.org/10.1007/978-3-540-74819-9_14

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*, 113114. https://doi.org/https://doi.org/10.1016/j.eswa.2019.113114

de Luis-García, R., Alberola-López, C., Aghzout, O., & Ruiz-Alzola, J. (2003). Biometric identification systems. *Signal Processing*, *83*(12), 2539-2557. https://doi.org/https://doi.org/10.1016/j.sigpro.2003.08.001

El-Abed, M., Charrier, C., & Rosenberger, C. (2012). Evaluation of Biometric Systems. *New Trends and Developments in Biometrics*. https://doi.org/10.5772/52084

Fatemifar, S., Arashloo, S. R., Awais, M., & Kittler, J. (2019, 12-17 May 2019). Spoofing Attack Detection by Anomaly Detection. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),

Fernandes, S. L., & Bala, G. J. (2016). Developing a Novel Technique for Face Liveness Detection. *Procedia Computer Science*, *78*, 241-247. https://doi.org/https://doi.org/10.1016/j.procs.2016.02.039

Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric Antispoofing Methods: A Survey in Face Recognition. *IEEE Access*, *2*, 1530-1552. https://doi.org/10.1109/ACCESS.2014.2381273

Gang Pan, Z. W. a. L. S. (2008). Liveness Detection for Face Recognition. In *Recent Advances in Face Recognition*. IntchOpen. https://doi.org/10.5772/6397

Ghaffar, I. A., & Mohd, M. N. H. (2017). Presentation Attack Detection for Face Recognition on Smartphones: A Comprehensive Review. *Journal of Telecommunication, Electronic and Computer Engineering*, *9*, 33-38.

Jia, S., Guo, G., & Xu, Z. (2020). A survey on 3D mask presentation attack detection and countermeasures. *Pattern Recognition*, *98*, 107032. https://doi.org/https://doi.org/10.1016/j.patcog.2019.107032

Jia, S., Guo, G., Xu, Z., & Wang, Q. (2020). Face presentation attack detection in mobile scenarios: A comprehensive evaluation. *Image and Vision Computing*, *93*, 103826. https://doi.org/https://doi.org/10.1016/j.imavis.2019.11.004

Joshi, P., & Singh, A. (2013). *Development of a Fuzzy Expert System based Liveliness Detection Scheme for Biometric Authentication*. Elsevier B. V.

Jung, H. Y., & Heo, Y. (2018). Fingerprint Liveness Map Construction Using Convolutional Neural Network. *Electronics Letters*, *54*. https://doi.org/10.1049/el.2018.0621

Kundargi, J., & Karandikar, R. G. (2018, 2018//). Fingerprint Liveness Detection Using Wavelet-Based Completed LBP Descriptor. Proceedings of 2nd International Conference on Computer Vision & Image Processing, Singapore.

Li, N., Guo, F., Mu, Y., Susilo, W., & Nepal, S. (2017, 5-8 June 2017). Fuzzy Extractors for Biometric Identification. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS),

Ltd., A. A. (2019). *Biometric Authentication: Literature Review*. All Answers Ltd. https://ukdiss.com/litreview/biometric-authentication-literature-review.php?vref=1

Malarvizhi, N., Selvarani, P., & Raj, P. (2020). Adaptive fuzzy genetic algorithm for multi biometric authentication. *Multimedia Tools and Applications*, *79*(13), 9131-9144. https://doi.org/10.1007/s11042-019-7436-4

Moutafis, P., & Kakadiaris, I. A. (2016). Exploiting Score Distributions for Biometric Applications. In T. Bourlai (Ed.), *Face Recognition Across the Imaging Spectrum*. Springer International Publishing https://doi.org/10.1007/978-3-319-28501-6_14

Murillo-Escobar, M., Cruz-Hernández, C., Abundiz-Pérez, F., & Lopez-Gutierrez, R. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*, 8198-8211. https://doi.org/10.1016/j.eswa.2015.06.035

Raheem, E. A., Ahmad, S. M. S., & Adnan, W. A. W. (2019). Insight on face liveness detection: A systematic literature review. *International Journal of Electrical and Computer Engineering*, *9*, 5865.

Ramachandra, R., & Busch, C. (2017). Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *ACM Comput. Surv.*, *50*(1), Article 8. https://doi.org/10.1145/3038924

Rattani, A., & Derakhshani, R. (2018). A Survey Of mobile face biometrics. *Computers & Electrical Engineering*, *72*, 39-52. https://doi.org/https://doi.org/10.1016/j.compeleceng.2018.09.005

Ross A., N. K., Jain A.K. . (2008). Introduction to Multibiometrics. In F. P. Jain A.K., Ross A. (Ed.), *Handbook of Biometrics*. Springer. https://doi.org/https://doi.org/10.1007/978-0-387-71041-9_14

Rubab, S., & Mir, A. (2011). Biometrics Verification: a Literature Survey. *5*, 67.

Salama AbdElminaam, D., Almansori, A. M., Taha, M., & Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. *PLOS ONE*, *15*(12), e0242269. https://doi.org/10.1371/journal.pone.0242269

Sanderson, C., & Paliwal, K. K. (2004). Identity verification using speech and face information. *Digital Signal Processing*, *14*(5), 449-480. https://doi.org/https://doi.org/10.1016/j.dsp.2004.05.001

Sarkar, A., & Singh, B. K. (2020). A review on performance,security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*(37), 27721-27776. https://doi.org/10.1007/s11042-020-09197-7

Singh, A. K., Joshi, P., & Nandi, G. C. (2014, 12-13 July 2014). Face recognition with liveness detection using eye and mouth movement. 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014),

Statista. (2021). *Global biometric technologies market revenue from 2018 to 2027*. https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/

Venkatraman, S. (2009, 22-24 Jan. 2009). An Adaptive Framework for Biometric Systems. 2009 International Conference on Computer Engineering and Technology,

Wang, G., Han, H., Shan, S., & Chen, X. (2019). *Improving Cross-database Face Presentation Attack Detection via Adversarial Domain Adaptation*. https://doi.org/10.1109/ICB45273.2019.8987254

Wang, G., Han, H., Shan, S., & Chen, X. (2020, 13-19 June 2020). Cross-Domain Face Presentation Attack Detection via Multi-Domain Disentangled Representation Learning. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),

Xia, Z., Yuan, C., Lv, R., Sun, X., Xiong, N. N., & Shi, Y. (2020). A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(4), 1526-1536. https://doi.org/10.1109/TSMC.2018.2874281

Yuan C, S. X., Wu QJ (2018). Difference co-occurrence matrix using BP neural network for fingerprint liveness detection. *Soft computing*, 1-13.