Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Anti-Spoofing Methods in Face Recognition

Konstantinos Bezas, Foteini Filippidou
kobezaa@mst.ihu.gr, fnfilip@cs.ihu.gr
International Hellenic University

Article Information

Submitted : 3 May 2023
Reviewed: 11 May 2023
Accepted : 9 June 2023

Keywords

Biometric systems, spoofing attacks, antispoofing, artificial intelligence, deep learning, neural network.

Abstract

Biometric data are personal data that result from specialized processing techniques and are associated with physical, biological, or behavioral characteristics of a natural person that allow for or confirm their unquestionable identification. These characteristics or identifiers are permanent and unique.

This paper refers to the biometric characteristics used by systems, their mode of operation, and the categories they are distinguished in. The types of attacks that they may be subjected to are then analyzed, along with the anti-spoofing methods proposed in some studies specifically for systems that use the face as a biometric feature. Finally, numerical data is presented regarding the scientific interest that the topic of anti-spoofing methods in biometric systems has shown in the last decade.

A. Introduction

Given that digital evolution dramatically changes people's daily lives, security is no longer limited to personal safety but also cybersecurity. As many of our daily activities concern our digital identity, it is truly important for us to maintain its security [1].

Biometric systems will not fully replace identity verification tools and technologies, but combining biometric approaches with traditional methods of identity verification will help improve security issues of applications. Methods and tools for recognition based on biometric elements have become popular for developing many useful, demanding, and widely accepted applications, such as security issues, monitoring, criminological investigations, malicious technologies, identity access management, and access control [2].

B. Research Method

The word biometric comes from the Greek words "βίο" (life) and "μετρικός" (measure). The concept of biometrics involves the analysis of the biological characteristics of a human being, and in this work we will use this term to refer to biometric identification of people. Biometric identification offers a promising approach to security applications, with advantages over classical methods that depend on something one has (key, card, etc.) or something one knows (password, PIN, etc.) [3].

Biometric characteristics (Figure 1) can be divided into two main categories, those related to **physiology** and those related to **behavior** [3]. The first category includes characteristics that cannot be easily changed, i.e., they are stable parts or properties of our body. Examples include fingerprints, DNA, iris, and retina. Behavioral characteristics are related to the way a person performs a specific action, such as their gait, signature, and typing style [4].

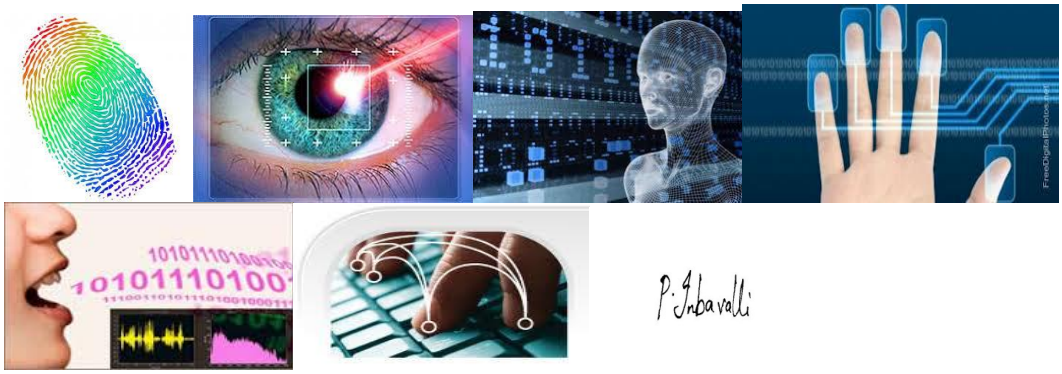

Figure 1. Some of the biometric characteristics used in biometric systems**.**

Any human characteristic related to physiology and/or behavior can be used as a biometric feature provided that it satisfies the following requirements [5]:

- Homogeneity: each individual should possess the characteristic.
- Discrimination: any two individuals should differ significantly in terms of this characteristic.

- Stability: the characteristic should be sufficiently invariant over a period of time.
- Collectability: the characteristic should be measurable quantitatively.

However, in a system that uses biometric data for individual identification, there are other issues that need to be examined, including [5]:

- Performance: which refers to the accuracy and speed of recognition as well as the resources required to achieve them.
- Acceptance: indicates the degree to which people are willing to accept the use of a particular biometric identifier (feature) in their daily lives.
- Bypass: which reflects how easily the system can be deceived by malicious methods.

Biometric Systems Function

A biometric system receives the raw biometric data of the user (Row biometric data) using a biometric sensor or scanner (Sensor Module). These raw biometric data are recorded, pre-processed, and then transferred to the next unit of the system for feature extraction (Feature Extraction Module), where appropriate feature extraction algorithms are used. There are many feature extraction and classification methods available according to the requirements of the biometric feature. After feature extraction, they are given as input to the matching unit (Matching Module) for further comparison with the stored templates in the database (DB). Finally, the decision-making unit (Decision Module) decides whether the user is a genuine user or an imposter. The flowchart of Figure 1 shows the structure and sequence of the units of a biometric system [6].

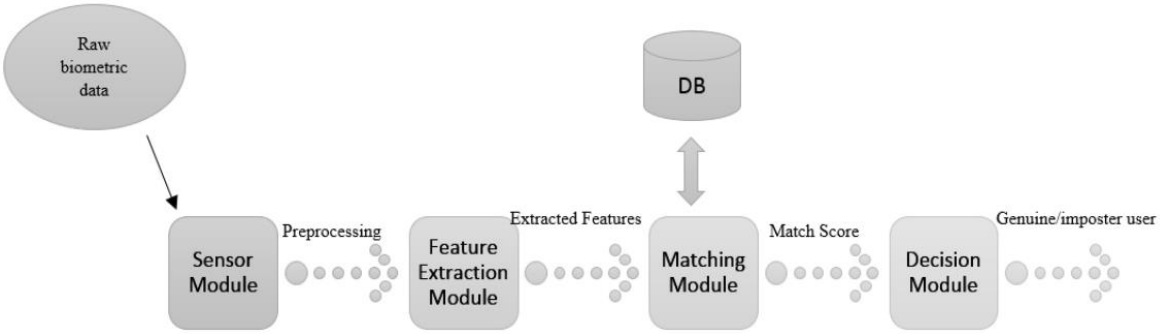

Figure 2. Structure of a Biometric System [6]

Categories of Biometric Systems

There are two types of biometric systems: **identification** and **verification** systems.

In identification systems, a biometric characteristic is taken from an unknown individual. The system compares this characteristic to a database of known biometric characteristics of individuals and identifies or infers the identity of the unknown person.

In verification systems, a user presents a biometric characteristic and makes a claim about their identity. The system either accepts or rejects the request [7].

Unimodal biometric systems rely on one biometric characteristic, which may result in lower performance and security [1].

On the other hand, there are **multimodal** biometric systems that use more than one biometric characteristic in combination to identify/verify an individual. These systems provide greater security than unimodal systems as they take multiple biometric characteristics into account [1].

Categories of attacks on biometric systems

There are two types of attacks that can occur on a biometric system, direct and indirect.

Direct attacks are executed at the sensor level, outside the digital boundaries of the biometric system. Despite the successes of biometric recognition systems in recent decades, they remain vulnerable to increasingly sophisticated direct attacks using spoofing, which involves the use of fake objects [8].

Indirect attacks, however, are executed within the digital boundaries by intruders such as cyber criminals. These attacks may attempt to bypass or replace the feature extractor stage from a program that creates the desired set of features. The comparison, matching, or decision stages may be subjected to Trojan horse attacks, or malicious individuals may exploit vulnerabilities in communication channels [9].

Figure 3 shows the typical points of attack on a biometric system [10].

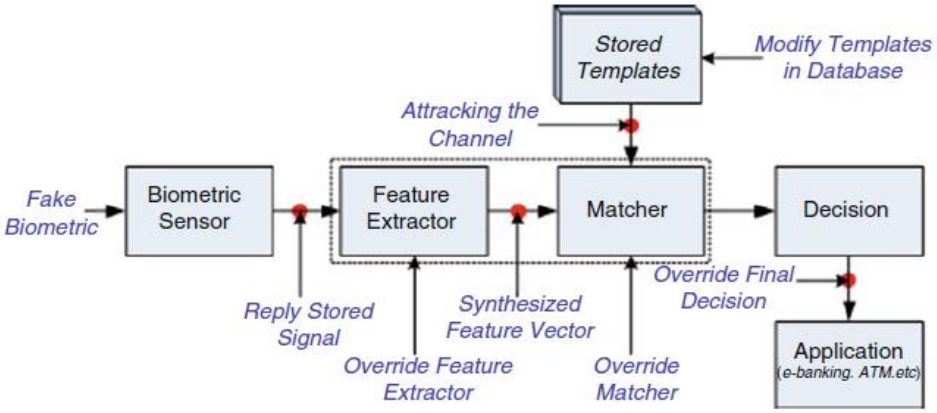

Figure 3. Typical attack points in a biometric system [10]

In cases of spoofing attacks, a fake biometric element created from the biometric information of legitimate users is presented to the sensors of the system. An attacker can present a fake biometric sample of a real user in a biometric recognition system to gain access to unauthorized data or facilities. Spoofing attacks are a direct attack on the sensor and do not require the attacker to have prior knowledge of the internal workings of the biometric system. To prevent such attacks at the sensor level, biometric systems must determine the vitality of the source of an acquired sample [8].

Regardless of the security measures in place in any system, none of them can be considered resistant (spoof-proof) to any attack. Measures taken against these attacks (anti-spoofing measures) simply make the system more secure [5].

Spoofing attacks on facial recognition systems

Detecting spoofing attacks on facial recognition systems has become a significant issue as the technology is widely used in various identity verification systems and portable devices.
In general, there are three ways to create a spoofing attack on a valid user [11]:

- Printing a photograph
- Reproducing a video
- Presenting a 3D facial representation

The most common attacks on such systems involve using a printed photograph, a repeated video, and a 3D mask. The attacker prints and presents a spoofed facial image on a 2D medium (e.g., paper and LCD screen), while in the case of a 3D facial mask, the intruder wears a 3D mask to deceive the facial recognition system [12].

"Anti-spoofing" Methods in Biometric Systems

Detection of liveness is a common countermeasure to prevent the deception of a biometric system. The existing techniques for liveness detection, illustrated in Figure 4, can generally be divided into two categories as follows:

1. **Hardware-based techniques** utilize the characteristics of liveness from the available biometric data at the acquisition stage, adding an additional device to the sensor to obtain indicators of liveness from the presented biometric sample, such as arterial pressure, skin distortion, or odor.
2. **Software-based techniques**, on the other hand, detect fake characteristics as soon as the sample is taken with a typical sensor during processing. Techniques based on software have the advantage over those based on hardware in that they are less expensive (as they do not require additional devices) and less intrusive to the user. Software-based approaches can detect any point of liveness from the acquired sample using static techniques (using one sample) (e.g., the finger is placed and lifted from the sensor once or several times) or dynamic techniques (using multiple samples taken in real-time) [13].

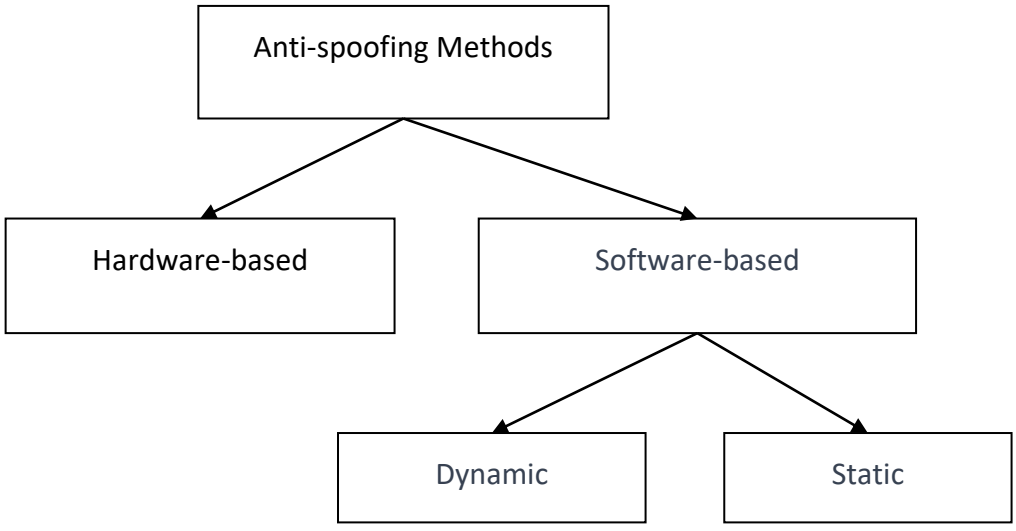

Figure 4. Categories of Anti-Spoofing Methods

Next-generation biometric systems may go beyond the human body. Several studies indicate the possibility of identifying individuals by examining the bacteria that inhabit their body [14]. Years ago, when the study of human microbiota began to flourish, researchers demonstrated that skin bacteria remaining on objects such as computer keyboards could be combined with the person who used these objects with a high degree of certainty [15]. In other words, we leave unique bacterial "fingerprints" on the objects we touch.

Most studies present algorithmic solutions for known attacks (spoofs), where models are trained and tested on the same type of attacks. However, in real-world applications, attackers can also cause types of attacks that algorithm designers are not familiar with, the so-called unknown spoof attacks. Researchers are increasingly paying attention to the generalization of anti-spoofing models, i.e., how well they are able to detect spoof attacks they have never seen before during their training [16].

"Anti-spoofing" Methods in Biometric Facial Recognition Systems

Facial recognition is one of the most remarkable abilities of the human visual system even after a long period of time and the second most widely used biometric technique [17]. It is the analysis of facial characteristics or patterns to verify the authenticity or identify the identity of an individual [18].

Facial recognition is used in a plethora of biometric system applications as it is socially acceptable, accurate, and convenient. However, facial recognition systems are considered more vulnerable compared to other systems that use biometric functions, as a simple photograph or video of a genuine user can be used to deceive the system. Therefore, a mechanism for detecting vitality is necessary to improve the security of biometric systems [18].

Standard technical detection methods can generally be classified into three categories based on the indications used [19]:

(i) methods based on the analysis of the movement of the entire face or some of its parts,
(ii) (ii) methods based on texture analysis, given that real skin presents different properties from fake materials or photography, and
(iii) (iii) methods based on material, i.e. systems that use LED arrangements of different wavelengths.

Methods based on motion analysis attempt to detect vital movements such as eye blinking or movements of the lips and head. Texture-based methods aim to exploit the distinctions in patterns between live and fake faces [20].

The use of video footage by the attacker is more realistic compared to using photos and is more difficult to be detected by systems that control vital characteristics such as eye movements to identify attempted attacks. In one of the early attempts to combat deepfakes based on video, artificial objects added to biometric samples during video playback on display devices as well as the noise added are examined. The Fourier spectrum of the video noise and the use of visual rhythms can detect the correct information to distinguish between valid and invalid users seeking forgery through video [21].

Detection of an individual's vitality as a technique to avoid deception of a facial recognition system has been studied and used in many systems. With an accuracy of 98.89%, the facial morphological functions, specifically the control of eye and mouth movements, can detect whether the individual being recognized is alive or possibly a photograph or video. Figure 5 shows the steps followed by the system to confirm or deny the live presence of an individual [17].

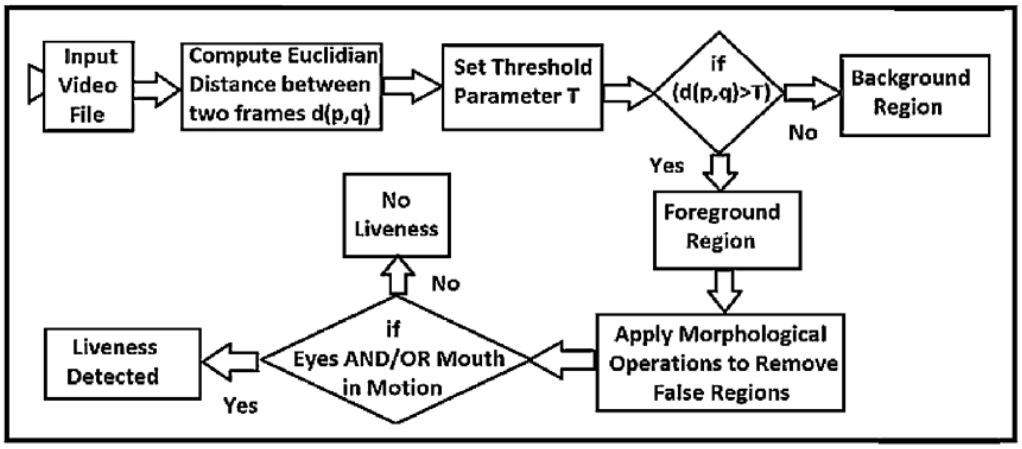

Figure 5. Vitality detection system [17]

The system reads the video and takes two consecutive frames of the video. The Euclidean distance between the two frames is calculated, i.e., the color difference of pixels between the two frames. The foreground and background areas are determined by adjusting the Threshold parameter and then morphological operations are applied to check the movement of the eyes and lips. The proposed technique is simple and requires very little processing time [17].

Studying the asymmetry of the image elements between the real and fake face in different color regions, a system based on the characteristic feature of face texture, color texture Markov feature (CTMF), was proposed. CTMF consists of CCMF that characterizes the texture information in each color channel and CCDMF that characterizes the mutual information between color channels (Figure 6). CTMF can effectively represent texture information of the face in each color channel and the mutual texture information of the face between different channels. In addition, the Support Vector Machine algorithm (SVM-RFE) is used to reduce the dimension of features. Initially, a filter is used to detect the texture difference between the real and fake face, which can be considered as a low-level feature. Then, the texture difference of the face is formed by the Markov process to form a high-level representation of the low-level features. Moreover, SVM-RFE is used to reduce the dimension of features and make the technique suitable for real-time detection [22].

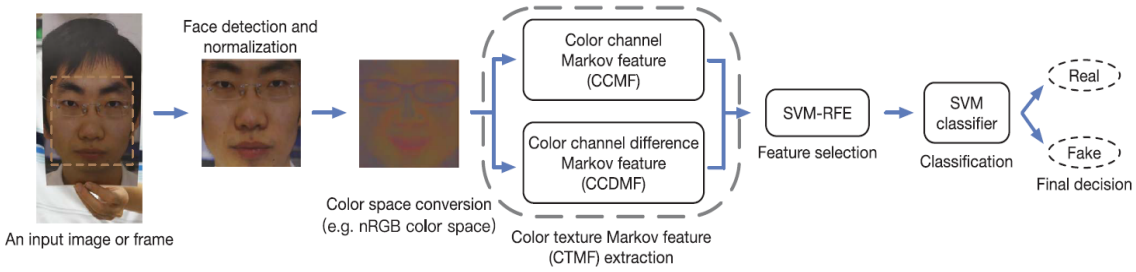

Figure 6. CTMF framework [22]

The Angular Radial Transformation (ART) method was used to extract a feature vector from the entire image and input it into a Maximum Likelihood (ML) classifier, which is particularly useful for images or NNCs to determine whether the subject is a real or fake person. The advantage of the proposed approach is that it can be used by any recognition system that uses RGB images, unlike other approaches that use specialized sensors and do not cause physical harm to humans. The inputs to the classifier are images that are decomposed with the ART transformation, which enables the distinction between light intensities reflected from a real person and a 3D mask [23].

In a research study, a linear combination of fusion between static image analysis and video analysis was used. Video analysis was used to detect vitality and motion indications through an algorithm, while a new static analysis was used to find indications frame by frame of the video. The proposed system is able to operate using only one frame of the video. Thus, the proposed combined rule allows for different indications from static analysis and video analysis to be taken into account, giving greater confidence in classification [24].

The easiest and cheapest attack on face recognition is the use of a photograph of the person to be recognized. The problem of dealing with forgery/impersonation attacks lies in finding technical methods and distinct characteristics that simultaneously require low computational resources. Many applications use the entire image of the face or full video for detecting vitality. Often, certain areas of the image are unnecessary or correspond to the noise of the video, generally leading to low performance. A simple and effective solution is based on selecting certain parts of an image. Specifically, seven innovative and fully automated algorithms were used in research to select regions of interest in a face image. These areas of an image are defined to be distinct (i.e., crucial for a particular classification, such as the presence of vitality), constant (i.e., appearing in different face images or frames of a video), significant (i.e., visible regions), and repetitive (i.e., frequently appearing in a set of images of a particular class). The basic idea is that these parts are specific to a face image (or video frame) and should contain features that enable verification of a live person. For the final classification, four well-known classifiers were used: SVM, Naive-Bayes, Quadratic Discriminant Analysis (QDA), and Ensemble. The system was evaluated on two datasets, REPLAY-ATTACK and CASIA-Face Antispoofing Database (FASD), which include printed photos, photos/videos displayed on a mobile phone and screen, and photos/videos projected on an HD screen [19].

In most research studies, detecting a system attack against forgery is treated as a classification problem into two or more classes, attempting to separate normal access from forgery attacks. In one research study, the approach of anomaly detection was adopted, where the detector is trained on genuine accesses only using classifiers of one class. Anomaly detection is the process of finding patterns that deviate from the expected behavior defined by the "normal" samples of a training dataset. Therefore, the fundamental task of a one-class classifier is to detect anomalous elements among the test samples [25].

Detection of a person's vitality could be a possible solution to the problem of combating spoofing in a face recognition system [17].

In another study, the lack of robust motion-based measures to combat attacks on face recognition systems is observed, as simple image processing can simulate blinking or head rotation. Spoofing attacks are executed by printing or displaying a digital image in front of the sensor. These additional reproduction stages create color distortions between fake and real faces. The research proposes an innovative framework/model for estimating the color distortions that arise from the recovery of a person under the same lighting conditions. The proposed method has two main limitations. First, it is difficult to distinguish color distortions that are due to unknown fluctuations in lighting. This disadvantage can be overcome in some cases, such as with indoor access control systems, where the lighting is always the same. Second, it can be easily fooled if there is video feedback during identity verification, as the person trying to deceive can adjust their screen settings to match the colors of a real access [26].

The motion magnification parameter in a video was considered to potentially improve the performance of forgery detection techniques and was used as the first step in the process. Then, the enhanced video is classified for forgery detection, using feature-based checks based on texture using LBP or motion estimation using a descriptor of the optical flow (Histogram of Oriented Optical Flows - HOOF). The HOOF descriptors obtained from the motion magnified video provide top performance in terms of accuracy and computational efficiency. Improvement of the approach under more challenging conditions is achieved by using a combination of motion and texture techniques using HOOF [27].

With the widespread application of artificial intelligence in daily life, facial recognition has become an important tool for achieving security.

The continuous development of deep learning and its exceptional performance in facial recognition is leading more and more researchers to apply it to avoid malicious forgery attacks.

In contrast to traditional non-automatic feature extraction methods, deep learning can automatically learn images, discover many basic facial features, and help accurately distinguish real people from deceptive ones.

In 2014, [28] proposed the application of Convolutional Neural Networks (CNN) for extracting highly discriminative features in a supervised manner, which in combination with some data preprocessing, significantly improves the performance against face spoofing.

The success of Convolutional Neural Networks (CNN) encouraged their use in face biometrics for anti-spoofing and face verification applications by [29], who developed a deep CNN architecture where the input to the neural network is a face

image and the output is the probability of a class. Additionally, they proposed an effective training strategy to enable the use of deeper CNN structures for face anti-spoofing applications and to allow for the development of training data autonomously when there is insufficient training data available.
Applying transfer learning, [30] used a pretrained convolutional neural network (CNN) for detecting spoofing attacks. The approach relied on the knowledge possessed by a pretrained CNN acquired from a Machine Learning model, which can be used if there is not enough data to train it from scratch. Transfer learning also saves computational resources, as training from scratch can take days to weeks.
[31] followed the same method by choosing the VGG-16 neural network, which was pretrained on the ImageNet database.

Table 1. Main characteristics of antispoofing methods per reference used for face recognition**.**

No	Reference	Characteristics of methods related to Face
1	[32]	Generating spoof data in a three-dimensional (3D) space.
2	[21]	Dealing with video-based spoofing, using the Fourier spectrum of video noise and visual rhythms.
3	[17]	Eye and mouth movements are checked by calculating the Euclidean distance between two frames of the video.
4	[22]	Color Texture Markov Feature (CTMF) which consists of CCMF-texture information in each color channel and CCDMF-mutual information between color channels. Support Vector Machine (SVM-RFE) algorithm.
5	[23]	Angular Radial Transformation (ART) method for feature vector extraction. Maximum Likelihood (ML) classifier. Differentiation between light intensities reflected from a real person and a 3D mask.
6	[24]	Linear combination fusion between static image analysis and video analysis. Only one frame of the video is used.
7	[19]	Using seven innovative and fully automated algorithms to select discrete regions of interest in a facial image. Final classification with SVM, Naive-Bayes, Quadratic Discriminant Analysis (QDA) and Ensemble classifiers.
8	[25]	Training on genuine accesses with classifiers of a class. Finding patterns that deviate from expected behavior.

9	[26]	Estimation of chromatic distortions that arise from the reacquisition of a face under the same lighting conditions (e.g. photo printing or presentation of the face through a device in front of the sensor).
10	[27]	Study of the motion magnification parameter in a video using LBP or Histogram of Oriented Optical Flows-HOOF.
11	[28]	Using a Convolutional Neural Network (CNN).
12	[29]	Usage of deeper CNN structures, development of training data autonomously when there are not enough training data available.
13	[30]	Transfer learning method, usage of pretrained CNN.
14	[31]	Usage of VGG-16 neural network that was pretrained on the ImageNet database.

Multimodal biometric systems

Polytropic biometric recognition techniques use features from multiple sources to enable a biometric system to acquire integrated information and more necessary data about the same object. In this direction, the biometric research community could overcome many problems faced by a system that relies on a single biometric feature, such as instability in feature extraction, noisy data from a sensor, limited degrees of freedom, and high error rates [33].

Multimodal biometric systems provide better measures against forgery, making it difficult for an intruder to simultaneously tamper with multiple biometric characteristics of a legitimate user.

By asking the user to present a random subset of biometric characteristics (e.g., right thumb and right middle finger, in that order), the system ensures that there is indeed a "live" user at the data collection point, whom it is called upon to recognize or authenticate [34].

To cover the high demands in information security, researchers have developed the architecture of a highly effective security system that can handle the security of private networks and autonomous computers. The architecture has combined different recognition systems after studying the advantages and disadvantages of each system.

The levels of the studied system are as follows:

- Activity recognition and face recognition
- Vein recognition
- One-time password mechanism
- Hand gesture recognition [35]

In another study, a different scheme for feature extraction of polytopic biometric data based on subclass discriminant analysis (SDA) was proposed. Two typical biometric features, the face and the palm, were examined. For an individual, these data are considered as two subclasses of a class, and the discriminant features are extracted by searching for an embedded space where the difference between the

subclasses belonging to different individuals is maximized and the difference within each subclass is minimized. Then, the obtained features are merged and used for classification [33].

Spectroscopy refers to a method of examining the matter and properties of it, by analyzing the light, sound, or particles emitted, absorbed, or scattered by the object under study. A system with multiple biometric factors that uses spectroscopy can make the success of forgery attacks very difficult and time-consuming, if not impossible. This is because the approach with spectroscopy, using various wavelengths, allows us to examine various parameters of the skin, underlying tissue, blood, fat, melanin pigment in the eyes, etc., which vary from person to person, making spoofing a very difficult task, as it must be able to mimic multiple normal characteristics [36].

Research interest in "Anti-spoofing" methods in biometric systems

Subsequently, the results of a search for works published in Scopus [37] related to anti-spoofing methods for various biometric characteristics are presented.

Figure 7 shows the graphical representation of the number of works that have dealt with anti-spoofing methods in recent years. Studying graph, we observe that the interest of researchers in studying anti-spoofing methods in biometric systems is increasing, and especially in the last two years, there has been a significant increase in the number of works studying this topic and published in Scopus.

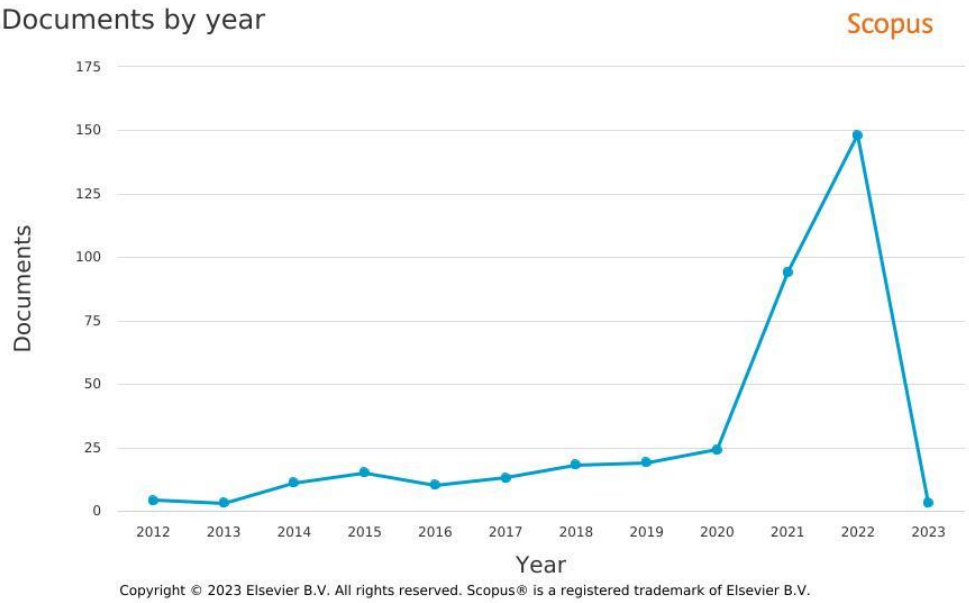

Figure 7. Number of research studies on antispoofing methods per year**.**

Figure 8 shows graphically the number of research studies that have dealt with antispoofing methods in facial recognition systems. As we can observe, similarly to the previous graph, interest in the topic has significantly increased in the last two years. Comparing the two diagrams, we notice that in 2022, the total number of studies on antispoofing methods is 150, out of which 90 focus on systems that use the face as a biometric characteristic. The same trend can be observed in other years, which confirms the claim that the face is the biometric characteristic that generates the most interest among all.

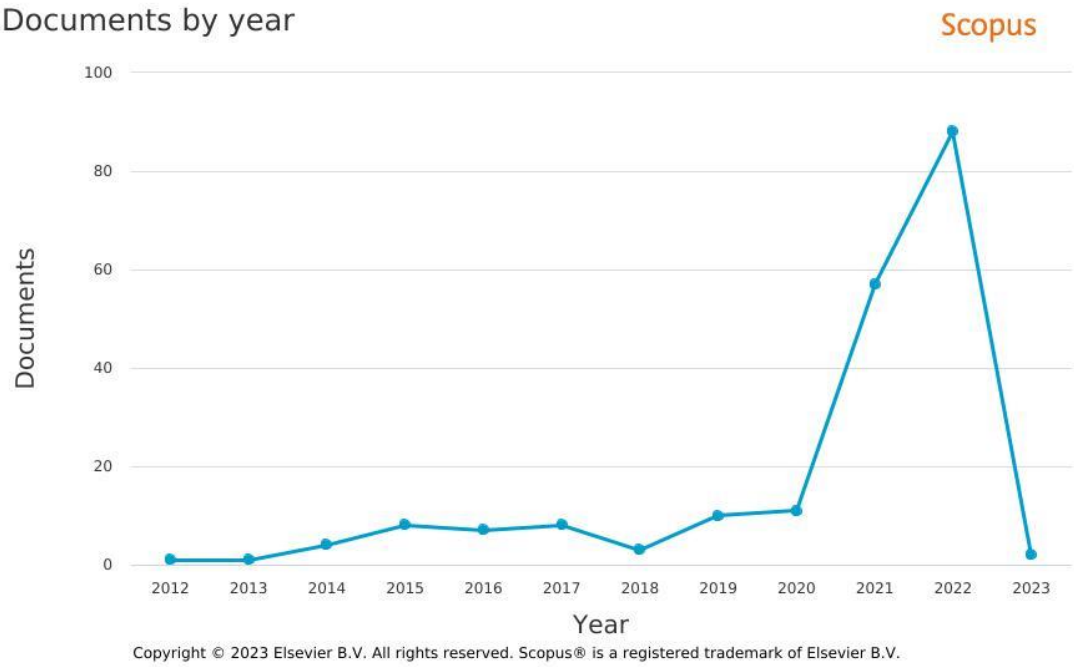

Figure 8. Number of research papers per year related to antispoofing methods in face recognition*.*

Conclusion

In this study, an attempt was made to examine the operation of biometric systems for the identification or authentication of an individual based on facial recognition. At the same time, the most common attacks that biometric systems face were studied, as well as some methods that were researched and applied from time to time to avoid attacks on the violation or deception of these systems. The efforts of attackers focus either on creating fake objects or trying to copy the behavior of the genuine person. Biometric identification or authentication systems aim not only to correctly identify the identity of an individual based on the given characteristic but also to decide on the authenticity and vitality of the sample.

The reliability and performance of a biometric system is of great interest from the perspective of the security of an individual's personal data and the assurance of the integrity of the data and systems that an individual may have access to, by applying various anti-spoofing methods.

In particular, in the last two years, the interest of researchers in studying anti-spoofing methods in biometric systems has been growing. Additionally, the majority of research focuses on studying anti-spoofing methods that relate to facial recognition.

References

[1] Y.-H. Khoo, B.-M. Goi, T.-Y. Chai, Y.-L. Lai, and Z. Jin, "Multimodal Biometrics System Using Feature-Level Fusion of Iris and Fingerprint," in *Proceedings of the 2nd International Conference on Advances in Image Processing*, in ICAIP '18. New York, NY, USA: Association for Computing Machinery, Mar. 2018, pp. 6–10. doi: 10.1145/3239576.3239599.

[2] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, p. 113114, Apr. 2020, doi: 10.1016/j.eswa.2019.113114.

[3] M. Faundez-Zanuy, "Biometric security technology," *Aerospace and Electronic Systems Magazine, IEEE*, vol. 21, pp. 15–26, Jul. 2006, doi: 10.1109/MAES.2006.1662038.

[4] B. B. Mjaaland, "The Plateau: Imitation Attack Resistance of Gait Biometrics," presented at the Second IFIP WG 11.6 Working Conference on Policies and Reseach Management (IDMAN), Springer, Nov. 2010, p. 100. doi: 10.1007/978-3-642-17303-5_8.

[5] S. A. C. Schuckers, "Spoofing and Anti-Spoofing Measures," *Information Security Technical Report*, vol. 7, no. 4, pp. 56–62, Dec. 2002, doi: 10.1016/S1363-4127(02)00407-7.

[6] W. Dahea and H. S. Fadewar, *Multimodal biometric system: A review*, vol. 4. 2018, p. 31. doi: 10.13140/RG.2.2.34056.65287.

[7] P. J. Phillips, A. Martin, C. l Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *Computer*, vol. 33, no. 02, pp. 56–63, Feb. 2000, doi: 10.1109/2.820040.

[8] A. Ali, F. Deravi, and S. Hoque, "Spoofing attempt detection using gaze colocation," in *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–12.

[9] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 20–30, Sep. 2015, doi: 10.1109/MSP.2015.2437652.

[10] A. Jain and A. Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, 2012, pp. 49–79. doi: 10.1007/978-94-007-3892-8_3.

[11] G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," *Recent advances in face recognition*, pp. 109–124, 2008.

[12] S. Arora and M. P. S. Bhatia, "Challenges and opportunities in biometric security: A survey," *Information Security Journal: A Global Perspective*, vol. 31, no. 1, pp. 28–48, Jan. 2022, doi: 10.1080/19393555.2021.1873464.

[13] H. Ahmed Salman and B. kareem, "iris anti-spoofing:static &dynamic technique," *Eng. &Tech.Journal,* vol. 34, pp. 598–609, Jan. 2016.

[14] A. Rinaldi, "Biometrics' new identity—measuring more physical and biological traits," *EMBO reports*, vol. 17, no. 1, pp. 22–26, Jan. 2016, doi: 10.15252/embr.201541677.

[15] N. Fierer, C. L. Lauber, N. Zhou, D. McDonald, E. K. Costello, and R. Knight, "Forensic identification using skin bacterial communities," *Proceedings of the National Academy of Sciences*, vol. 107, no. 14, pp. 6477–6481, Apr. 2010, doi: 10.1073/pnas.1000162107.
[16] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep Tree Learning for Zero-Shot Face Anti-Spoofing," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Long Beach, CA, USA: IEEE, Jun. 2019, pp. 4675–4684. doi: 10.1109/CVPR.2019.00481.
[17] M. Singh and A. Arora, "A Robust Anti-Spoofing Technique for Face Liveness Detection with Morphological Operations," *Optik - International Journal for Light and Electron Optics*, vol. 139, Apr. 2017, doi: 10.1016/j.ijleo.2017.04.004.
[18] "Types of Biometrics," *Biometrics Institute*. https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (accessed Dec. 31, 2022).
[19] Z. Akhtar and G. L. Foresti, "Face Spoof Attack Recognition Using Discriminative Image Patches," *Journal of Electrical and Computer Engineering*, vol. 2016, p. e4721849, May 2016, doi: 10.1155/2016/4721849.
[20] J. Guo, X. Zhu, J. Xiao, Z. Lei, G. Wan, and S. Z. Li, "Improving face anti-spoofing by 3d virtual synthesis," in *2019 International Conference on Biometrics (ICB)*, IEEE, 2019, pp. 1–8.
[21] A. da S. Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video-Based Face Spoofing Detection through Visual Rhythm Analysis," in *2012 25th SIBGRAPI Conference on Graphics, Patterns and Images*, Dec. 2012, pp. 221–228. doi: 10.1109/SIBGRAPI.2012.38.
[22] L.-B. Zhang, F. Peng, L. Qin, and L. Min, "Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination," *Journal of Visual Communication and Image Representation*, vol. 51, Feb. 2018, doi: 10.1016/j.jvcir.2018.01.001.
[23] B. Hamdan and K. Mokhtar, "The detection of spoofing by 3D mask in a 2D identity recognition system," *Egyptian Informatics Journal*, vol. 19, no. 2, pp. 75–82, Jul. 2018, doi: 10.1016/j.eij.2017.10.001.
[24] R. Tronci *et al.*, "Fusion of multiple clues for photo-attack detection in face recognition systems," *2011 International Joint Conference on Biometrics (IJCB)*, 2011, Accessed: Dec. 31, 2022. [Online]. Available: https://www.academia.edu/2982168/Fusion_of_multiple_clues_for_photo_attack_detection_in_face_recognition_systems
[25] S. Fatemifar, S. Arashloo, M. Awais, and J. Kittler, "Spoofing Attack Detection by Anomaly Detection," May 2019, pp. 8464–8468. doi: 10.1109/ICASSP.2019.8682253.
[26] T. Edmunds and A. Caplier, "Face spoofing detection based on colour distortions," *IET Biometrics*, vol. 7, pp. 27–38, Jan. 2018, doi: 10.1049/iet-bmt.2017.0077.
[27] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally Efficient Face Spoofing Detection with Motion Magnification," in *2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, OR, USA: IEEE, Jun. 2013, pp. 105–110. doi: 10.1109/CVPRW.2013.23.

[28] J. Yang, Z. Lei, and S. Z. Li, "Learn convolutional neural network for face anti-spoofing," *arXiv preprint arXiv:1408.5601*, 2014.
[29] Y. A. U. Rehman, L. M. Po, and M. Liu, "Deep learning for face anti-spoofing: An end-to-end approach," in *2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, IEEE, 2017, pp. 195–200.
[30] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep learning for face anti-spoofing: A survey," *arXiv preprint arXiv:2106.14948*, 2021.
[31] O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle, and R. Lotufo, "Transfer Learning Using Convolutional Neural Networks for Face Anti-spoofing," in *Image Analysis and Recognition*, F. Karray, A. Campilho, and F. Cheriet, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 27–34. doi: 10.1007/978-3-319-59876-5_4.
[32] J. Guo, X. Zhu, J. Xiao, Z. Lei, G. Wan, and S. Z. Li, "Improving Face Anti-Spoofing by 3D Virtual Synthesis".
[33] X.-Y. Jing *et al.*, "Palmprint and face multi-modal biometric recognition based on SDA-GSVD and its kernelization," *Sensors*, vol. 15, no. 5, pp. 5551–5571, 2012.
[34] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.
[35] P. Ranjan and K. Jindal, "Proposed Architecture for Enhancing the Efficiency of Security Systems by using Systematic Combination of Different Recognition Systems," *International Journal of Computer Applications*, vol. 123, no. 10, 2015.
[36] D. Pishva, "Use of spectral biometrics for aliveness detection," in *Advanced biometric technologies*, IntechOpen, 2011.
[37] "Scopus preview - Scopus - Sources." https://www.scopus.com/sources.uri?zone=TopNavBar&origin=searchauthorfreelookup (accessed Jan. 02, 2023).