JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Review of Face Anti-Spoofing Techniques: Challenges, Advances and Research Directions

Satish Kumar Nath[1], Dr. Pallavi Pratap[2]
Research Scholar[1], Associate Professor[2]
Computer Sc. & Engg. Department, Maulana Azad University, Jodhpur, India
satishkumar.nath@gmail.com[1], pratappallavi@gmail.com[2]

ABSTRACT

The problem of face recognition systems is a staple of contemporary biometric authentication. It is non-invasive and it can integrate easily with existing camera-based systems. Although the accuracy of recognition has increased significantly due to the use of deep learning, but such systems are highly susceptible to presentation attacks. Such attacks are also known as face spoofing attacks. These attacks are based on the use of printed photographs, replayed videos, digital display or 3D face mask to impersonate recognition systems [1], [3]. In this regard, face anti-spoofing, also referred to as face presentation attack detection (PAD) has become a critical research topic that is meant to discriminate between real and spoofing facial presentations [2], [29].

This article provides a critical summary of face anti-spoofing methods. It assesses the development of the systematically the evolution of the field. It begins with the simple feature-based methods of the early days, through rich deep learning models [3], [18]. Existing algorithms are divided by the cues they take advantage of. Examples of cues are the texture, motion, frequency-domain and learned deep representations [5], [14]. The most common benchmark datasets and evaluation protocols in addition to performance metrics are addressed to shed light on up-to-date practices and limitations [8], [17]. General problems of face anti spoofing are discussed. Cross-dataset generalization, computational efficiency and resistance to new sophisticated spoofing attacks are explored [21], [28]. Lastly, future research directions are provided. This might help in building scalable and deployment-ready face anti-spoofing systems.

INDEX TERMS

Face anti-spoofing, presentation attack detection, biometric security, face recognition, deep learning, literature survey.

I. INTRODUCTION

The use of biometric authentication systems has become a popular trend because it avails a safe and convenient way of identifying identity. Face recognition has been one of the most popular biometric modalities and is utilized widely due to the fact that it is contact-free and can be integrated with the already existing cameras [1]. The face recognition can be used in mobile authentication, access control, surveillance, border security, and online identity verification.

The recent development of deep learning, especially convolutional neural networks (CNNs) has greatly enhanced the face recognition performance in unconstrained situations that include pose, lighting, and facial expression variations [11], [12]. Nevertheless, even with these improvements, face recognition systems are still susceptible to presentation attacks, in which attackers are trying to circumvent the authentication process by showing some kind of fake facial image [3], [29].

The availability of high-resolution cameras and advanced display equipment, as well as facial images on the social media platform, has only escalated the risk of a spoofing attack [5]. Facial anti-spoofing or presentation attack detection (PAD) has, therefore, become an urgent research field that seeks to check the liveness and authenticity of facial inputs [2], [6]. The face anti-spoofing problem is an intra-class problem, unlike face recognition, which is an inter-class problem that entails determining the minute variations between authentic and imposture presentations of same identity [18].

II. FACE ANTI-SPOOFING: PROBLEM DEFINITION AND CHALLENGES

The aim of face anti-spoofing is to ascertain whether the facial presentation presented to a system is that of a live human being or the presentation is done over a spoofing medium [29]. PAD systems generally rate facial presentations as either bona fide (real) or attack (fake) [30] using visual, temporal or physiological representations.

The presentation attacks are generally divided into three attacks; print attacks, replay attacks and three-dimensional (3D) mask attacks [8], [10]. Print attacks are based on printed photographs, replay attacks on digital images or videos on the screens, and 3D mask attacks on physical masks that mimic the facial geometry and texture [14].

Such similarity of both genuine and spoofed samples in addition to the difference in camera sensors, lighting, background and user behaviour contributes largely to the challenge presented in detecting spoofing [17], [21]. In addition, the PAD systems should have high generalization ability to invisible types and environments of attack, which is primarily not achieved by existing systems [20], [22].

III. TRADITIONAL FACE ANTI-SPOOFING TECHNIQUES

A. Texture-Based Methods: These are some of the initial face anti-spoofing methods. They use micro-textual inconsistencies that are added in the printing, displaying and image recapture processes [4], [5]. One of the earliest algorithms used to compute local texture differences on PAD was the Local Binary Patterns (LBP). It proved useful in detection between authentic and spoofed faces [4]. Multi-scale LBP and Colour LBP were suggested as extensions to the algorithm in order to increase resistance to changes in illumination [5], [7]. Other handcrafted descriptors such as Local Phase Quantization (LPQ), Histogram of Oriented Gradients (HOG), Gabor wavelets had also been investigated in conjunction with classical classifiers like Support Vector Machines (SVMs) [6], [29]. In spite of encouraging outcomes in the controlled conditions, texture-based techniques have poor generalization in the real-world settings [18].

B. Frequency-Domain and Reflectance-Based Methods: Frequency-domain techniques mainly include examination of printing halftones, display refresh patterns and sensor noise spectral artifacts [9], [25]. Methods that utilize either Discrete Cosine Transform (DCT) or Fourier analysis have been used to identify these artifacts [9]. On the other hand, Reflectance-based techniques focus on variations in light interaction among real human, and spoofing material. In real skin, subsurface scattering is visible, whereas in spoof media, artificial, unnatural specular scattering is visible [5], [19]. But, these methods are also vulnerable to imaging conditions and sensor properties [6].

C. Motion-Based Methods: Such methods use time-varying signals available in video sequences. Eye blink, head, and optical flow patterns are examples of such signals [10]. Eye-blink has been popularly applied to identify static print attacks [10]. Even though they are good at some types of attacks, they fail to recognize replay attacks with realistic motion and usually need video input which makes them more complex to compute [6], [18].

IV. DEEP LEARNING-BASED FACE ANTI-SPOOFING

Deep learning has made a big breakthrough in face anti-spoofing studies by providing automatic learning of discriminative attributes with raw data [14], [18]. CNN-based methods are superior to handcrafted approaches due to their ability to capture complex texture, reflectance and contextual information [15], [16].

VGGNet, ResNet, and DenseNet are example of some popular networks that are used extensively in PAD tasks [11]–[13]. Researchers suggested 3D CNNs and CNN-RNN hybrids [19] to use spatial and time information. Frequency-aware learning, transformer-based learning and contrastive learning were investigated more recently. These methods enhance robustness and generalization [25]–[27].

The success of deep learning-based PAD approaches tends to have low cross-dataset generalization associated with domain shift [20], [21]. Moreover, most of the models are computationally intensive, which restricts their application in real-time use on resource-constrained devices [24].

V. BENCHMARK DATASETS AND EVALUATION MATRICES

A number of benchmark datasets are created to aid the face anti-spoofing studies, such as CASIA-FASD, Replay-Attack, MSU-MFSD, and OULU-NPU [8], [17]. These datasets vary in the attacks, capturing equipment and the environment.

The metrics that are typically employed in evaluations involving PAD comprise Accuracy, Precision, Recall, F1-score, Equal Error Rate (EER), and Attack Presentation Classification Error Rate (APCER) [29], [30]. Nonetheless, non-uniform evaluation measures between datasets make it difficult to compare them fairly and denounce the necessity of standard benchmarking [30].

VI. OPEN CHALLENGES AND RESEARCH GAPS

Even though a lot has been achieved, there are still a number of issues in face anti-spoofing studies. The problem of cross-dataset generalization is still significant. Models, trained on a specific dataset, tend to be very poor on the unseen data [20], [21]. This is further complicated by the growth of the sophisticated spoofing attacks, such as 3D masks and deepfake-based synthesis of faces [28].

There are other issues like computational efficiency and real-time deployment, especially in mobile and embedded systems [24]. In addition, a majority of the available methods are based on multi-stage pipelines that split face detection and spoofing classification. It adds more latency and is potentially susceptible to error propagation [7], [18].

VII. FUTURE RESEARCH DIRECTIONS

The future face anti-spoofing research must be aimed at creating domain-generalization models that are able to sustain their performance under different environments and types of attacks [20], [22]. Coherent models that combine face detection and spoofing classification into one model can eliminate systems complexity and inference time [7], [29].

Real-world applications require lightweight architectures with edge deployment [24]. Besides, the risk of attacks associated with deepfakes is increasing. It requires PAD systems that can detect both low-level visual elements and high-level semantic anomalies [28]. Re-producibility and fair comparison are also imperative by using the standardized datasets and evaluation protocols [30].

VIII. CONCLUSION

The current paper has discussed face anti-spoofing methods in detail including the traditional handcrafted techniques, the use of deep learning approaches, benchmark datasets, and evaluation protocols. Although spoof detection performance has markedly improved with the adoption of deep learning, issues of generalization, efficiency and resistance to advanced attacks still persist. The research gaps and the insights created by this survey give a solid basis to another research in the future where scalable, reliable and deployment-ready face anti-spoofing systems can be developed.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] S. Marcel, M. S. Nixon, and S. Z. Li, *Handbook of Biometric Anti-Spoofing*, 2nd ed. Cham, Switzerland: Springer, 2019.

[3] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey," *Pattern Recognit. Lett.*, vol. 32, no. 16, pp. 213–224, 2014.

[4] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. IEEE BIOSIG*, 2012, pp. 1–7.

[5] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face spoofing detection using colour texture analysis," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1818–1830, 2016.

[6] T. de Freitas Pereira et al., "Face liveness detection using dynamic texture," *EURASIP J. Image Video Process.*, vol. 2014, no. 1, 2014.

[7] J. Komulainen, A. Hadid, and M. Pietikäinen, "Context based face anti-spoofing," in *Proc. IEEE BTAS*, 2013, pp. 1–8.

[8] Z. Zhang et al., "A face antispoofing database with diverse attacks," in *Proc. IEEE BTAS*, 2012, pp. 1–8.

[9] J. Li, Y. Wang, T. Tan, and A. Jain, "Live face detection based on the analysis of Fourier spectra," in *Proc. SPIE*, 2004, pp. 296–303.

[10] K. Kollreider et al., "Real-time face detection and motion analysis with application in liveness assessment," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 548–558, 2007.

[11] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv:1409.1556*, 2014.

[12] K. He et al., "Deep residual learning for image recognition," in *Proc. IEEE CVPR*, 2016, pp. 770–778.

[13] G. Huang et al., "Densely connected convolutional networks," in *Proc. IEEE CVPR*, 2017, pp. 4700–4708.

[14] Y. Liu et al., "Learning deep models for face anti-spoofing: Binary or auxiliary supervision," in *Proc. IEEE CVPR*, 2018, pp. 389–398.

[15] A. George and S. Marcel, "Deep pixel-wise binary supervision for face presentation attack detection," in *Proc. IEEE ICIP*, 2019, pp. 4542–4546.

[16] Z. Yu et al., "Searching central difference convolutional networks for face anti-spoofing," in *Proc. IEEE CVPR*, 2020, pp. 5293–5303.

[17] J. Yang et al., "Face anti-spoofing: Model matters, so does data," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 358–372, 2021.

[18] Z. Yu et al., "Deep learning for face anti-spoofing: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 10, pp. 6763–6781, 2022.

[19] Y. Atoum et al., "Face anti-spoofing using patch and depth-based CNNs," in *Proc. IEEE IJCB*, 2017, pp. 319–328.

[20] S. Jia et al., "Single-side domain generalization for face anti-spoofing," in *Proc. IEEE CVPR*, 2020, pp. 848–857.

[21] J. Sun et al., "Domain generalization via adversarial learning for face anti-spoofing," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 123–135, 2020.

[22] X. Tu et al., "Learning generalizable representations for face anti-spoofing," in *Proc. IEEE ICCV*, 2021, pp. 9233–9242.

[23] A. Mohammadi et al., "Domain adaptation for face anti-spoofing," *IEEE Access*, vol. 8, pp. 134590–134601, 2020.

[24] C. Benrabah et al., "Lightweight CNN for face anti-spoofing on mobile devices," *IEEE Access*, vol. 9, pp. 16312–16324, 2021.

[25] Z. Wang et al., "Frequency-aware face anti-spoofing," in *Proc. IEEE CVPR*, 2020, pp. 645–654.

[26] H. Wang et al., "Face anti-spoofing with supervised contrastive learning," *IEEE Signal Process. Lett.*, vol. 29, pp. 1739–1743, 2022.

[27] S. Chen et al., "Transformer-based face anti-spoofing," *IEEE Access*, vol. 10, pp. 72118–72129, 2022.

[28] Y. Qin et al., "Deepfake face detection: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 1, pp. 1–22, 2023.

[29] J. Fierrez et al., "Biometric presentation attack detection: State of the art," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1270–1285, 2018.

[30] ISO/IEC 30107-3, "Information technology—Biometric presentation attack detection—Part 3: Testing and reporting," ISO/IEC Standard, 2017.