Studi Literatur *Presentation Attack* dan Set Data *Anti-Spoof* Wajah

I Kadek Dendy Senapartha* dan Gabriel Indra Widi Tamtama

Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana
Jl. Dr. Wahidin Sudirohusodo No.5-25, Kotabaru, Kec. Gondokusuman, Kota Yogyakarta,
Daerah Istimewa Yogyakarta, 55224, Indonesia
**Corresponding author. Email: dendy.prtha@staff.ukdw.ac.id*

Abstract— Face anti-spoof systems are needed in facial recognition systems to ward off attacks that present fake faces in front of the camera or image capture sensor (presentation attack). To build the system, a data set is needed to build a classification model that distinguishes the authenticity of the face of the input image received by the system. In the past decade anti-face spoof research has produced many data sets that are public, but often researchers need time to build or use the right public data sets that are used to build facial anti-spoof models. This article conducts a literature study of public data sets using a systematic literature review method to find out the types of attacks that appear on the facial anti-spoof system, the development process, evolution, and availability of facial anti-spoof data sets. From the search and selection results based on the specified criteria, there were 42 primary research manuscripts in the period 2010 to 2021. The results of the literature study found that there were three trends in the development of anti-spoof facial data sets, namely, 1) data sets with a very large number, 2) datasets with different types of facial samples, and 3) datasets constructed with various devices and sensors. These various public data sets can be accessed freely but with special rules such as agreeing to an end user license agreement document from the researcher or the institution that owns the data set. However, there are also datasets that cannot be accessed due to invalid URLs or due to special rules from the cloud storage service provider where the datasets are stored.

Keywords— face anti-spoof dataset; face anti-spoof model; face anti-spoof system; face recognition system; presentation attack

Abstrak— Sistem *anti-spoof* wajah dibutuhkan dalam sistem pengenalan wajah untuk menangkal serangan yang menghadirkan wajah palsu di hadapan kamera atau sensor penangkap gambar (*presentation attack*). Untuk membangun sistem tersebut, dibutuhkan set data (*dataset*) untuk membangun model klasifikasi yang membedakan keaslian wajah gambar *input* yang diterima sistem. Dalam satu dekade ini penelitian *anti-spoof* wajah telah banyak menghasilkan set data yang bersifat publik, namun sering kali peneliti membutuhkan waktu untuk membangun atau menggunakan set data publik yang tepat yang digunakan untuk membangun model *anti-spoof* wajah. Artikel ini melakukan studi literatur set data publik dengan metode *systematic literature review* (SLR) untuk mengetahui jenis-jenis serangan yang muncul pada sistem *anti-spoof* wajah, proses pembangunan, perkembangan dan ketersediaan set data *anti-spoof* wajah. Dari hasil pencarian dan seleksi berdasarkan kriteria yang ditentukan, terdapat 42 naskah penelitian primer dalam rentang waktu 2010 hingga 2021. Hasil studi literatur ditemukan bahwa terdapat tiga tren dalam perkembangan set data *anti-spoof* wajah yaitu, 1) set data dengan jumlah yang sangat besar, 2) set data dengan jenis sampel wajah berbeda, dan 3) set data yang dibangun dengan beragam perangkat dan sensor. Berbagai set data publik ini dapat diakses secara bebas namun dengan aturan khusus seperti menyepakati dokumen perjanjian lisensi pengguna akhir dari peneliti atau institusi pemilik set data. Namun terdapat pula set data yang tidak dapat diakses karena URL yang sudah tidak valid atau karena aturan khusus dari penyedia layanan penyimpanan *cloud* tempat set data disimpan.

Kata kunci— set data *anti-spoof* wajah; model *anti-spoof* wajah; sistem *anti-spoof* wajah; sistem pengenalan wajah; *presentation attack*

I. PENDAHULUAN

Saat ini perkembangan metode dan mekanisme sistem pengenalan wajah berkembang pesat, semenjak dimulainya penelitian dibidang pengenalan wajah yang telah dilakukan lebih dari 40 tahun yang lalu [1]. Perkembangan pesat ini terjadi karena paradigma *your are your own key* sangat memudahkan sehingga seseorang tidak perlu mengingat *password* atau menyimpan kartu keamanan untuk melakukan autentikasi. Penelitian dari berbagai bidang seperti *image processing*, *computer vision* atau pengenalan pola banyak dilakukan untuk menemukan dan membangun teknik-teknik baru agar dapat meningkatkan performa sistem keamanan biometrik [2]. Hal tersebut menjadi motivasi untuk mengadopsi sistem tersebut ke berbagai aktivitas seperti forensik, pengecekan akses masuk wilayah, sistem pengawasan, dan sistem *e-commerce* [3].

Kepopuleran sistem pengenalan wajah tersebut menjadikan target bagi banyak orang untuk melakukan serangan penipuan (*spoofing attacks*) [4]. Sehingga sistem *spoofing detection* perlu ditambahkan untuk mengetahui apakah wajah yang diperlihatkan adalah asli atau palsu, yang sering kali menjadi pekerjaan yang rumit dilakukan bahkan oleh manusia. Terdapat beberapa pendekatan yang digunakan untuk membangun

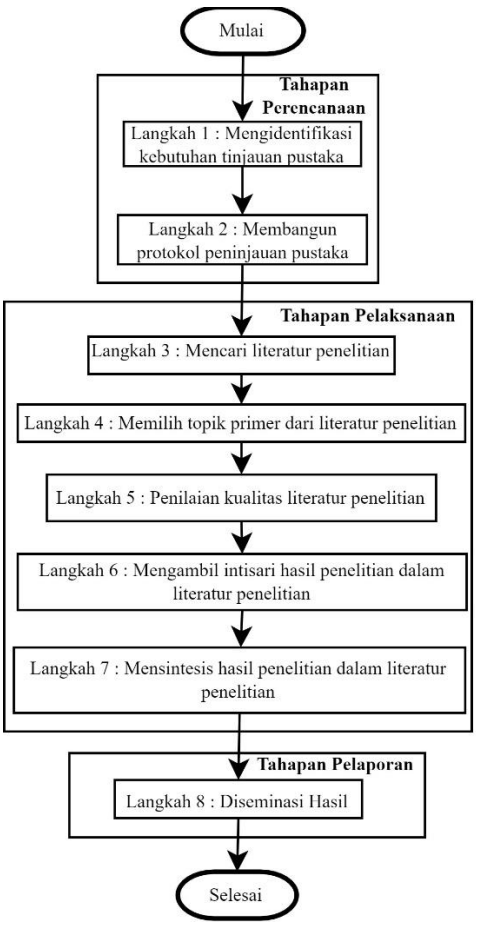
Received 12 April 2022, Accepted 22 June 2022, Published 27 June 2022.
DOI: https://doi.org/10.15294/jte.v14i1.36108

model klasifikasi (*classifier*) untuk dapat membedakan keaslian dari wajah seseorang. Salah satu metode yang populer untuk membangun model klasifikasi *anti-spoof* wajah adalah dengan menggunakan *deep learning* [5]. Oleh karena itu, set data yang bervariasi dibutuhkan untuk membangun, melatih (*training*) dan menguji (*testing*) model klasifikasi *anti-spoofing* wajah.

Di era informasi saat ini set data publik merupakan sumber daya berharga dalam berbagai macam aktivitas dan kegiatan, sehingga data-data yang didapat secara bebas menjadi bahan bakar dalam menjalankan penelitian dengan lebih cepat dan progresif [6]. Set data yang bersifat publik telah banyak dihasilkan dalam rentang waktu 2010-2021. Oleh karena itu, studi literatur ini bertujuan untuk mengulas proses pembangunan, perkembangan dan ketersediaan set data *anti-spoof* wajah dan jenis serangan *presentation attack* (PA) yang muncul pada sistem *anti-spoof*.

II. METODE

Systematic literature review (SLR) digunakan untuk melakukan tinjauan pustaka set data *anti-spoof* wajah dan jenis serangan PA. SLR terdiri dari serangkaian proses untuk melakukan identifikasi, penilaian, penafsiran semua bukti penelitian yang tersedia, dan bertujuan untuk mencari jawaban atas pertanyaan penelitian tertentu [7]. Metode ini memiliki tiga tahapan yaitu, perencanaan, pelaksanaan dan pelaporan tinjauan pustaka, seperti yang digambarkan pada Gambar 1. Pada tahapan pertama, kebutuhan studi pustaka diidentifikasi dengan melakukan pencarian pustaka, penelitian dan publikasi terkait deteksi *anti-spoof* wajah dan PA. Pada tahap kedua, membangun protokol studi pustaka yang digunakan untuk mengarahkan proses peninjauan. Tahapan ini memformulasikan pertanyaan penelitian, strategi penelitian, proses pemilihan pustaka yang digunakan atau diabaikan, peninjauan kualitas pustaka, dan pengambilan data akhir pada penelitian. Pada tahap ini juga dilakukan proses pendefinisian pertanyaan penelitian yang dibangun dengan bantuan kerangka kerja yang terdiri dari *population*, *intervention*, *comparison*, *outcomes* dan *context* (PICOC) [7]. Struktur pertanyaan penelitian menggunakan kerangka kerja PICOC dapat dilihat pada Tabel I, sedangkan pertanyaan dan tujuan penelitian dapat dilihat pada Tabel II.



Gambar 1. Diagram langkah studi literatur

Proses pencarian terdiri dari pemilihan pustaka digital, menentukan kata kunci pencarian, melakukan pencarian, menyempurnakan kata kunci pencarian, dan mengambil dokumen pustaka utama hasil pencarian, seperti yang dapat dilihat diagram alur pada Gambar 2. Studi literatur dilakukan terhadap pencarian pustaka yang berasal dari repositori digital IEEE Xplore, ScienceDirect dan arXiv. Pencarian dilakukan dengan menggunakan kata kunci utama *face impostor*, *face liveness*, *face antispoofing* dengan penambahan kata akhir *dataset* atau *database* pada akhir kata kunci untuk melakukan penyesuaian akurasi pencarian. Pencarian dibatasi pada pustaka yang dipublikasi dari tahun 2010 hingga 2021. Dari hasil pencarian literatur tersebut dipilih artikel-artikel penelitian dengan kriteria sebagai berikut:

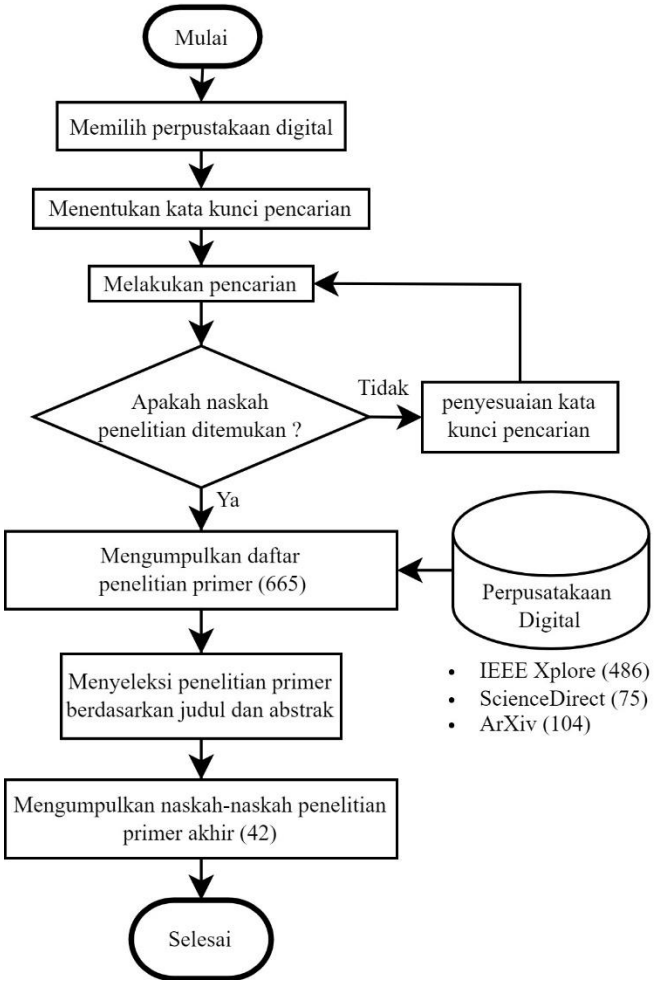
- Penelitian menghasilkan set data yang bersifat publik.
- Penelitian dilakukan menggunakan set data publik.
- Artikel penelitian sudah *peer-reviewed*.
- Jika penelitian memiliki naskah prosiding dan jurnal, maka naskah jurnal akan digunakan.
- Jika terdapat naskah dengan penelitian yang sama, maka akan dipilih naskah dengan tahun publikasi terbaru.

TABEL I. PICOC STUDI LITERATUR

No	Kerangka Kerja	Definisi Pertanyaan Penelitian
1.	*Population*	*face anti-spoofing database, face liveness database*
2.	*Intervention*	*face PA detection, 2D face PA, 3D PA attack*
3.	*Comparison*	-
4.	*Outcomes*	*face imposter database, face anti-spoofing database, PA detection database*
5.	*Context*	Penelitian dibidang akademik yang menghasilkan set data dengan berbagai skala.

TABEL II. PERTANYAAN PENELITIAN STUDI LITERATUR

No	Id	Pertanyaan Penelitian	Tujuan Penelitian
1.	IP01	Jenis PA apa saja yang terjadi pada sistem pengenalan wajah?	Mengidentifikasi jenis-jenis PA sistem pengenalan wajah yang menentukan karakteristik set data *anti-spoof* wajah.
2.	IP02	Bagaimana set data *anti-spoof* wajah dibangun?	Mengidentifikasi karakteristik set data *anti-spoof* wajah yang dihasilkan.
3.	IP03	Set data *anti-spoof* apa saja yang dapat diakses secara bebas?	Mengidentifikasi set data publik yang dapat digunakan dalam penelitian *anti-spoof* wajah.
4.	IP04	Bagaimana ketersediaan akses terhadap set data publik *anti-spoof* wajah?	Mengidentifikasi bagaimana ketersediaan set data publik bila ingin digunakan.



Gambar 2. Diagram proses pencarian dan pemilihan naskah penelitian primer

Proses pencarian dan seleksi literatur penelitian menghasilkan 42 naskah penelitian primer. Studi dan analisis secara mendalam dilakukan untuk mendapatkan data yang relevan terhadap pertanyaan penelitian yang telah didefinisikan. Penentuan properti pertanyaan penelitian dilakukan untuk membantu pengambilan data dari literatur dan menghubungkannya dengan pertanyaan penelitian. Properti pertanyaan penelitian dapat dilihat pada Tabel III. Untuk menganalisis data yang didapatkan, studi literatur ini menggunakan metode deskriptif dengan bantuan diagram alur dan tabel.

TABEL III. PROPERTI PENGAMBILAN DATA DAN HUBUNGANNYA DENGAN PERTANYAAN PENELITIAN

No	Properti	Pertanyaan Penelitian
1.	Set data yang digunakan dalam penelitian	IP01, IP02
2.	Penelitian menghasilkan set data *anti-spoof* wajah	IP03
3.	Cara mengakses set data publik	IP04

III. HASIL DAN PEMBAHASAN

A. Jenis Serangan *Presentation Attack*

Serangan-serangan pada sistem *anti-spoof* wajah dapat dibagi menjadi dua kategori: manipulasi gambar digital [8], [9] dan manipulasi kehadiran fisik (PA) [10]. Serangan pada kategori PA, dapat dibagi menjadi dua jenis *use case*, yaitu 1) *impersonation*, penyerang menggunakan tipuan sehingga wajahnya mirip dengan orang lain, 2) *obfuscation*, penyerang melakukan penyamaran dengan menyembunyikan wajahnya agar identitasnya tidak diketahui. Jenis serangan *impersonation* dapat dilakukan dengan menggunakan alat seperti foto cetak, tampilan layar elektronik atau topeng, untuk menduplikasi wajah asli. Sedangkan jenis serangan yang *obfuscation* dilakukan dengan menyamarkan wajah menggunakan kaca mata, hiasan wajah (*make up*), rambut palsu (*wig*), operasi plastik, dan penutup wajah secara menyeluruh atau sebagian.

Berdasarkan bentuk geometrinya, kedua jenis tersebut dapat dibagi menjadi dua, yaitu serangan 2D dan 3D. 2D PA dilakukan dengan cara menampilkan wajah dengan menggunakan foto atau video pada sensor [11]. Teknik serangan ini dapat menggunakan foto yang tercetak pada kertas saja, foto yang membungkus wajah, foto tercetak dengan bagian mulut atau mata yang dipotong, dan tampilan wajah pada video yang diputar ulang (*video replay attack*). Untuk serangan *video replay attack* akan memiliki karakter serangan yang lebih dinamis karena dapat memanipulasi kedipan mata, pergerakan mulut dan perubahan ekspresi wajah.

3D PA saat ini mulai marak dilakukan karena mudahnya akses terhadap fasilitas 3D *printing* [12]. Pada 3D PA, serangan dengan topeng wajah akan tampak asli karena memiliki detail tekstur, warna, dan geometri yang lebih baik. Topeng wajah dapat dibuat dengan berbagai material seperti kertas, resin, plastik atau silikon. Topeng wajah yang dibuat dengan menggunakan bahan kertas akan menghasilkan serangan dengan kualitas yang rendah dibandingkan dengan topeng wajah berbahan resin, plastik, atau silikon.

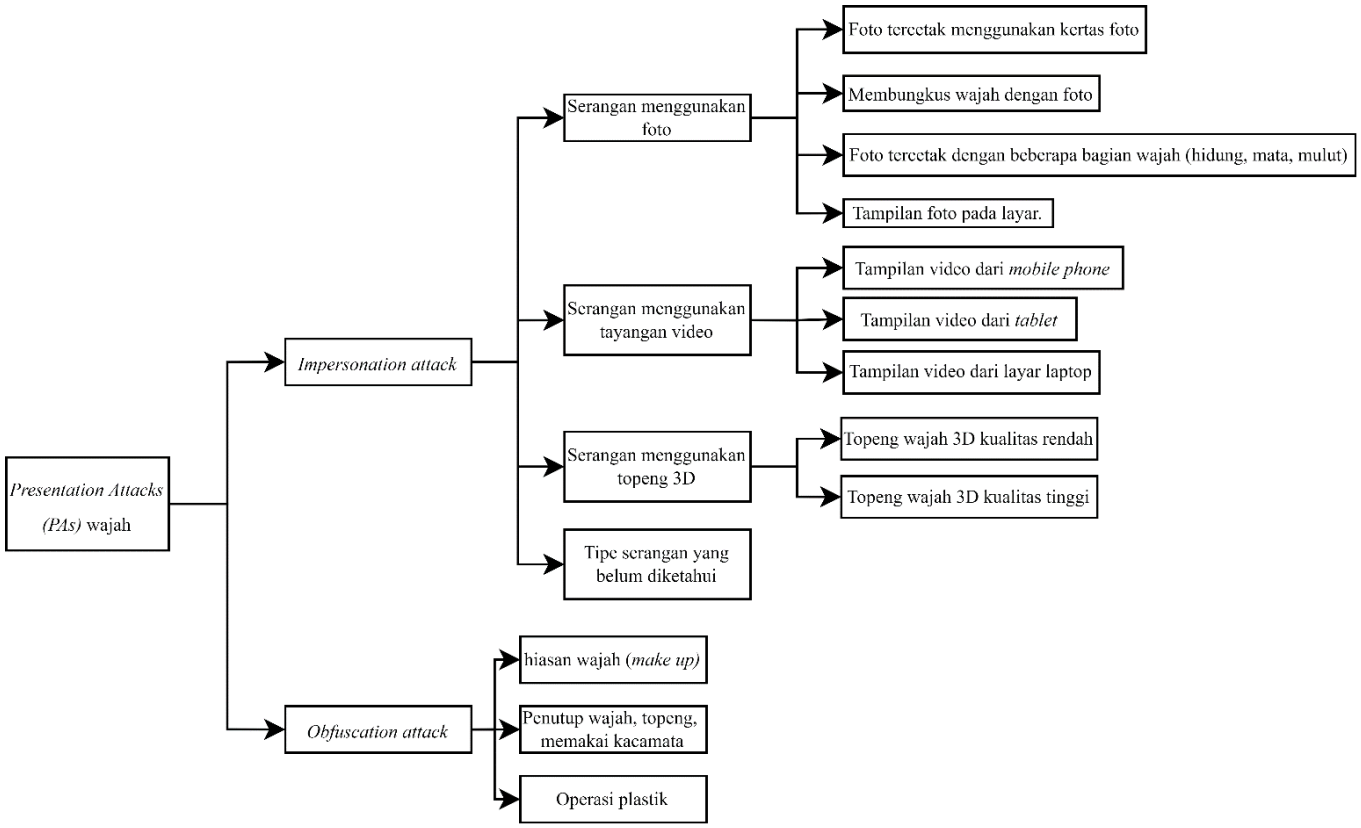
Berdasarkan bagian wajah yang ditutupinya, PA dapat dibagi menjadi dua jenis [5], serangan sebagian (parsial) atau keseluruhan. Penyerang yang menggunakan teknik serangan parsial, menutupi sebagian wajahnya dengan menggunakan alat seperti topeng atau kertas foto bercetak gambar wajah, yang bagian mata atau mulutnya sudah dipotong sehingga menjadi lebih sulit untuk dikenali. Gambar 3 merupakan diagram jenis-jenis PA pada sistem *anti-spoof* wajah.

B. Proses Pembangunan Set Data *Anti-Spoof* Wajah

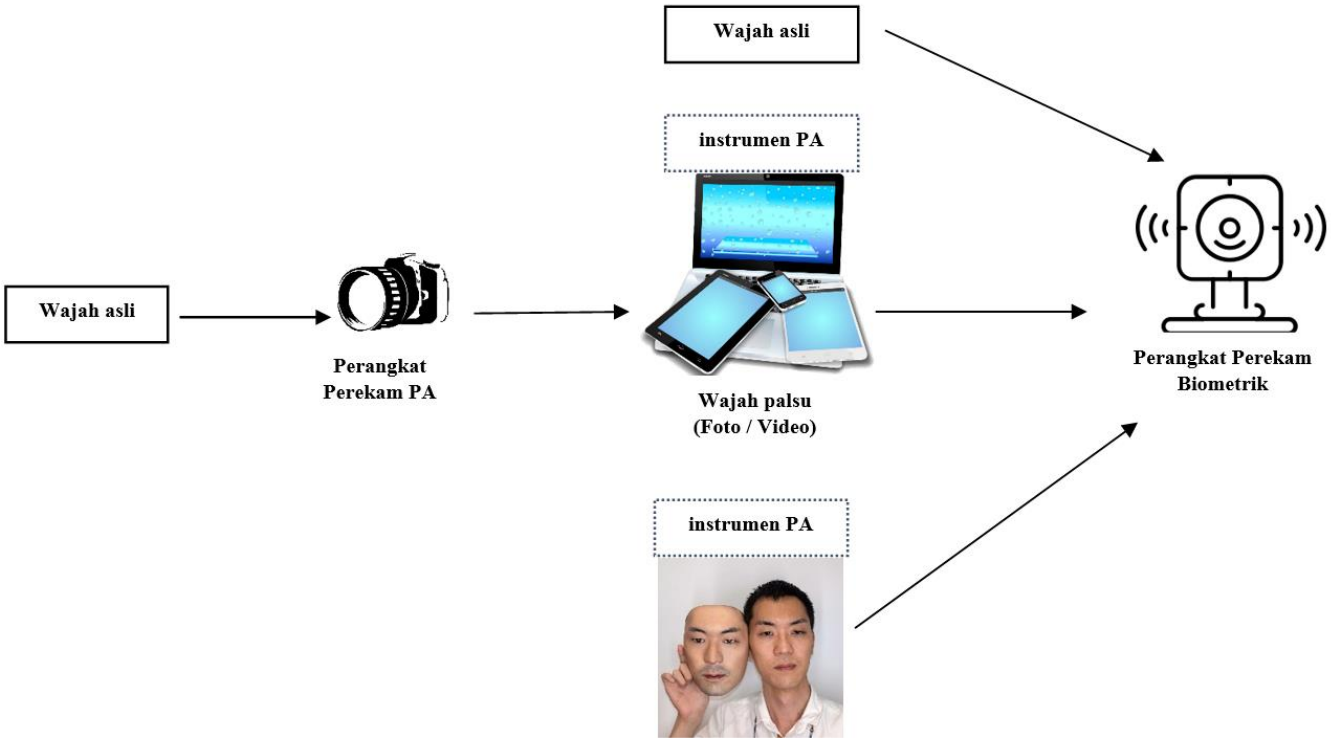
Set data publik untuk *anti-spoof* wajah umumnya terbagi menjadi dua jenis file yaitu bentuk foto atau video. Set data dalam studi literatur ini terbagi menjadi dua kategori, "wajah asli" yang berisi file foto atau video wajah pengguna asli dan "wajah palsu" yang berisi file foto atau video wajah palsu (foto cetak, *video replay*, atau wajah bertopeng). Data wajah asli dan palsu umumnya diambil dengan menggunakan perangkat yang sama sehingga perangkat ini memiliki peran penting terhadap set data dan secara langsung memiliki dampak terhadap akurasi sistem *anti-spoof* wajah yang dibangun.

Seperti yang ditampilkan pada Gambar 4, pembuatan data wajah asli dilakukan dengan cara merekam wajah secara langsung dengan menggunakan perangkat elektronik. Proses perekaman ini berusaha merekam wajah asli secara natural, seperti pergerakan wajah, kedip mata, atau pencahayaan pada wajah. Kualitas perangkat elektronik yang digunakan seperti resolusi kamera dan kualitas sensor warna mempengaruhi hasil akhir dari data wajah asli ini.

Sedangkan data wajah palsu berupa gambar atau video dibangun dengan cara membuat instrumen wajah palsu yang dicetak atau video yang dimainkan ulang pada perangkat elektronik. *Printer* digunakan untuk mencetak wajah asli pada kertas foto sedangkan perangkat elektronik seperti *smartphone*, laptop, atau kamera digital digunakan untuk merekam foto atau video digital. Hasil rekam foto atau video kemudian direkam dengan kamera biometrik untuk dijadikan data wajah palsu. Beberapa set data [13] merekam ulang data wajah asli atau



Gambar 3. Diagram serangan PA



Gambar 4. Ilustrasi proses pengembangan dataset *anti-spoof* wajah

palsu yang dihasilkan sebelumnya untuk membuat instrumen PA dengan sistem biometrik khusus. Perangkat khusus ini memiliki kemampuan untuk memindai kontur wajah secara 3 dimensi dengan menggunakan *infrared* (*near* atau *short-wave*), sudut pencahayaan khusus, kamera *multidirectional*, atau suhu obyek. Teknik seperti ini disebut sebagai "*recaptured*" karena proses merekam ulang data PA dengan sistem biometrik khusus[14].

Set data wajah palsu dibangun dengan membuat instrumen berupa foto wajah menggunakan kertas biasa, kertas foto, atau kertas yang terlipat. Gambar-gambar ini dicetak dengan menggunakan *printer* 2D. Kualitas warna dan resolusi *printer* yang digunakan sangat berpengaruh terhadap kualitas instrumen PA yang dibuat sehingga akan berdampak pada keberhasilan instrumen saat menyerang sistem. Sedangkan instrumen serangan wajah 3D dibangun menggunakan material berupa silikon atau resin yang dicetak dengan menggunakan perangkat 3D *printer* sedangkan material lilin (*wax*) dipahat secara manual. Perbedaan jenis material ini akan berdampak pada tingkat sukses serangan sistem biometrik karena adanya

perbedaan kehalusan tekstur dari material yang digunakan [15]–[17].

C. Gambaran Umum dan Ketersediaan Set Data Publik

Set data yang berskala besar dan bervariatif merupakan hal yang penting untuk membangun sistem *anti-spoof* wajah yang tangguh. Untuk sistem *anti-spoof* wajah dengan metode *deep learning*, hal ini menjadi sangat penting pada fase *training* dan evaluasi model yang dibangun. Secara umum terdapat tiga *trend* dalam perkembangan set data *anti-spoof* wajah. Set data jenis pertama memiliki jumlah subyek yang besar sehingga jumlah data wajah yang dihasilkan akan sangat banyak. Set data seperti CelebA-Spoof [18] dan CASIA-SURF HiFiMask [19] berisi 600.000 gambar dan 50.000 video. Set data jenis kedua adalah set data dengan jenis *sample* wajah berbeda. Jenis set data ini tidak hanya terdapat sampel gambar wajah pada kondisi tertentu saja, tetapi juga terdapat data wajah palsu yang dibuat dengan material berbeda (plastik, resin, atau silikon). Set data jenis ketiga adalah set data yang dibangun dengan menggunakan perangkat dan sensor yang beragam. Set data ini tidak hanya berisi gambar wajah RGB yang diambil dengan kamera biasa, tetapi juga menggunakan perangkat dan sensor lain seperti *near infrared* (NIR), *short-wave infrared* (SWIR), *light field* (LF) atau *depth*.

Saat membangun sistem *anti-spoof* wajah, peneliti dapat membangun set datanya sendiri atau menggunakan set data publik yang telah tersedia. Set data publik untuk penelitian *anti-spoof* wajah pertama kali tersedia pada tahun 2010 [20] bernama NUAA set data. Set data ini merupakan pionir yang memfasilitasi para peneliti untuk melakukan *benchmarking* hasil penelitian dengan acuan data yang sama.

Setelah itu pada tahun 2011 hingga 2012, muncul set data publik bernama YALE *recaptured* [17], CASIA-FASD [21], PRINT-ATTACK [22], dan REPLAY-ATTACK [23]. Set data PRINT-ATTACK berisi data foto wajah yang digunakan untuk melakukan penelitian pada *anti-spoof* wajah. Set data ini kemudian ditambahkan dengan data-data berbentuk video agar dapat digunakan untuk melakukan permodelan *anti-spoof* wajah dengan serangan video dan diberi nama set data REPLAY-ATTACK. Set data YALE *recaptured* dibangun menggunakan YALE *face database* B yang kemudian direkam ulang dengan menggunakan kamera [14]. CASIA-FASD merupakan set data yang lebih menantang yang memiliki data berupa foto dan video namun dengan variasi PA, resolusi video dan perangkat yang lebih banyak.

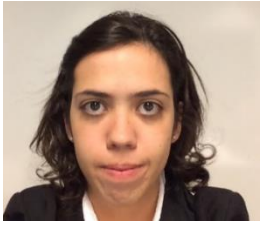
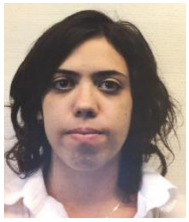
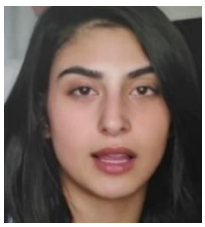
Ditahun 2013 hingga 2017 muncul set data publik Kose & Dugelay [15], MSU-MFSD [24], UAVD [25], REPLAY-Mobile [26], HKBU-MARs V2 [16], MSU USSA [13], SMAD [27], dan OULUPU-NPU [28] yang tidak hanya dapat digunakan untuk membangun sistem *anti-spoof* serangan gambar atau video 2 dimensi tetapi juga serangan 3 dimensi dengan menggunakan topeng. Set data *anti-spoof* wajah dengan serangan 3 dimensi dibangun dengan membuat topeng wajah berbahan kertas, resin, lilin (*wax*), 3D *prints* atau silikon. Set data ini juga dibangun dengan subjek yang berasal dari ras, suku, bangsa dan warna kulit yang bervariatif.

Ditahun 2018 hingga 2021 muncul set data Rose-Youtu [29], SiW [30], WFFD [31], SiW-M [32], CASIA-SURF [18], Swax [17], CelebA-Spoof [33], RECOD-MPAD [34], CASIA-SURF 3D Mask [35], CASIA-SURF HiFiMask [19], GREAT-FASD-S [36] dan LCC FASD [37]. Set data seperti CASIA-SURF, CelebA-Spoof, dan CASIA-SURF HiFiMask memiliki kompleksitas yang tinggi karena memiliki jumlah data yang besar dan menggunakan subjek yang sangat banyak. Selain itu set data ini juga dapat digunakan untuk membangun sistem *anti-spoof* wajah dengan serangan gambar atau video 2 dimensi dan 3 dimensi.

Seiring perkembangan teknologi pada perangkat bergerak *smartphone*, sistem operasi Android dan IOS telah mengadopsi teknologi *face unlock* dalam melakukan autentikasi pengguna [24]. Oleh karena itu, terdapat set data yang dibangun secara khusus untuk skenario serangan pada perangkat *mobile* seperti MSU-MFSD, REPLAY-Mobile, OULU-NPU dan RECOD-MPAD. Set data tersebut dibangun dengan menggunakan konfigurasi pencahayaan dan perangkat *mobile* yang berbeda-beda [13], [26], [28], [34]. Beberapa contoh set data yang menjadi subjek studi literatur dapat dilihat pada Tabel IV. Sedangkan Tabel V berisi informasi mendetail tentang set data yang digunakan dalam studi literatur ini.

Seiring perkembangan teknologi pada perangkat bergerak *smartphone*, sistem operasi Android dan IOS telah mengadopsi teknologi *face unlock* dalam melakukan autentikasi pengguna [24]. Oleh karena itu, terdapat set data yang dibangun secara khusus untuk skenario serangan pada perangkat *mobile* seperti MSU-MFSD, REPLAY-Mobile, OULU-NPU dan RECOD-MPAD. Set data tersebut dibangun dengan menggunakan konfigurasi pencahayaan dan perangkat *mobile* yang berbeda-beda [13], [26], [28], [34]. Beberapa contoh set data yang menjadi subjek studi literatur dapat dilihat pada Tabel IV. Sedangkan Tabel V berisi informasi mendetail tentang set data yang digunakan dalam studi literatur ini.

TABEL IV. CONTOH SET DATA *ANTI-SPOOF* WAJAH

No	Nama Set Data	Asli	Palsu
1.	NUAA		
2.	CASIA-FASD		
3.	Replay-Mobile		
4.	LCC-FASD		

TABEL V. SET DATA YANG DIGUNAKAN PADA STUDI LITERATUR

No	Nama Set Data	Tahun	Subjek	Ras Subjek	Jenis Serangan	Asli / Palsu
1.	NUAA [20]	2010	15	Asia	Foto tercetak Datar, foto membungkus wajah	5.105/7.509 (Gambar)
2.	YALE_Recaptured [38]	2011	10	Kaukasia Asia	Foto tercetak datar	640/1.920 (Gambar)
3.	CASIA-FASD [21]	2012	50	Asia	Foto tercetak Datar, foto membungkus wajah, foto terpotong, *replay* video	150/450 (Video)
4.	REPLAY-ATTACK [23]	2012	50	Kaukasia 76%, Asia 22%, Afrika 2%	Foto tercetak Datar, *replay* video	200/1.000 (Video)
5.	Kose & Dugelay [15]	2013	20	-	Topeng resin	200/198 (Gambar)
6.	MSU-MFSD [24]	2014	35	Kaukasia 70%, Asia 28%, Afrika 2%	Foto tercetak datar, *replay* video	70/210 (Video)
7.	UAVD [25]	2015	404	Kaukasia 44%, Asia 54%, Afrika 3%	*Replay* video	808/16.268 (Video)
8.	REPLAY-Mobile [26]	2016	40	Multi etnis	Foto tercetak datar, *replay* video	390/640 (Video)
9.	HKBU-MARs V2 [16]	2016	12	Asia	Topeng resin dan 3D print	504/504 (Video)
10.	MSU USSA [13]	2016	1.140	Multi etnis	Foto tercetak datar, replay video	1.140/9.120 (Video)
11.	SMAD [27]	2017	-		Topeng silikon	65/65 (Video)
12.	OULUPU-NPU [28]	2017	55	Kaukasia 5%, Asia 95%	Foto tercetak datar, *replay* video	720/2.880 (Video)
13.	Rose-Youtu [29]	2018	20	Asia	Foto tercetak datar, *replay* video, topeng kertas	500/2.850 (Video)
14.	SiW [30]	2018	165	Kaukasia 35%, Asia 35%, Afrika-American 7%, India 23%	Foto tercetak datar, *replay* video	1.320/3.300 (Video)
15.	WFFD [31]	2019	745	kaukasian 60%, Asia 20%, Afrika 10%, India 2%	Topeng lilin (*wax*)	2.300/2.300 (Gambar) 140/145 (Video)
16.	SiW-M [32]	2019	493	-	Foto tercetak datar, foto terpotong, replay video, topeng resin, plastik, silikon, kertas, makeup	680/968 (Video)
17.	CASIA-SURF [18]	2019	1.000	Asia (China)	Foto tercetak datar, foto membungkus wajah, foto terpotong	3.000/18.000 (Video)
18.	Swax [17]	2020	55	Multi etnis (diambil dari internet)	Topeng lilin (*wax*)	1.812 (Gambar) /110 (Video)
19.	CelebA-Spoof [33]	2020	10.177	Multi etnis (diambil dari internet)	Foto tercetak datar, foto membungkus wajah, foto terpotong, *replay* video	15.6384/ 469.153 (Gambar)
20.	RECOD-MPAD [34]	2020	45	Multi etnis	Foto tercetak datar, *replay* video	450/1.800 (Video)
21.	CASIA-SURF 3D Mask [35]	2020	48	Asia	Topeng 3D print	288/864 (Video)
22.	CASIA-SURF HiFiMask [19]	2021	75	Asia	Topeng resin	13.650/40.950 (Video)
23.	LCC FASD [37]	2021	243	Multi etnis (diambil dari internet)	Foto tercetak datar, *replay* video	1.942/16.885 (Gambar)

Pada umumnya, untuk dapat mengakses set data publik tersebut, pengguna harus menandatangani dokumen perjanjian lisensi pengguna akhir dan mengirimkannya kembali kepada peneliti atau institusi pemilik set data tersebut. Namun beberapa set data seperti Kose & Dugelay dan SiW-M tidak dapat diakses karena URL yang tidak valid. Selain itu set data seperti CASIA-SURF hanya tersedia pada media *cloud* Baidu, sedangkan untuk dapat mengakses data pada layanan cloud tersebut diharuskan memiliki akun yang untuk membuatnya harus menggunakan nomor telepon berdomisili China [39]. Hal tersebut membuat set data tersebut sulit untuk diakses secara bebas oleh para peneliti yang berasal dari luar China. Tabel VI berisi informasi lebih mendetail ketersediaan set data yang digunakan dalam studi literatur ini.

TABEL VI. KETERSEDIAAN AKSES SET DATA YANG DIGUNAKAN PADA STUDI LITERATUR

No	Nama Set Data	*Download Link*
1.	NUAA [20]	http://parnec.nuaa.edu.cn/_upload/tpl/02/db/731/template731/pages/xtan/NUAAImposterDB_download.html
2.	YALE_Recaptured [38]	http://vision.ucsd.edu/content/yale-face-database
3.	CASIA-FASD [21]	https://drive.google.com/drive/folders/1nJCPdJ7R67xOiklF1omkfz4yHeJwhQsz
4.	REPLAY-ATTACK [23]	https://www.idiap.ch/en/dataset/replayattack
5.	Kose & Dugelay [15]	-
6.	MSU-MFSD [24]	http://www.cse.msu.edu/rgroups/biometrics/Publications/Databases/MSUMobileFaceSpoofing/index.htm
7.	UAVD [25]	https://signalprocessingsociety.org/technical-committees/list/ifs-tc/ifs-tc-resources/
8.	REPLAY-Mobile [26]	https://www.idiap.ch/en/dataset/replay-mobile
9.	HKBU-MARs V2 [16]	https://rds.comp.hkbu.edu.hk/mars/
10.	MSU USSA [13]	http://biometrics.cse.msu.edu/Publications/Databases/MSU_LFW+_back/
11.	SMAD [27]	http://iab-rubric.org/resources.html
12.	OULUPU-NPU [28]	https://sites.google.com/site/oulunpudatabase/
13.	Rose-Youtu [29]	https://rose1.ntu.edu.sg/dataset/faceLivenessDetection/
14.	SiW [30]	http://cvlab.cse.msu.edu/siw-spoof-in-the-wild-database.html
15.	WFFD [31]	https://github.com/shanface33/Wax_Figure_Face_DB
16.	SiW-M [32]	-
17.	CASIA-SURF [18]	https://sites.google.com/qq.com/face-anti-spoofing/dataset-download/casia-surfcvpr2019?authuser=0
18.	Swax [17]	http://sense.dcc.ufmg.br/en/dataset/swax-dataset/
19.	CelebA-Spoof [33]	https://github.com/Davidzhangyuanhan/CelebA-Spoof
20.	RECOD-MPAD [34]	https://zenodo.org/record/3749309
21.	CASIA-SURF 3D Mask [35]	https://sites.google.com/qq.com/face-anti-spoofing/dataset-download/casia-surf-cefacvpr2020?authuser=0
22.	CASIA-SURF HiFiMask [19]	https://sites.google.com/qq.com/face-anti-spoofing/dataset-download/casia-surf-hifimaskiccv2021?authuser=0
23.	LCC FASD [37]	https://drive.google.com/file/d/1NeyTFAwdJSjxA9ZtdviwdUjdptEVjM_i/view

IV. PENUTUP

Studi literatur telah dilakukan terhadap 42 naskah penelitian primer dan diketahui bahwa terdapat 2 jenis PA, yaitu *impersonation* dan *obfuscation*. Serangan berupa *impersonation* dilakukan dengan menampilkan foto/video wajah atau dengan menggunakan topeng/patung wajah yang dibuat dengan material berbeda. Sedangkan serangan *obfuscation* dilakukan dengan menyamarkan atau menutupi sebagian wajah dengan perhiasan atau aksesoris khusus. Studi literatur ini juga mengulas beberapa tipe set data publik yang tersedia untuk membangun sistem *anti-spoof* wajah. Set data yang digunakan dapat berupa foto maupun video dan terdiri dari kategori wajah asli dan palsu. Beberapa jenis set data dapat diakses secara bebas, namun dengan aturan khusus seperti *user agreement*. Akan tetapi, terdapat set data yang tidak bisa diakses karena URL yang sudah kadaluwarsa atau karena protokol khusus yang harus dipenuhi pada penyedia penyimpanan *cloud* set data. Limitasi studi literatur ini yaitu belum mengulas tentang PA dan set data yang bersifat multimoda, yang set datanya memiliki informasi *depth*, *infra red* dan suhu, sehingga studi literatur berikutnya perlu dilakukan untuk mendapatkan informasi yang komprehensif terhadap berbagai serangan dan set data *anti-spoof* wajah.

REFERENSI

[1] W. W. Bledsoe, "The Model Method in Facial Recognition," Palo Alto, California, 1964.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006, doi: 10.1109/TIFS.2006.873653.

[3] S. Abbass, "A Model for Trust-building in E-commerce from Consumer to Consumer Perspective in KSA," *International Journal of e-Education, e-Business, e-Management and e-Learning*, vol. 1, no. 3, pp. 223–227, 2011, doi: 10.7763/ijeeee.2011.v1.35.

[4] L. Souza, L. Oliveira, M. Pamplona, and J. Papa, "How far did we get in face spoofing detection?," *Engineering Applications of Artificial Intelligence*, vol. 72, no. December 2017, pp. 368–381, 2018, doi: 10.1016/j.engappai.2018.04.013.

[5] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," pp. 1–25, 2021, [Online]. Available: http://arxiv.org/abs/2106.14948

[6] E. H. Gebre and E. Morales, "How 'accessible' is open data?: Analysis of context-related information and users' comments in open datasets," *Information and Learning Science*, vol. 121, no. 1–2, pp. 19–36, 2020, doi: 10.1108/ILS-08-2019-0086.

[7] B. Kitchenham, "Procedures for Performing Systematic Reviews," Keele, Staffs ST5 5BG, UK, 2004.

[8] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A Survey of face manipulation and fake detection," *Information Fusion*, vol. 64, pp. 131–148, 2020, doi: 10.1016/j.inffus.2020.06.014.

[9] G. Goswami, A. Agarwal, N. Ratha, R. Singh, and M. Vatsa, "Detecting and Mitigating Adversarial Perturbations for Robust Face Recognition," *International Journal of Computer Vision*, vol. 127, no. 6–7, pp. 719–742, 2019, doi: 10.1007/s11263-019-01160-w.

[10] A. Liu *et al.*, "Cross-ethnicity face anti-spoofing recognition challenge: A review," *IET Biometrics*, vol. 10, no. 1, pp. 24–43, 2021, doi: 10.1049/bme2.12002.

[11] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Computing Surveys*, vol. 50, no. 1, 2017, doi: 10.1145/3038924.

[12] S. Jia, G. Guo, and Z. Xu, "A survey on 3D mask presentation attack detection and countermeasures," *Pattern Recognition*, vol. 98, p. 107032, 2020, doi: 10.1016/j.patcog.2019.107032.

[13] K. Patel, H. Han, and A. K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones," *IEEE Transactions on Information Forensics and*

Security, vol. 11, no. 10, pp. 2268–2283, 2016, doi: 10.1109/TIFS.2016.2578288.

[14] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," *Proceedings - International Conference on Image Processing, ICIP*, no. July, pp. 3557–3560, 2011, doi: 10.1109/ICIP.2011.6116484.

[15] N. Kose and J. L. Dugelay, "Shape and texture based countermeasure to protect face recognition systems against mask attacks," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 111–116, 2013, doi: 10.1109/CVPRW.2013.24.

[16] S. Liu, B. Yang, P. C. Yuen, and G. Zhao, "A 3D Mask Face Anti-Spoofing Database with Real World Variations," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1551–1557, 2016, doi: 10.1109/CVPRW.2016.193.

[17] R. H. Vareto, A. Marcia Saldanha, and W. R. Schwartz, "The Swax Benchmark: Attacking Biometric Systems with Wax Figures," *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, vol. 2020-May, pp. 986–990, 2020, doi: 10.1109/ICASSP40776.2020.9053946.

[18] S. Zhang *et al.*, "CASIA-SURF: A Large-Scale Multi-Modal Benchmark for Face Anti-Spoofing," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 2, pp. 182–193, 2020, doi: 10.1109/tbiom.2020.2973001.

[19] A. Liu *et al.*, "Contrastive Context-Aware Learning for 3D High-Fidelity Mask Face Presentation Attack Detection," 2021, [Online]. Available: http://arxiv.org/abs/2104.06148

[20] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model," *European Conference on Computer Vision*, vol. VI, pp. 504–517, 2010, doi: 10.1007/978-3-642-15567-3_37.

[21] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," *Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012*, pp. 26–31, 2012, doi: 10.1109/ICB.2012.6199754.

[22] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," *2011 International Joint Conference on Biometrics, IJCB 2011*, 2011, doi: 10.1109/IJCB.2011.6117503.

[23] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," *Proceedings of the International Conference of the Biometrics Special Interest Group, BIOSIG 2012*, 2012.

[24] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, 2015, doi: 10.1109/TIFS.2015.2400395.

[25] A. Pinto, W. R. Schwartz, H. Pedrini, and A. D. R. Rocha, "Using visual rhythms for detecting video-based facial spoof attacks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 5, pp. 1025–1038, 2015, doi: 10.1109/TIFS.2015.2395139.

[26] A. Costa-Pazo, S. Bhattacharjee, E. Vazquez-Fernandez, and S. Marcel, "The REPLAY-MOBILE face presentation-attack database," *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, vol. P-260, no. September, 2016, doi: 10.1109/BIOSIG.2016.7736936.

[27] I. Manjani, S. Tariyal, M. Vatsa, R. Singh, and A. Majumdar, "Detecting silicone mask-based presentation attack via deep dictionary learning," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 1713–1723, 2017, doi: 10.1109/TIFS.2017.2676720.

[28] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, and A. Hadid, "OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations," *Proceedings - 12th IEEE International Conference on Automatic Face and Gesture Recognition, FG 2017 - 1st International Workshop on Adaptive Shot Learning for Gesture Understanding and Production, ASL4GUP 2017, Biometrics in the Wild, Bwild 2017, Heteroge*, no. June, pp. 612–618, 2017, doi: 10.1109/FG.2017.77.

[29] H. Li, W. Li, H. Cao, S. Wang, F. Huang, and A. C. Kot, "Unsupervised Domain Adaptation for Face Anti-Spoofing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1794–1809, 2018, doi: 10.1109/TIFS.2018.2801312.

[30] Y. Liu, A. Jourabloo, and X. Liu, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 389–398, 2018, doi: 10.1109/CVPR.2018.00048.

[31] S. Jia, X. Li, C. Hu, G. Guo, and Z. Xu, "3D Face Anti-Spoofing with Factorized Bilinear Coding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 10, pp. 4031–4045, 2021, doi: 10.1109/TCSVT.2020.3044986.

[32] Y. Liu, J. Stehouwer, A. Jourabloo, and X. Liu, "Deep tree learning for zero-shot face anti-spoofing," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2019-June, pp. 4675–4684, 2019, doi: 10.1109/CVPR.2019.00481.

[33] Y. Zhang *et al.*, "CelebA-Spoof: Large-Scale Face Anti-spoofing Dataset with Rich Annotations," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12357 LNCS, pp. 70–85, 2020, doi: 10.1007/978-3-030-58610-2_5.

[34] W. R. Almeida *et al.*, "Detecting face presentation attacks in mobile devices with a patch-based CNN and a sensor-aware loss function," *PLoS ONE*, vol. 15, no. 9 september, pp. 1–24, 2020, doi: 10.1371/journal.pone.0238058.

[35] Z. Yu, J. Wan, Y. Qin, X. Li, S. Z. Li, and G. Zhao, "NAS-FAS: Static-Dynamic Central Difference Network Search for Face Anti-Spoofing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 9, pp. 3005–3023, 2021, doi: 10.1109/TPAMI.2020.3036338.

[36] X. Chen, S. Xu, Q. Ji, and S. Cao, "A Dataset and Benchmark towards Multi-Modal Face Anti-Spoofing under Surveillance Scenarios," *IEEE Access*, vol. 9, pp. 28140–28155, 2021, doi: 10.1109/ACCESS.2021.3052728.

[37] D. Timoshenko, K. Simonchik, V. Shutov, P. Zhelezneva, and V. Grishkin, "Large Crowdcollected Facial Anti-Spoofing Dataset," *12th International Conference on Computer Science and Information Technologies, CSIT 2019*, pp. 123–126, 2019, doi: 10.1109/CSITechnol.2019.8895208.

[38] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 643–660, 2001, doi: 10.1109/34.927464.

[39] Tenba Group, "How to Get a Baidu Account," 2022. https://tenbagroup.com/how-to-get-a-baidu-account/ (accessed Apr. 08, 2022).