OPEN ACCESS
Indo-JC
Indonesia Journal of Computing
ISSN 2460-9056
socj.telkomuniversity.ac.id/indojc

IND. JOURNAL ON COMPUTING
VOL. 5, ISSUE. 1, MARCH 2020. PP. 53-62
DOI:10.21108/INDOJC.2020.5.1.376

Deteksi Spoofing Wajah Manusia Berbasis Video menggunakan Metode Local Derivative Pattern-Three Orthogonal Planes

Febryanti Sthevanie [#1], Diah Ajeng Dwi Yuniasih [#2], Kurniawan Nur Ramadhani [#3]

Laboratorium Multimedia, Fakultas Informatika, Universitas Telkom
Jalan Telekomunikasi No. 01, Terusan Buah Batu, Bandung, Indonesia

[1] sthevanie@telkomuniversity.ac.id
[2] diahajengdwu@students.telkomuniversity.ac.id
[3] kurniawannr@ telkomuniversity.ac.id

Abstract

Today many systems use face recognition for system's security. However, facial recognition system is still vulnerable to spoofing attacks, an attack by faking photos or videos of the face owner of the system. To avoid this crime, the author built a system that can detect spoofing attacks using Local Derivative Pattern method from the Three Orthogonal Planes. The dataset sources that used in this research is video format from four different public databases, Idiap Replay Attack Database, MSU MFSD Database, Casia FASD Database and NUAA Imposter Database. The test results in intra-dataset scenario obtained the best performance with average of F1-Score 97.77% and average of HTER 8.47% and in cross-dataset scenario the system achieved average of F1-Score 74.77% and average of HTER 29.05%.

Keywords: Spoofing Detection, Local Derivative Pattern-Three Orthogonal Planes, Support Vector Machine, intra-database, cross-database

Abstrak

Saat ini banyak sistem yang menggunakan pengenalan wajah sebagai keamanan. Namun, penggunaan wajah tersebut masih memiliki kerentanan terhadap serangan spoofing, yaitu serangan dengan cara memalsukan foto atau video dari pengguna asli sistem tersebut. Untuk menghindari adanya tindakan kriminal tersebut, diusulkan sebuah sistem yang dapat mendeteksi serangan spoofing menggunakan metode Local Derivative Pattern dari Three Orthogonal Planes. Dataset yang digunakan adalah bersumber dari empat dataset publik yang berbeda yaitu Idiap Replay-Attack Database, MSU MFSD Database, Casia FASD Database dan NUAA Imposter Database yang berformat video. Dari hasil pengujian, pada skenario intra-dataset didapatkan performansi terbaik dengan rata-rata F1-Score 97.77% dan rata-rata HTER 8.47%, sedangkan pada skenario cross-dataset rata-rata F1-Score 74.77% dan rata-rata HTER 29.05%.

Kata Kunci: Deteksi Spoofing, Local Derivative Pattern-Three Orthogonal Planes, Support Vector Machine, intra-database, cross-database

I. PENDAHULUAN

TEKNOLOGI biometrik biasa didefinisikan sebagai metode untuk mengidentifikasi identitas diri seseorang. Secara umum, ciri khas dari diri seseorang bisa berupa wajah, sidik jari, iris mata, cara berjalan, tanda tangan, suara, dan lain-lain[5]. Saat ini otentikasi sistem biometrik pengenalan wajah menjadi alternatif untuk memperkuat tingkat keamanan dari sebuah sistem informasi. Namun, sistem tersebut masih rentan terhadap sebuah serangan yang disebut dengan serangan spoofing. Penyerangan tersebut dapat dilakukan dengan cara menampilkan foto atau video rekaman dari wajah asli dari pengguna sistem yang sah [6]. Seiring dengan

RECEIVED ON JAN 2020. ACCEPTED ON MARCH 2020

meningkatnya pertumbuhan internet khususnya dari jejaring sosial dimana banyak orang yang tidak keberatan untuk memyebarkan informasi pribadi mereka khususnya foto dan video dari muka mereka. Hal tersebut akan memudahkan penyerang dalam mendapatkan foto atau video seseorang untuk digunakan oleh mereka dalam menyerang sistem. Berdasarkan masalah tersebut, diusulkan sebuah sistem yang dapat mendeteksi spoofing pada wajah manusia, apakah wajah tersebut merupakan wajah asli atau palsu. Berikut adalah contoh dari serangan spoofing dengan cara menampilkan foto wajah (yang dicetak) dari pemilik atau pengguna sistem yang dapat dilihat pada Gambar 1. Sedangkan contoh dari serangan spoofing dengan cara menampilkan rekaman video wajah dari pemilik atau pengguna sistem yang sah dapat dilihat pada Gambar 2.

Gambar 1. Contoh *Spoofing Print Photo* bersumber dari *dataset* CASIA

Gambar 2. Contoh *Spoofing Replayed Video* bersumber dari ***dataset*** CASIA

Penelitian mengenai deteksi *spoofing* sudah banyak dilakukan oleh beberapa peneliti didunia. Salah satunya dengan cara mengkombinasikan modalitas sistem biometrik lainnya dengan wajah. Namun, metode tersebut mem- butuhkan *user cooperation* yang membuat waktu komputasinya menjadi lebih lama [12]. Maka diperlukan sistem yang lebih handal tanpa memerlukan *user cooperation* agar waktu komputasinya lebih cepat. Pada penelitian ini, diusulkan metode berbasis analisis tekstur untuk mendeteksi serangan *spoofing* pada video yaitu Local Derivative Pattern-Three Orthogonal Planes (LDP-TOP). Dengan metode analisis tekstur akan lebih mudah dalam mengidentifikasi perbedaan antara wajah asli manusia dan wajah palsu berdasarkan penelitian [6]. Pada penelitian tersebut, metode analisis tekstur yang digu- nakan dalam menangani masalah serangan *spoofing* adalah analisis *micro texture* menggunakan metode ekstraksi ciri Local Binary Pattern (LBP) dengan akurasi yang didapat sebesar 98%. Pada dasarnya, LBP adalah pola lokal orde pertama *non-directional* dari LDP [1]. Penelitian ini mengimplementasikan metode Local Derivative Pattern (LDP) dari *Three Orthogonal Planes* (TOP) untuk mengekstraksi ciri dari video untuk digunakan dalam proses deteksi spooofing. LDP (*Local Derivative Pattern*) merupakan perluasan dari metode LBP yang dapat membedakan karakteristik orde pertama untuk semua arah yang sudah ditentukan [1]. Operator pada metode LDP dapat mengambil ciri dari setiap citra atau gambar ke beberapa tingkat orde untuk semua arah yang sudah ditentukan, sehingga informasi yang diperoleh dari citra atau gambar akan lebih rinci [1]. Selain itu, pola LDP juga dapat menangani masalah kesensitifan terhadap *noise* yang membuat sistem menjadi lebih handal.

II. Studi Terkait

Penelitian mengenai deteksi spoofing wajah telah banyak dilakukan oleh beberapa peneliti atau institusi di dunia. Dalam penelitian [6], peneliti tersebut menganalisis perbedaan antara citra wajah asli dan wajah palsu dari citra atau gambar yang di cetak. Perbedaan citra atau gambar tersebut dapat dilihat dari micro-texturenya dengan cara mendeteksi citra atau gambar wajah (printed photos) yang cacat. Operator analisis yang digunakan pada penelitian ini adalah LBP (Local Binary Pattern) dan algoritma klasifikasi yang digunakan adalah algoritma SVM (Support Vector Machine). Metode tersebut cukup handal dalam mendeteksi serangan spoofing dengan melakukan komputasi yang cepat dan mendapatkan nilai Error Equal Rate (EER) sebesar 2.9%.

Dalam penelitian [1], peneliti menawarkan metode LDP (Local Derivative Pattern) yang dapat menangkap informasi lebih detail dari suatu citra atau gambar daripada metode LBP (Local Binary Pattern). Karena meto- de LDP (Local Derivative Pattern) dapat menghitung nilai biner dari citra hingga ke beberapa tingkat orde dari

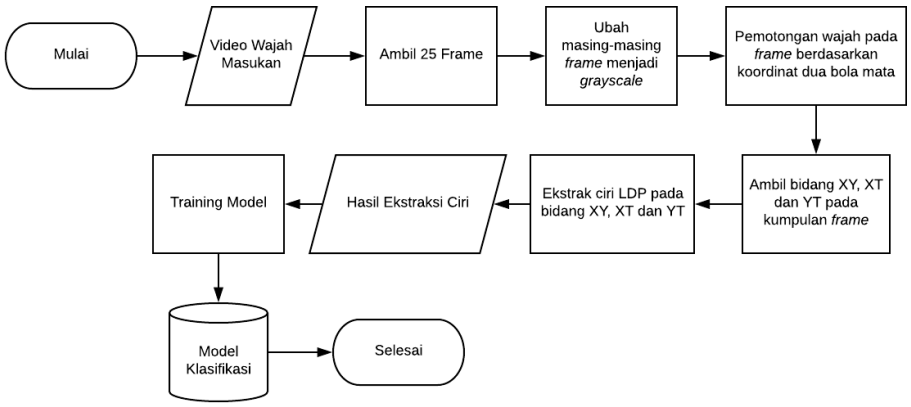
empat arah yang sudah ditentukan yaitu (0◦, 45◦, 90◦, 135◦). Hasil pengujian menunjukan bahwa untuk masalah pengenalan wajah, metode LDP (Local Derivative Pattern) memiliki performansi yang lebih baik dari LBP (Local Binary Pattern) dengan menghasilkan nilai akurasi sebesar 92.9% pada LDP orde ke-3.

Dalam penelitian [3], peneliti melakukan klasifikasi tekstur citra atau gambar menggunakan metode high order Local Derivative Pattern. Tingkatan orde yang digunakan pada penelitian ini yaitu LDP (Local Derivative Pattern) dari orde ke-2 sampai orde ke 4. Hasil penelitian mendapatkan rata-rata nilai kebenaran pada klasifikasi teksktur Brodatz sebesar 91.67% (LDP Orde ke-2), 82.22% (LDP Orde ke-3), 83.33% (LDP Orde ke-4).

Dalam penelitian [8], peneliti mengusulkan menggunakan metode high order Local Derivative Pattern from Three Orthogonal Planes (LDP-TOP) untuk mendeteksi spoofing pada wajah manusia dari video. Metode ini mampu mengambil informasi dari sebuah video masukan hingga ke beberapa tingkat orde pada LDP (Local Derivative Pattern). Penambahan metode TOP (Three Orthogonal Planes) pada penelitian ini, ternyata mampu meningkatkan kehandalan dari sistem yang dibangun karena metode TOP (Three Orthogonal Planes) mampu melakukan pemotongan pada tiga bidang yang berbeda dari sebuah video yaitu bidang XY, XT dan YT. Algoritma klasifikasi yang digunakan yaitu SVM (Support Vector Machine). Hasil penelitian mendapatkan rata-rata nilai HTER (Half Total Error Rate) (%) pada intra-dataset sebesar 6.035, rata-rata nilai EER (Equal Error Rate) (%) sebesar 6.3575 dan rata-rata nilai TPR (True Positive Rate) (%) 23.9875 pada cross-dataset.

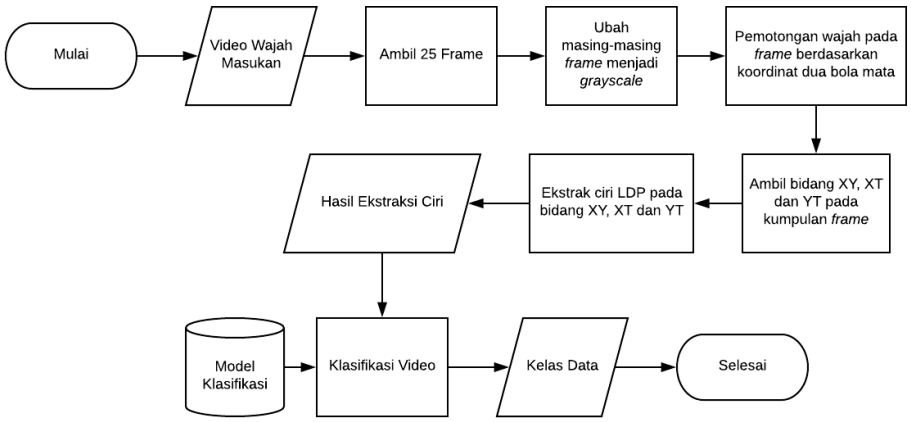
III. RANCANGAN SISTEM

Pada penelitian ini dibangun sebuah sistem yang dapat mendeteksi spoofing pada wajah manusia berbasis video. Sistem tersebut dapat membedakan wajah yang ada pada video masukkan merupakan wajah asli atau wajah palsu. Metode ekstraksi ciri yang digunakan pada pembangunan sistem ini adalah Local Derivative Pattern dari Three Orthogonal Planes (LDP-TOP). Pada sistem ini secara garis besar terbagi menjadi dua skema yaitu skema pelatihan dan skema pengujian. Skema pelatihan seperti yang terlihat pada Gambar 3 dan skema pengujian sistem seperti yang terlihat pada Gambar 4.



Gambar 3. Alur skema pelatihan

Skema pelatihan bertujuan untuk melatih sistem dalam mengenali video masukan apakah video masukan ter- sebut merupakan video wajah asli atau palsu dengan cara membuat model klasifikasi yang disimpan ke dalam database. Setelah itu, skema pengujian bertujuan untuk mendeteksi apakah video masukan merupakan video wajah asli atau palsu berdasarkan model klasifikasi yang dilakukan pada skema pelatihan.



Gambar 4. Alur skema pengujian

Berdasarkan gambar kedua skema di atas yaitu Gambar 3 dan Gambar 4, maka dapat diuraikan sebagai berikut:

1. Pre-processing

Proses ini dilakukan dengan merubah setiap frame pada video menjadi grayscale menggunakan rumus[7]:

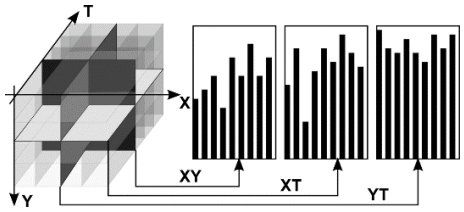
$$grayscale = 0.2989 * R + 0.5870 * G + 0.1140 * B \quad (1)$$

Kemudian dilakukan pemotongan wajah pada citra berdasarkan koordinat dua bola mata, dan ukuran citra diubah menjadi 64x64.

2. Ekstraksi Ciri

Proses ekstraksi ciri bertujuan untuk mengambil ciri pada citra atau gambar agar kemudian dapat diproses ke dalam proses klasifikasi. Dalam sistem ini citra atau gambar yang dimaksud adalah frame dari video. Metode ekstraksi ciri yang digunakan pada sistem ini adalah Local Derivative Pattern dari Three Orthogonal Planes (LDP- TOP). Karakteristik utama dari ekstraksi ciri LDP (Local Derivative Pattern) adalah mengambil fitur lokal dari empat arah yang sudah ditentukan antara lain yaitu: 0◦, 45◦, 90◦, 135◦. Lalu hasil dari keempat arah tersebut digabungkan transisinya sebagai string biner 32-bit. Orde ke-N dari LDP dikodekan dari orde ke-(N-1) local derivative. Sehingga dapat dikatakan bahwa Orde pertama dari LDP adalah LBP (Local Binary Pattern) non-directional [1].

LDP-TOP dibentuk dengan menghitung fitur LDP (Local Derivative Pattern) dari tiga bidang yaitu XY, XT dan YT dari suatu video (T adalah jumlah frame dari video masukan). Dengan keterangan, bidang XY mewakili informasi tampilan, sedangkan bidang XT memberikan kesan visual dari satu baris dalam perubahan waktu dan YT menggambarkan gerakan satu kolom di ruang temporal[11]. Kemudian histogram dari ketiga bidang tersebut digabungkan seperti pada Gambar 5. Histogram merupakan sebuah grafik yang menampilkan frekuensi kemunculan dari setiap nilai intensitas pixel dalam suatu citra[10].



Gambar 5. Ilustrasi LDP-TOP

3. Klasifikasi

Proses klasifikasi bertujuan untuk melakukan proses pelabelan pada data uji dengan melakukan proses pembelajaran terlebih dahulu. Proses pembelajaran dan pelabelan yang dilakukan pada sistem yang dibangun dilakukan menggunakan algoritma klasifikasi. Penelitian ini menggunakan algoritma klasifikasi SVM (*Support Vector Machine*) dan algoritma KNN (k-*Nearest Network*). Tujuan dari penggunaan dua algoritma klasifikasi yang berbeda adalah untuk mengetahui seberapa stabil performansi yang dihasilkan dari fitur LDP-TOP menggunakan dua algoritma klasifikasi yang berbeda karakteristiknya. Setiap algoritma klasifikasi memiliki parameter yang digunakan untuk mengklasifikasikan seperti parameter kernel (*Linear*, *Radial Basis Function* (RBF), *Polynomial*) pada SVM (*Support Vector Machine*) [2] dan parameter jumlah tetangga pada KNN (k-*Nearest Network*) [9]. Terdapat dua skenario yang digunakan pada penelitian ini yaitu skenario *intra-database* dan skenario *cross-database*. Skenario *intra-database* adalah skenario dengan wajah citra data uji merupakan wajah yang terdapat di dalam citra data latih. Skenario *cross-database* adalah skenario dengan wajah citra data uji merupakan wajah yang tidak terdapat di dalam citra data latih. Penggunaan skenario *cross-database* ini dilakukan untuk menjamin kemampuan generalisasi dari system. Kemampuan generalisasi adalah kemampuan dari sistem untuk mengenali pola baru yang belum pernah dipelajari sebelumnya, dalam kasus ini adalah wajah baru. Nilai performansi yang didapat dari skenario *intra-database* digunakan sebagai acuan pada skenario *cross-database*.

4. Evaluasi Performansi

Berdasarkan hasil prediksi kelas pada data uji, maka langkah selanjutnya yang dilakukan dalam penelitian ini adalah mengevaluasi sistem yang dibuat dengan cara melakukan perhitungan performansi sistem berdasarkan nilai akurasi yang didapatkan. Dalam menentukan nilai akurasi sistem, dibutuhkan adanya perhitungan nilai akurasi dengan membandingkan hasil klasifikasi dengan nilai sebenarnya kemudian dihitung nilai-nilai yang dibutuhkan untuk menghitung akurasi dengan menggunakan confussion matrix. Perhitungan performansi sistem yang digunakan pada penelitian ini antara lain yaitu F1-Score dan HTER (Half Total Error) yang dapat dihitung menggunakan rumus sebagai berikut [4] :

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F1\ score = \frac{2\ x\ Precision\ x\ Recall}{Precision+Recall} \quad (4)$$

$$FAR = \frac{FA}{NI} \quad (5)$$

$$FRR = \frac{FR}{NC} \quad (6)$$

$$HTER = \frac{FAR+FRR}{2} \quad (7)$$

Dengan keterangan, FAR adalah rata-rata false acceptance rate, FRR adalah rata-rata (false rejected rate), FA adalah total false acceptance (false positive), FR adalah total false rejection (false negative), NI adalah total gambar spoof (wajah palsu) dan NC adalah total gambar non-spoof (wajah asli). Untuk menentukan nilai TP (True Positive), TN (True Negative), FP (False Positive) dan FN (False Negative) dapat dilihat pada Tabel 1.

Tabel 1. Confussion Matrix [4].

		Aktual	
		Positif	Negatif
Prediksi	Positif	TP (True Positive)	FP (False Positive)
	Negatif	FN (False Negative)	TN (True Negative)

IV. PENGUJIAN SISTEM

Pada penelitian ini, terdapat 2 skenario pengujian yaitu *intra-database* dan *cross-database*. Tujuannya yaitu untuk mendapatkan parameter optimal dan menguji tingkat generalisasi sistem yang dibangun dengan metode LDP-TOP. Dataset yang digunakan merupakan video wajah manusia dengan kelas data *spoof* (wajah palsu) atau *non-spoof* (wajah asli) yang masing-masing memiliki karakteristik berbeda-beda. Terdapat 4 sumber dataset yang digunakan yaitu:

a. Idiap REPLAY-ATTACK Database (https://www.idiap.ch/dataset/replayattack)
b. CASIA Face-Anti Spoofing Database (https://pythonhosted.org/bob.db.casia_fasd/)
c. MSU Mobile Face Spoofing Database (https://pythonhosted.org/bob.db.msu_mfsd_mod/)
d. NUAA Imposter Database (http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html).

Namun, dataset yang berasal dari NUAA Imposter Database merupakan dataset dalam bentuk citra yang berurutan, sehingga diseleksi untuk didapatkan 25 foto dalam setiap urutan foto sesuai dengan pengambilan jumlah frame pada setiap video. Pengambilan 25 frame tersebut menyesuaikan dengan frame rate dari dataset lainnya yakni sebesar 25 Hz atau 25 frame per detik. Dari seleksi foto-foto tersebut kemudian digabung menjadi sebuah video.

Dari pengujian yang telah dilakukan pada skenario intra-database dan skenario cross-database didapatkan hasil sebagai berikut:

a. Hasil Pengujian Intra-database

Pada pengujian ini, dilakukan pembandingan performansi sistem dengan masing-masing parameter yang ada pada metode ekstraksi ciri LDP. Selain itu, digunakan dua algoritma klasifikasi yang berbeda yaitu KNN dengan parameter k = 7,9 dan 11 dan SVM dengan kernel Linear, Radial Basis Function (RBF) dan Polynomial. Jumlah ketetanggaan yang digunakan pada algoritma klasifikasi KNN adalah maksimal 11 karena terdapat dataset yang hanya berjumlah minimal 30 video. Selain itu, pada pengujian intra-database ini dilakukan perhitungan performansi dengan menggunakan 1 ting- katan orde yaitu orde 1 sampai 4, 2 tingkatan Orde pada LDP (Orde 1 + 2, Orde 1 + 3, dan Orde 1 + 4), 3 tingkatan Orde pada LDP (Orde 1 + 2 + 3, dan Orde 1 + 2 + 4) dan 4 tingkatan Orde pada LDP (Orde 1 + 2 + 3 + 4). Besaran radius yang digunakan adalah 1 sampai 5. Dengan keterangan bahwa LDP Orde 1 adalah LBP non-directional. Penggabungan beberapa tingkat orde ini bertujuan untuk mendapatkan informasi yang lebih detail dari frame yang ada pada video.

Tabel 2. Rata-rata F1-score dan HTER 1 Orde menggunakan Classifer SVM

Kernel	Orde	Radius 1		Radius 2		Radius 3		Radius 4		Radius 5	
		F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER
Linear	1	**95.25**	10.51	93.57	11.67	92.65	11.74	93.41	10.95	92.53	11.30
	2	95.12	10.99	92.61	11.29	95.94	9.97	95.25	11.06	**97.95**	10.68
	3	**95.80**	9.52	95.46	10.51	95.52	10.46	95.59	10.72	93.23	11.12
	4	95.18	10.27	**95.49**	9.97	94.92	11.18	94.68	10.84	94.73	9.75
RBF	1	**96.34**	14.22	94.50	15.41	93.99	15.26	93.77	15.33	93.48	15.09
	2	94.90	15.14	95.67	15.11	**95.80**	14.71	95.22	14.59	94.39	15.38
	3	95.01	14.70	95.24	14.95	**95.48**	17.32	94.78	15.34	93.82	15.49
	4	94.63	15.12	94.62	15.14	**94.72**	14.88	94.33	15.49	93.55	15.56
Polynomial	1	**96.74**	8.42	95.52	10.60	95.02	10.79	95.15	10.72	94.34	11.24
	2	96.86	9.59	**97.18**	9.61	97.08	8.90	96.97	9.38	96.63	9.69
	3	96.50	8.15	96.56	8.14	**96.90**	7.23	96.29	9.93	95.97	9.70

Dilakukan observasi pada masing-masing tingkatan orde dengan radius 1 sampai 5. Hasil performansi sistem yang didapat dan terlihat pada Tabel 2 menunjukkan bahwa performansi terbaik terletak pada LDP Orde ke-2 dengan Radius 5 yang menghasilkan nilai rata-rata F1-Score sebesar 97.95% dan rata-rata HTER sebesar 10.68% pada kernel Linear, sedangkan pada kernel Polynomial nilai rata-rata HTER yang diperoleh adalah sebesar 7.23%. Artinya, kernel Polynomial lebih mampu mentranformasikan data menjadi lebih kompleks dan lebih cocok untuk algoritma klasifikasi SVM yang digunakan, sehingga yang digunakan pada observasi selanjutnya adalah kernel Polynomial.

Tabel 3. Rata-rata F1-score dan HTER Penggabungan 2 Orde menggunakan Classifer SVM

Kernel	Orde	Radius 1		Radius 2		Radius 3		Radius 4		Radius 5	
		F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER
Linear	1 + 2	**96.17**	10.16	95.87	9.67	95.26	10.44	95.49	10.51	95.84	10.11
	1 + 3	**96.81**	9.20	96.65	8.61	94.53	10.41	96.62	8.19	95.78	8.91
	1 + 4	**96.73**	8.05	96.13	9.92	95.67	10.04	95.32	8.95	96.18	7.75
RBF	1 + 2	95.33	15.01	95.82	14.88	**96.08**	14.64	95.65	14.54	94.83	15.18
	1 + 3	95.15	14.81	95.24	14.83	**95.88**	13.89	95.38	15.02	94.29	15.33
	1 + 4	95.25	14.89	95.11	15.11	**95.34**	14.58	94.97	15.55	94.22	11.82
Polynomial	1 + 2	97.12	8.81	97.38	9.47	**97.47**	8.50	97.13	9.17	97.22	9.45
	1 + 3	96.74	7.76	96.95	7.48	97.37	6.09	**97.44**	8.38	96.97	8.45
	1 + 4	96.95	7.45	96.96	8.04	**97.35**	7.76	96.70	7.99	96.59	8.38

Dilakukan observasi dengan cara menggabungkan dua tingkatan orde dengan masing-masing radius 1 sampai 5. Dari hasil yang dapat dilihat pada Tabel 3, dengan menggabungkan 2 tingkatan Orde LDP yaitu Orde 1 + 2, Orde 1 + 3, Orde 1 + 4 dengan keterangan Orde 1 merupakan LBP non-directional, menunjukkan bahwa performansi terbaik terletak pada LBP non-directional (LDP Orde 1) + LDP Orde 3 Radius 4 dengan rata-rata F1-Score 97.44% dan rata-rata HTER 8.38% pada kernel Polynomial. Artinya, nilai rata-rata F1-Score pada saat menggabungkan 2 tingkatan orde pada LDP lebih besar daripada menggunakan 1 tingkatan orde (97.44% lebih besar dari 96.90%).

Tabel 4. Rata-rata F1-score dan HTER Penggabungan 3 Orde menggunakan Classifer SVM

Kernel	Orde	Radius 1		Radius 2		Radius 3		Radius 4		Radius 5	
		F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER
Linear	1 + 2 + 3	94.07	13.98	91.36	12.47	94.66	10.98	94.10	10.38	**95.49**	9.20
	1 + 2 + 4	96.16	10.02	**96.45**	9.97	92.80	12.87	94.51	9.97	95.65	13.18
RBF	1 + 2 + 3	95.24	14.83	95.84	14.75	**96.05**	14.72	96.04	14.61	95.09	14.95
	1 + 2 + 4	95.92	39.91	95.89	14.75	**96.19**	14.10	95.40	14.85	95.31	14.94
Polynomial	1 + 2 + 3	96.98	8.18	97.32	7.91	97.60	6.33	**97.77**	8.47	97.57	8.34
	1 + 2 + 4	97.00	8.15	97.56	8.69	**97.62**	7.52	97.26	8.98	97.51	8.36

Dengan menggabungkan 3 tingkatan orde pada LDP yaitu LBP non-directional (LDP Orde 1) + LDP Orde 2 + LDP Orde 3, dan LBP non-directional (LDP Orde 1) + LDP Orde 2 + LDP Orde 4, hasil performansi sistem pada Tabel 4 menunjukkan bahwa performansi terbaik terletak pada LBP non-directional (LDP Orde 1) + LDP Orde 2 + LDP Orde 3 Radius 4 dengan nilai rata-rata F1-Score 97.77% dan rata-rata HTER 8.47% pada kernel

Polynomial. Artinya, nilai rata-rata F1-Score pada saat menggabungkan 2 tingkatan orde pada LDP lebih kecil daripada menggabungkan 3 orde (97.44% lebih kecil dari 97.77%).

Tabel 5. Rata-rata F1-score dan HTER Penggabungan 4 Orde menggunakan Classifer SVM

Kernel	Radius 1		Radius 2		Radius 3		Radius 4		Radius 5	
	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER
Linear	92.18	15.71	94.14	10.79	93.73	14.15	**94.91**	9.96	94.20	14.74
RBF	95.39	18.55	95.56	14.85	**95.83**	14.28	95.51	14.87	94.83	14.97
Polynomial	97.10	7.69	97.37	7.67	**97.69**	7.04	97.35	8.73	97.38	8.10

Dengan menggabungkan 4 tingkatan LDP yaitu dari LDP Orde 1 sampai Orde 4 hasil performansi sistem pada Tabel 5 menunjukkan bahwa performansi terbaik terletak pada LDP Orde 1 (LBP non-directional) + Orde 2 + Orde 3 + Orde 4 dengan Radius 1 yaitu 97.69% untuk nilai rata-rata F1-Score dan 7.04% untuk rata-rata HTER pada kernel Polynomial. Artinya, nilai rata-rata F1-Score pada saat menggabungkan 3 tingkatan orde pada LDP lebih besar daripada menggabungkan 4 orde (97.77% lebih besar dari 97.69%).

Berdasarkan percobaan yang telah dilakukan dan tercantum pada Tabel 2, 3, 4 dan 5. Performansi terbaik adalah ketika menggunakan LDP Orde 1 (LBP non-directional) + Orde 2 + Orde 3 dengan Radius 4 dan menggunakan algoritma klasifikasi SVM. Sehingga pada pengujian yang menggunakan algoritma klasifikasi KNN digunakan parameter tersebut.

Tabel 6. Rata-rata F1-score dan HTER Penggabungan 4 Orde menggunakan Classifer KNN

K	Radius 1		Radius 2		Radius 3		Radius 4		Radius 5	
	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER	F1 Score	HTER
k = 7	93.01	20.01	93.03	24.71	**93.03**	21.11	92.60	21.42	91.91	21.65
k = 9	**93.56**	21.62	93.03	19.60	92.49	20.65	92.45	21.65	92.07	20.83
k = 11	**93.59**	20.82	92.66	20.59	92.46	18.73	92.15	20.45	91.93	20.65

Tabel 6 menunjukkan performansi terbaik terletak pada LDP Orde 1 + 2 + 3 dengan Radius 2 dan K = 11 dengan rata-rata F1-Score 93.59% dan rata-rata HTER 20.82%. Dari hasil yang didapat, hasil F1-Score pada saat menggunakan algoritma klasifikasi SVM dan KNN keduanya memperoleh nilai diatas 90%. Artinya, ekstraksi ciri LDP-TOP bagus digunakan pada pengujian intra-database. Namun, jika F1-Score SVM dan KNN dibandingkan maka hasil yang lebih baik adalah ketika menggunakan algoritma klasifikasi SVM. Sehingga yang digunakan pada skenario kedua (cross-database) adalah parameter yang digunakan pada saat menggunakan algoritma klasifikasi SVM.

b. Hasil Pengujian *Cross-database*

Pada skenario *cross-database* ini, dilakukan pengujian untuk mengetahui kemampuan generalisasi dari deteksi *spoofing* menggunakan algoritma LDP-TOP. Berikut hasil yang diperoleh:

Tabel 7. Rata-rata F1-score dan HTER Penggabungan 3 Orde menggunakan Classifer SVM

Dilatih pada	Diuji pada	F1 Score	HTER	Jml Data	Rata-rata F1Score	Rata-rata HTER
Idiap	Casia	77.34	27.97	360.00	**74.77**	29.05
	MSU	64.86	34.17	100.00		
	NUAA	76.92	25.00	30.00		
Casia	Idiap	69.93	27.20	279.00	68.00	28.97
	MSU	66.67	33.23	100.00		

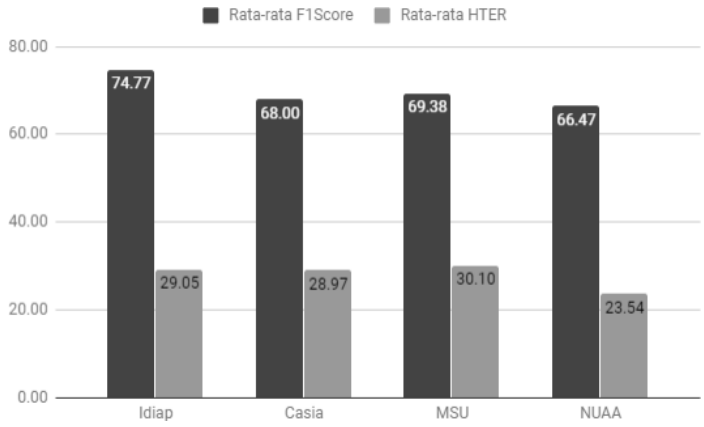
	NUAA	54.55	31.25	30.00		
MSU	Idiap	86.59	25.18	279.00	69.38	30.10
	Casia	55.42	34.34	360.00		
	NUAA	76.92	25.00	30.00		
NUAA	Idiap	45.00	35.48	279.00	66.47	23.54
	Casia	85.71	12.50	360.00		
	MSU	57.14	30.00	100.00		

Tabel 7 menunjukkan bahwa dengan menggunakan usulan penggabungan beberapa orde pada metode LDP, performansi terbaik terletak pada saat menggunakan dataset Idiap dengan rata-rata F1-Score 74.77% dan rata-rata HTER 29.05%.

c. Analisis Hasil Pengujian

Pengujian *intra-database* bertujuan untuk mencari parameter terbaik pada metode yang digunakan, kemudian menggunaan parameter tersebut untuk pengujian *cross-database*. Setelah dianalisis, hasil terbaik ketika menggunakan algoritma klasifikasi SVM pada kernel polynomial dengan menggabungkan 3 tingkatan orde LDP yaitu orde 1 (LBP non- directional), 2 dan 3 dengan radius 4. Karena semakin tinggi orde yang diambil maka semakin detail informasi yang ditangkap, dan ketika menggunakan radius yang lebih tinggi maka lebih banyak informasi yang diambil. Sehingga, ketika menggabungkan beberapa orde, informasi yang didapat akan semakin detail.

Pengujian *cross-database* bertujuan untuk mengetahui kemampuan generalisasi dari fitur LDP pada deteksi *spoofing*. Hasil pengujian *cross-database* dapat dilihat pada Gambar 6 berikut.



Gambar 6. Grafik performansi cross-database

Dari penelitian yang dilakukan, mengacu pada F1-Score, performansi terbaik dengan nilai rata-rata F1-Score sebesar 74.77% yang dilatih menggunakan dataset Idiap seperti yang terlihat pada grafik 6. Berdasarkan hasil yang didapatkan, kemampuan generalisasi pada sistem ini di bawah 90% dan masih kurang jika dibandingkan dengan penelitian sebelumnya menggunakan analisis distorsi citra yang mencapai F1-Score di atas 90%[12]. Kemampuan generalisasi yang dimaksud adalah ketika data latih dan data uji yang digunakan adalah berbeda, maka sistem akan tetap mengenali bahwa data masukan adalah wajah asli atau palsu. Pada pengujian ini, setiap dataset dibandingkan dengan dataset lain yang memiliki karakteristik berbeda-beda baik karena kondisi resolusi kamera, faktor cahaya, dan lain-lain.

V. KESIMPULAN

Pada penelitian ini telah dibangun sebuah sistem untuk deteksi *spoofing* pada wajah manusia berbasis video menggunakan metode *Local Derivative Pattern-Three Orthogonal Planes* (LDP-TOP). Pada penelitian ini

digunakan dua metode klasifikasi yang memiliki karakteristik berbeda, yaitu SVM dan KNN, untuk mengukur kestabilan dari fitur LDP yang dihasilkan. Sistem yang dibangun diuji menggunakan skenario *intra-database* dan *cross-database*. Dari hasil pengujian pada skenario *intra-database* didapatkan performansi terbaik yaitu rata-rata F1-Score 97.77% dan rata-rata HTER 8.47% dengan menggabungkan 3 orde pada LDP yaitu Orde 1 sampai Orde 3 radius 4, sedangkan pada skenario *cross-database* rata-rata F1-Score 74.77% dan rata-rata HTER 29.05%. Hal ini menunjukkan perlu adanya pengembangan pada metode ekstraksi ciri yang digunakan. Salah satu alternatif yang dapat dilakukan untuk pengembangan metode ini adalah dengan menggunakan skema piramid atau skema multi resolusi untuk ukuran dari kernel LDP yang digunakan.

Daftar Pustaka

[1] S. Z. J. L. Baochang Zhang, Yongsheng Gao. Local derivative pattern versus local binary pattern: Face recognition with high-order local pattern decriptor. 2010.
[2] D. S. Chouhan. Svm kernel functions for classification. 2013.
[3] B. M. D. B. E. R. Dr U S B Raju, A Sridhar Kumar. Texture classification with high order local pattern descriptor: Local derivative pattern. 2010.
[4] GeeksforGeeks. Confusion Matrix in Machine Learning. https://www.geeksforgeeks.org/confusion-matrix-machine-learning/. [Online; accessed 14-January-2019].
[5] A. Jain, Anil K.; Ross. Handbook of Biometrics. Springer, 2008.
[6] M. P. Jukka Maatta, Abdenour Hadid. Face spoofing detection from single images using micro-texture analysis. 2011.
[7] MathWorks. rgb2gray. https://www.mathworks.com/help/matlab/ref/rgb2gray.html, 2018. [Online; accessed 14-January-2019].
[8] G. B. F. G. D. N. Quoc-Tin Phan, Duc-Tien Dang-Nguyen. Face spoofing detection using ldp-top. 2016.
[9] M. Z.-X. Z. R. W. Shichao Zhang, Xuelong Li. Efficient knn classification with different numbers of nearest neighbors. 2018.
[10] E. S. V. N. O. D. W. Sutoyo, T.; Mulyanto. Teori Pengolahan Citra Digital. Penerbit Andi, 2009.
[11] G. Z. Xiaopeng Hong, Yingyue Xu. Lbp-top: a tensor unfolding revisit. 2017.
[12] A. H. Zinelabidine Boulkenafet, Jukka Komulainen. Face spoofing detection using colour texture analysis. 2016.