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

IND. JOURNAL ON COMPUTING
VOL. 3, ISSUE. 1, MARCH 2018. PP. 55-64
DOI:10.21108/INDOJC.2018.31.213

Deteksi Serangan *Spoofing* Pada Citra Wajah menggunakan Ekstraksi Ciri *Local Derivative Pattern*

Ni Gusti Ayu Mirah Eka Darmayanti [#1], Kurniawan Nur Ramadhani [#2], Anditya Arifianto [#3]

[#] Laboratorium Multimedia, Fakultas Informatika, Universitas Telkom
Jalan Telekomunikasi No.01, Terusan Buah Batu, Bandung 40257

[1] mirahekad@student.telkomuniversity.ac.id
[2] kurniawannr@telkomuniversity.ac.id
[3] anditya@telkomuniversity.ac.id

Abstract

This research proposed a facial image detection system using Local Derivative Pattern (LDP) feature extraction method. We used k-Nearest Neighbour (k-NN) and Support Vector Machine (SVM) as the classification method. We used NUAA Imposter and Photograph Database as the dataset. The optimal parameters for feature extraction using LDP are 2nd order LDP with radius value 5 which is non-uniform overlapping using SVM classification algorithm with Radial Basis Function kernel. The best performance was obtained using F1-Score value of 99.8%. The uniform pattern in LDP speeded up computing time by an average of 2.09 seconds, while the non-uniform pattern computing time is 5.49 seconds.

Keywords: *Face*, *Spoofing-Attack*, *Local Derivative Pattern*, *k-Nearest Neighbors*, *Support Vector Machine*

Abstrak

Pada penelitian ini, diusulkan sistem pendeteksi serangan spoofing pada citra wajah manusia menggunakan metode ekstraksi ciri Local Derivative Pattern (LDP). Metode klasifikasi yang digunakan adalah k-Nearest Neighbour (k-NN) dan Support Vector Machine (SVM). Penelitian ini menggunakan NUAA Imposter and Photograph Database sebagai datasetnya. Parameter optimal untuk ekstraksi ciri menggunakan LDP, adalah sebagai berikut: LDP orde ke-2 dengan radius bernilai 5 yang bersifat overlapping non-uniform menggunakan algoritma klasifikasi SVM dengan kernel Radial Basis Function. Performansi terbaik didapatkan menggunakan F1-Score sebesar 99.8%. Pola uniform pada LDP mempercepat waktu komputasi dengan rata-rata 2.09 detik, sedangkan waktu komputasi pola non-uniform yaitu 5.49 detik.

Kata Kunci: Wajah, *Spoofing-Attack*, *Local Derivative Pattern*, *k-Nearest Neighbors*, *Support Vector Machine*

I. PENDAHULUAN

Sistem biometrik khususnya pengenalan wajah banyak dikembangkan untuk berbagai kebutuhan, seperti: kontrol akses, penegakan hukum, multimedia serta interaksi antara manusia dan komputer [1]. Saat ini sistem pengenalan wajah juga banyak dimanfaatkan untuk sistem keamanan karena kemudahan dalam pengembangannya. Namun disamping itu, sistem pengenalan wajah rentan terhadap serangan pemalsuan yang biasa disebut serangan *spoofing*. Pada serangan ini, pelaku akan memalsukan data wajah korbannya sehingga mendapatkan akses ilegal serta keuntungan untuk dirinya sendiri dan pihak terkait [2]. Serangan *spoofing* ini mudah dan tidak memerlukan banyak biaya, biasanya dilakukan dengan menampilkan gambar cetakan wajah, video rekaman wajah atau menggunakan model 3D dari wajah korban sebagai bentuk pemalsuannya [3].

Penelitian yang telah dilakukan untuk pendeteksian *spoofing* pada citra wajah ini adalah mengidentifikasi tanda-tanda fisiologis wajah(kedipan mata [4], gerakan bibir [5] dan rotasi kepala [6]). Selain itu, ada pula yang mengkombinasikan wajah dengan modalitas sistem biometrik lainnya. Namun, metode tersebut membutuhkan *user cooperation* sehingga waktu komputasinya lebih lama dan membutuhkan biaya yang cukup besar [7].

RECEIVED ON FEB 2018. ACCEPTED ON MARCH 2018

Maka diperlukan sistem yang lebih handal tanpa memerlukan *user cooperation* sehingga waktu komputasinya lebih cepat dan tidak memerlukan biaya untuk peralatan lainnya. Pada penelitian ini, penulis mengusulkan metode pendeteksi serangan *spoofing* pada citra wajah menggunakan analisis tekstur. Ini didasari dari perbedaan antara wajah asli manusia dan gambar cetakan wajah lebih jelas diidentifikasi dengan metode analisis tekstur ini [7]. Metode analisis tekstur yang pernah digunakan untuk menangani masalah serangan *spoofing* ini adalah analisis *micro texture* menggunakan operator LBP (*Local Binary Pattern*) dengan akurasinya sebesar 98.0% [2]. Untuk itu, pada penelitian ini penulis mengusulkan operator analisis tekstur lainnya yaitu LDP (*Local Derivative Pattern*), yang mana merupakan perluasan dari metode LBP yang mendiskriminasikan ciri pada orde pertama untuk semua arah. Sedangkan, operator LDP ini dapat mengambil ciri dari sebuah citra hingga beberapa tingkat orde pada arah tertentu, sehingga informasi yang didapat lebih detail [8]. Selain itu, metode ini juga dapat menangani masalah terhadap kesensitifan *noise* yang membuat sistem menjadi lebih stabil dan handal.

Pada penelitian ini, metode LDP digunakan sebagai metode ekstraksi ciri citra. Penelitian ini melakukan identifikasi terhadap parameter optimal untuk LDP. Selain itu, untuk proses klasifikasi digunakan metode *k-Nearest Neighbors* dan *Support Vector Machine* untuk mengetahui performansi sistem yang dibangun. Pola *uniform* dan *non-uniform* pada LDP diteliti disini untuk mengetahui pengaruhnya terhadap waktu komputasi sistem. Pada bagian selanjutnya, dijelaskan dasar teori yang berkaitan dengan penelitian ini, penjelasan metode yang digunakan, hasil dan analisis dari penelitian serta kesimpulan yang didapat dari penelitian yang dilakukan.

II. Dasar Teori

A. *Local Derivative Pattern*

LDP (*Local Derivative Pattern*) adalah deskriptor pola lokal dengan orde tinggi yang merupakan kerangka umum untuk mengkodekan fitur pola direktif dari berbagai derivatif lokal [9]. Karakteristik utama dari metode LDP ini adalah mengambil fitur lokal dari empat arah, yaitu: 0°, 45°, 90°, 135° lalu menggabungkan hasil transisinya sebagai string biner 32-bit. Orde ke-N LDP dikodekan dari orde ke-(N-1) lokal derivatifnya. Dapat dikatakan bahwa, LBP (*Local Binary Pattern*) adalah orde pertama pola lokal derivatif dari LDP di semua arah. Jika dibandingkan dengan LBP, LDP memiliki performansi yang lebih baik karena dapat mengambil informasi lebih detail [1].

1. Orde Ke-2 *Local Derivative Pattern*

Seperti yang sudah dibahas sebelumnya, ketika ingin menghitung orde ke-N dari LDP, harus dihitung turunan ke-(N-1) lokal derivatifnya terlebih dahulu. Maka, jika ingin menghitung orde ke-2 maka harus dihitung dulu turunan pertama lokal derivatifnya. Diberikan citra I(Z), perhitungan turunan pertamanya dilakukan pada arah 0°, 45°, 90°, 135° yang dinotasikan sebagai $I'_\alpha(Z)$ dimana $\alpha = 0°, 45°, 90°, 135°$. Berikut gambaran dari ketetanggaan I(Z), Z_0 menjadi pusat dan dikelilingi oleh Z_i, i = 1, ..., 8. Perhitungan matriks ketetanggaan ini dilakukan pada citra keabuan, dimana besarnya matriks ketetanggaannya diukur berdasarkan R (radius) [10]. Pada gambar 1, ukuran matriks ketetanggaannya adalah 3x3 dimana R=1.

Z_1	Z_2	Z_3
Z_8	Z_0	Z_4
Z_7	Z_6	Z_5

Gambar 1 Delapan Tetangga Sekitar Z_0

Empat turunan pertama lokal derivatif dari $Z = Z_0$ dituliskan, sebagai berikut.

$$I'_{0^\circ}(Z_0) = I(Z_0) - I(Z_4) \quad (1)$$

$$I'_{45^\circ}(Z_0) = I(Z_0) - I(Z_3) \quad (2)$$

$$I'_{90^\circ}(Z_0) = I(Z_0) - I(Z_2) \quad (3)$$

$$I'_{135^\circ}(Z_0) = I(Z_0) - I(Z_1) \quad (4)$$

Orde ke-2 dari LDP dinotasikan sebagai $LDP^2_\alpha(Z_0)$ di $Z = Z_0$ didefinisikan sebagai berikut.

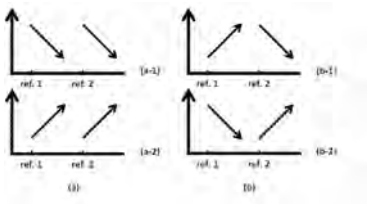
$$LDP^2_\alpha(Z_0) = \{f\left(I'_\alpha(Z_0), I'_\alpha(Z_1)\right), \dots, f\left(I'_\alpha(Z_0), I'_\alpha(Z_8)\right)\} \quad (5)$$

Dimana f(.,.) adalah fungsi biner yang menentukan tipe dari transisi pola lokalnya. Pengkodean pada *co-occurrence* dari dua arah derivatifnya untuk ketetanggan piksel yang berbeda, dapat ditulis seperti berikut.

$$f\left(I'_\alpha(Z_0), I'_\alpha(Z_i)\right) = \begin{cases} 0, & if\ I'_\alpha(Z_i).I'_\alpha(Z_0) > 0 \\ 1, & if\ I'_\alpha(Z_i).I'_\alpha(Z_0) \le 0 \end{cases} i = 1,2,\dots,8 \quad (6)$$

LDP orde ke-2 dinotasikan sebagai $LDP^2(Z)$ adalah urutan string biner 32-bit yang mana pengabungan dari 8-bit LDP dari empat arah. Perumusan $LDP^2(Z)$ sebagai berikut.

$$LDP^2(Z) = \{LDP^2_\alpha(Z) | \alpha = 0^\circ, 45^\circ, 90^\circ, 135^\circ\} \quad (7)$$



Gambar 2 Ilustrasi Fungsi Biner LDP [8]

Ilustrasi gambar 2 menunjukkan cara kerja dari fungsi biner LDP. Ketika nilai dari Z_0 dan Z_i monoton turun atau naik seperti (a-1) dan (a-2) maka fungsi binernya berlabel "0", sedangkan jika nilainya bergantian seperti (b-1) dan (b-2) maka fungsi binernya berlabel "1".

2. Orde Ke-N *Local Derivative Pattern*

Sama seperti orde sebelumnya, perhitungan orde ke-N harus menghitung turunan ke-(N-1) terlebih dahulu. Turunan ke-(N-1) ini dihitung dengan persamaan berikut.

$$I^{(N-1)}_{0^\circ}(Z_0) = I^{(N-2)}(Z_0) - I^{(N-2)}(Z_4) \quad (8)$$

$$I^{(N-1)}_{45^\circ}(Z_0) = I^{(N-2)}(Z_0) - I^{(N-2)}(Z_3) \quad (9)$$

$$I^{(N-1)}_{90^\circ}(Z_0) = I^{(N-2)}(Z_0) - I^{(N-2)}(Z_2) \quad (10)$$

$$I^{(N-1)}_{135^\circ}(Z_0) = I^{(N-2)}(Z_0) - I^{(N-2)}(Z_1) \quad (11)$$

LDP pada orde ke-N dituliskan seperti berikut

$$LDP^N_\alpha(Z_0) = \{f\left(I^{(N-1)}_\alpha(Z_0), I^{(N-1)}_\alpha(Z_1)\right), \dots, f\left(I^{(N-1)}_\alpha(Z_0), I^{(N-1)}_\alpha(Z_8)\right)\} \quad (12)$$

Dengan $\alpha = 0^\circ, 45^\circ, 90^\circ, 135^\circ$. Setelah dilakukan perhitungan fungsi biner pada setiap arahnya, maka dilakukan penggabungan menjadi string biner 32-bit, dengan rumus:

$$LDP^N(Z) = \{LDP^N_\alpha(Z) | \alpha = 0^\circ, 45^\circ, 90^\circ, 135^\circ\} \quad (13)$$

Fungsi pengkodean LDP dapat meringakan masalah terhadap sensifitas *noise* pada citra derivatif orde tinggi yang membuat LDP lebih kuat dan stabil dalam mengambil ciri pada wajah manusia. Namun, jika LDP sudah mencapai tingat tertentu maka terjadi titik kejenuhan yang membuat performansi LDP menurun.

3. *Uniform Local Derivative Pattern*

ULDP (*Uniform Local Derivative Pattern*) adalah perluasan dari metode ekstraksi ciri LDP. Perbedaan diantara keduanya adalah pola transisi binernya dimana ULDP menggunakan pola *uniform* [9]. Pola pada LDP terbagi menjadi dua kategori, yaitu *uniform* dan *non-uniform* berdasarkan jumlah transisi spasialnya.

Sebuah pola LDP dikatakan *uniform* jika transisi biner antara 0 dan 1 atau sebaliknya tidak lebih dari dua kali transisi sirkular, selain itu termasuk kedalam pola *non-uniform*. Contoh dari transisi biner yang termasuk pola *uniform* adalah "00000000" (0 transisi), "0110000" (2 transisi). Sedangkan, untuk pola *non-uniform* contohnya seperti: "01010000" (4 transisi), "1010010" (6 transisi). Untuk ketetanggaan yang berjumlah delapan buah, maka transisi biner pola *uniform* ini digambarkan pada gambar 3, dimana terdapat sembilan pola transisi. Untuk "00000000" dan "11111111" memiliki nol transisi. Sedangkan yang lainnya, memiliki tepat dua transisi sirkular sehingga setiap pola tersebut memiliki delapan jenis rotasi. Maka dari itu, jumlah total pola *uniform* adalah 7x8+2 = 58. Nilai bit "0" dan "1" direpresentasikan sebagai titik putih dan titik hitam.

Gambar 3 Pola *Uniform* untuk Jumlah Ketetanggan Delapan [9]

Perhitungan ULDP di $Z = Z_0$ pada arah α untuk delapan ketetanggaan, dapat dirumuskan sebagai berikut.

$$ULDP = \begin{cases} \left[\sum_{p-1}^{8} f\left(I'_\alpha(Z_0), I'_\alpha(Z_p)\right) 2^{p-1}\right] \\ -N\left[\sum_{p-1}^{8} f\left(I'_\alpha(Z_0), I'_\alpha(Z_p)\right) 2^{p-1}\right] \\ 58, otherwise \end{cases}, if\ g(LDP) \leq 2 \tag{14}$$

$$g(LDP) = \left\{ \left| f\left(I'_\alpha(Z_0), I'_\alpha(Z_8)\right) - f\left(I'_\alpha(Z_0), I'_\alpha(Z_1)\right) \right| + \sum_{p-1}^{7} \left| f\left(I'_\alpha(Z_0), I'_\alpha(Z_{p+1})\right) - f\left(I'_\alpha(Z_0), I'_\alpha(Z_p)\right) \right| \right\} \tag{15}$$

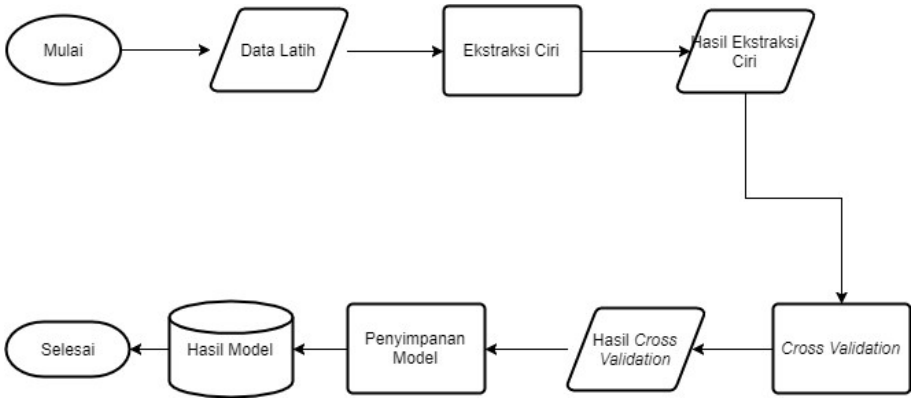
yang mana N(x) merupakan fungsi untuk menghitung jumlah pola *non-uniform* yang lebih kecil dari x dan g(LDP) digunakan untuk menghitung jumlah transisi spasial antara 0/1 dan sebaliknya yang terjadi pada pola LDP. Persamaan 2.9 menyatakan bahwa pola LDP pertama bergerak 1-bit, kemudian dikurangi dengan nilai biner asli dari pola biner LDP yang dihasilkan setelah pemindahan. Akhirnya, jumlah transisi spasial diperolah dengan menghitung jumlah nilai absolut dari selisihnya. Hasil dari proses ekstraksi ciri ini yang digunakan untuk proses klasifikasi dengan metode *k-Nearest Neighbors* dan *Support Vector Machine*.

III. Perancangan Sistem

A. *Pembangunan Model*

Pembangunan sistem pendeteksi *spoofing* pada wajah manusia berbasis gambar wajah yang dicetak adalah penelitian yang dilakukan untuk penelitian ini. Tujuan dari penelitian ini adalah mengenali masukan citra sebagai *spoof* dan *non-spoof*. Skema yang dijalankan sistem dibagi menjadi dua yaitu pembangunan model dan pengujian sistem.

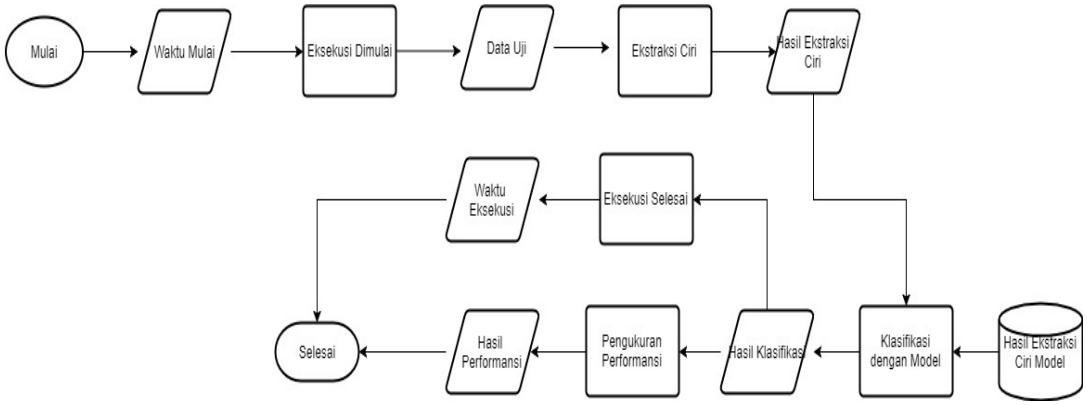
Pembangunan model dilakukan untuk mendaftarkan data ciri citra wajah (*spoof* dan *non-spoof*) ke dalam model *database*. Selain mendaftarkan ciri, pada tahap ini pula ada proses validasi sistem. Pada proses validasi ini juga menentukan model klasifikasi yang tepat antara metode *k-Nearest Neighbors* dan *Support Vector Machine*. Tujuan dilakukan validasi ini adalah untuk memastikan bahwa sistem dan model yang telah dibangun sudah memiliki performansi dan kehandalan yang tinggi untuk menangani masalah.



Gambar 4 *Flow Chart* Pembangunan Model

B. Pengujian Sistem

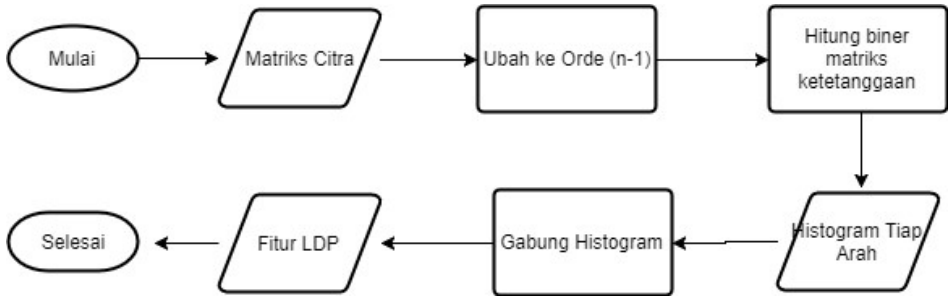
Setelah model dibuat, maka tahap pengujian dilakukan dengan mengimplementasikan model yang telah ada yang bertujuan untuk mengklasifikasikan masukan citra baru. Hasil klasifikasi ini kemudian menjadi prediksi dari citra baru tersebut adalah *spoof* atau *non-spoof*. Dataset sebenarnya telah memiliki label, oleh karena itu perhitungan performansi sistem dilakukan dengan membandingkan hasil prediksi sistem dengan label citra yang sebenarnya. Selain untuk mengidentifikasi performansi dan kehandalam sistem, proses pengujian ini juga digunakan untuk mengetahui pengaruh pola *uniform* pada *Local Derivative Pattern* terhadap waktu eksekusi sistem.



Gambar 5 *Flow Chart* Pengujian Sistem

C. Ekstraksi Ciri

Ekstraksi ciri dilakukan untuk mendapatkan informasi penting dari citra. Proses ini menggunakan metode LDP *Local Derivative Pattern* yang mengekstrak citra hingga beberapa orde dari arah-arah yang sudah ditentukan. Pada proses ini, diidentifikasi orde pada tingkat tertentu yang memiliki efektifitas paling tinggi untuk mengekstraksi ciri citra.



Gambar 6 *Flow Chart Local Derivative Pattern*

IV. Hasil Pengujian Dan Analisis

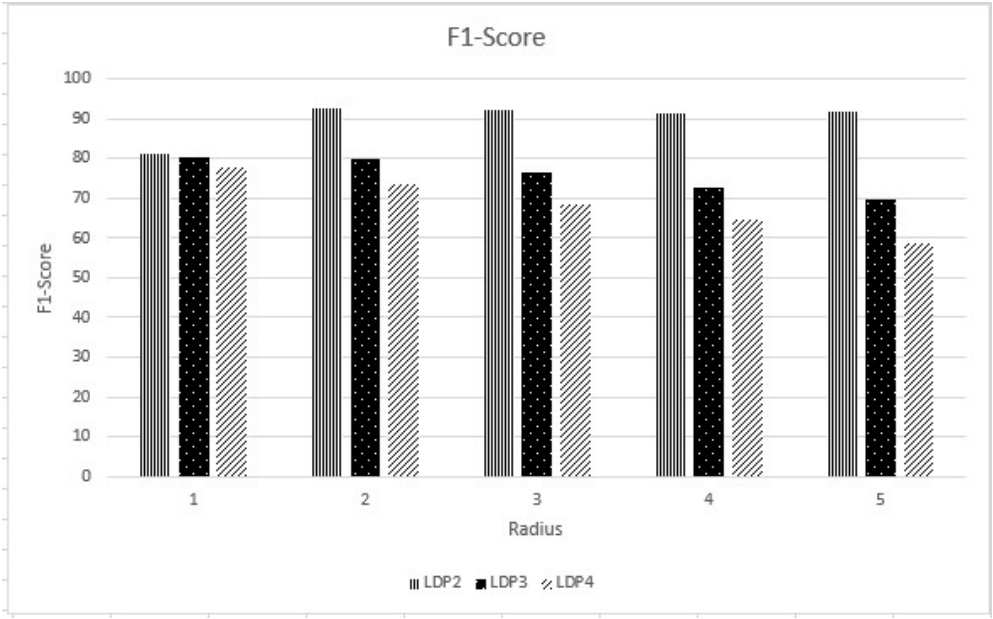
Pengujian ini menggunakan dataset *NUAA Imposter and Photograph Database* dimana dataset dibagi menjadi dua bagian yaitu data latih dan data uji. Tahap pengujian ini dilakukan dalam dua tahap, yaitu : tahap validasi yang dilakukan pada data latih saja dan tahap pengujian yang dilakukan pada seluruh dataset.

A. Tahap Validasi

Proses validasi ini dilakukan pada data latih saja yang bertujuan untuk menentukan model yang paling baik untuk sistem ini, baik kombinasi parameter pada ekstraksi cirinya dan parameter metode klasifikasi yang digunakan. Pada proses ini dilakukan dua skenario, sebagai berikut.

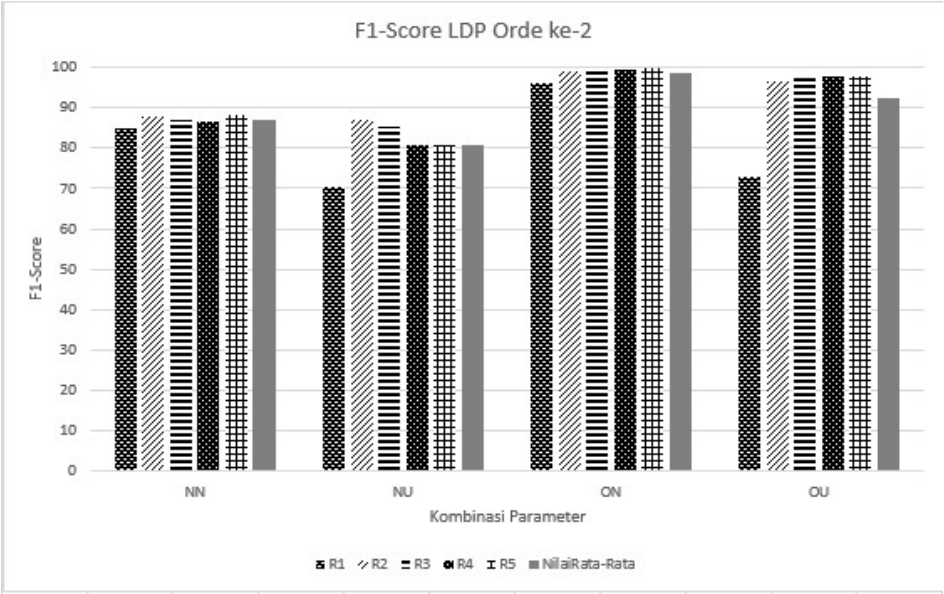
1. Skenario 1

Skenario 1 ini dilakukan untuk mengidentifikasi kombinasi parameter LDP yang tepat diterapkan pada sistem. Hasil dari pengujian validasi ini didapat dalam bentuk *F1-Score* yang menggambarkan performansi sistem. Metode klasifikasi yang digunakan pada skenario ini secara keseluruhan adalah metode *Support Vector Machine* dengan kernelnya yaitu *Linear*. Pada tahap pertama, diidentifikasi orde pada LDP pada semua kombinasi parameter. Kombinasi tersebut, antara lain: NN (*non-overlapping non-uniform*), NU (*non-overlapping uniform*), ON (*overlapping non-uniform*) dan OU (*overlapping uniform*). Hasilnya digambarkan dalam grafik berikut.



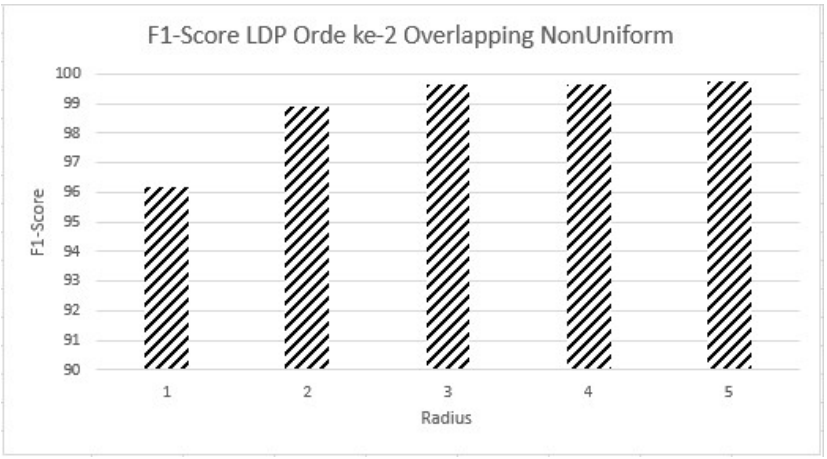
Gambar 7 *F1-Score* LDP pada Setiap Radius

Grafik gambar 7 menggambarkan hasil rata-rata *F1-Score* disemua kombinasi pada R = 1 .. 5. Pada grafik terlihat bahwa pada orde ke-2 pada R = 1 .. 5 memiliki nilai *F1-Score* tertinggi di setiap radiusnya yaitu 81.00%, 92.58%, 92.26%, 91.20% dan 91.64%. Hal ini disebabkan karena semakin tinggi ordenya, semakin detail informansi yang ditangkap. Walaupun LDP dapat menangani masalah kesensitifan *noise* pada orde yang lebih tinggi, namun hanya mampu menangani hingga orde ke-2 untuk kasus serangan *spoofing* ini. Sedangkan, pada orde ke-3 dan ke-4 informasi yang ditangkap terlalu detail sehingga performansi dan kehandalannya menjadi menurun. LDP orde ke-2 ini selanjutnya digunakan untuk menganalisis radius dan kombinasi parameter.



Gambar 8 *F1-Score* Setiap Radius pada Semua Kombinasi

Grafik gambar 8 adalah *F1-Score* pada LDP orde ke-2 di setiap radius (1..5) untuk semua kombinasi (NN, NU, ON dan OU). Pengambilan matriks secara *overlapping* pada kombinasi ON dan OU memiliki performansi yang lebih tinggi dibandingkan dengan pengambilan matriks secara *non-overlapping* pada kombinasi NN dan NU. Ini dikarenakan *overlapping* melakukan pengambilan informasi di setiap piksel citra sehingga ciri yang didapat lebih detail sedangkan *non-overlapping* tidak melakukan hal tersebut sehingga banyak ciri dari citra yang terlewat. Dari grafik gambar 8 dapat dilihat bahwa nilai rata-rata semua radius pada kombinasi ON dan OU memiliki F1-Score yang tinggi yaitu 98.83% dan 92.43%. Untuk pola *uniform* dan *non-uniform* pada pengambilan matriks *overlapping*, terlihat dari grafik bahwa pola *non-uniform* (ON) memiliki performansi dan kehandalan yang lebih baik dari pada pola *uniform* (OU), ini dikarenakan *uniform* mampu mereduksi dimensi namun membuat banyak ciri dari citra hilang.

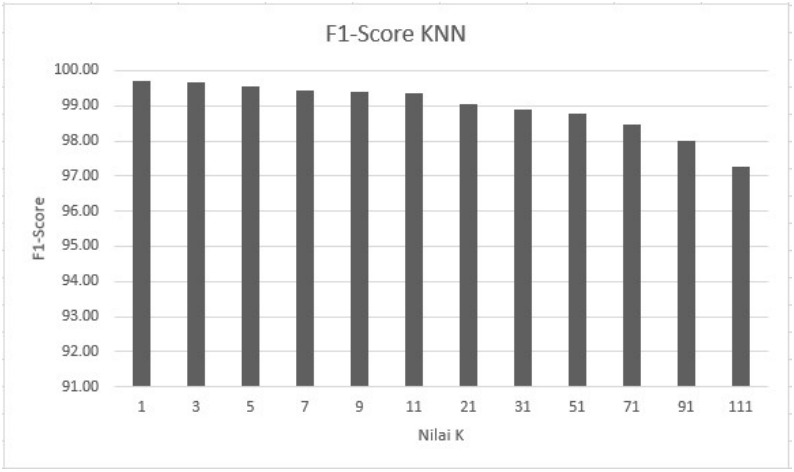


Gambar 9 *F1-Score* Pada LDP Orde Ke-2 Overlapping Non Uniform

Penentuan radius kemudian dilakukan pada LDP orde ke-2 dengan kombinasi ON (*overlapping non-uniform*). Dari grafik gambar 8 terlihat bahwa radius bernilai 5 memiliki performansi paling baik. Ini dapat dibuktikan dengan nilai *F1-Score*nya adalah 99.74%. Ini dikarenakan semakin besar radiusnya, maka semakin banyak pula informasi yang dapat diambil.

2. Skenario 2

Skenario 2 ini dilakukan untuk mengidentifikasi metode klasifikasi beserta parameternya yang paling tepat untuk menangani serangan *spoofing* pada citra wajah. Kombinasi parameter yang telah didapat pada pengujian skenario 1, digunakan pada skenario ini. Kombinasi fitur itu adalah LDP orde ke-2 dengan radiusnya bernilai 5 dan *overlapping non-uniform*. Metode klasifikasi yang diujikan adalah *k-Nearest Neighbors* dan *Support Vector Machine*. Pengujian terhadap k-NN dilakukan untuk mengetahui nilai K yang memiliki performansi paling baik.

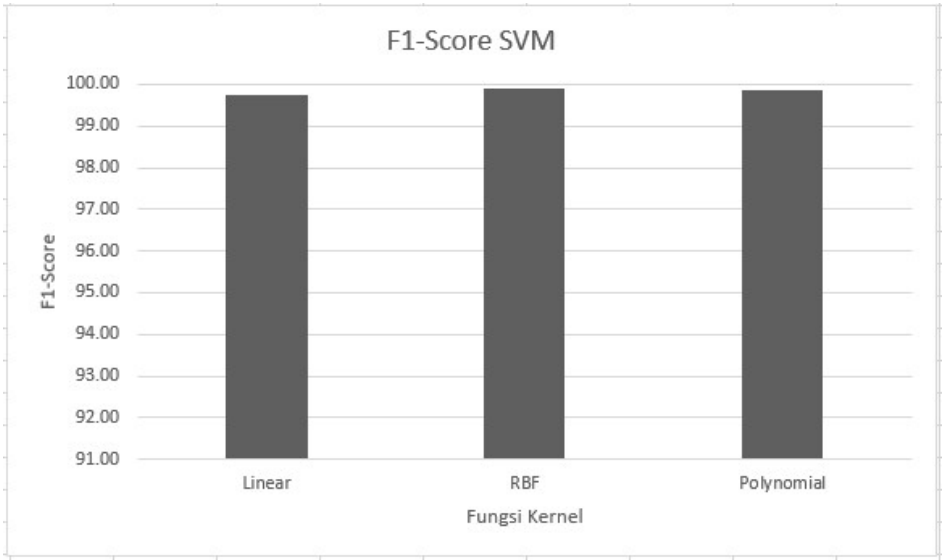


Gambar 10 *F1-Score* pada k-NN

Pada metode klasifikasi k-NN untuk kombinasi parameter yang telah didapat sebelumnya, K = 1 memiliki performansi yang paling baik. Ini dilihat dari grafik gambar 9 bahwa nilai *F1-Score* K = 1 yaitu 99.71% paling tinggi diantara nilai K yang lain. Ini dikarenakan, kemiripan antar datanya sangat tinggi, ketika K = 1 maka data yang diambil adalah data yang memiliki kemiripan paling besar. Semakin tinggi Knya, data

yang diambil semakin banyak namun hasil prediksinya semakin kecil kehandalannya karena terpengaruh data yang memiliki kemiripan juga namun bukan merupakan kelas sebenarnya dari data tersebut.

Sedangkan, untuk metode klasifikasi *Support Vector Machine*, yang menjadi pengujian adalah penggunaan fungsi kernelnya. Kernel yang diuji, antara lain: *Linear*, *Radial Basis Function* dan *Polynomial*.



Gambar 11 *F1-Score* pada SVM

Grafik gambar 10 menggambarkan performansi kombinasi parameter di setiap kernelnya. Terlihat bahwa kernel RBF memiliki performansi dan kehandalan palng tinggi, yaitu ditunjukkan dengan *F1-Score*nya sebesar 99.89%. Kernel RBF memiliki performansi yang paling tinggi, karena mampu mentransformasi data menjadi lebih kompleks dan lebih cocok untuk metode SVM yang digunakan. Sehingga SVM mampu mengklasifikasikan data lebih baik daripada penggunaan kernel lain untuk kasus *spoofing* ini.

Antara metode klasifikasi k-NN K = 1 dengan SVM kernel RBF, yang memiliki performansi yang lebih baik adalah metode SVM sebesar 99.89% nilai *F1-Score*nya. Sedangkan, metode k-NN *F1-Score*nya sebesar 99.71%. Walaupun perbedaannya tidak cukup jauh, namun SVM dengan kernel RBF dapat menangani masalah serangan *spoofing* lebih baik.

B. Tahap Pengujian

Tahap pengujian ini dilakukan untuk semua dataset *NUAA Photograph and Imposter Database*. Kombinasi parameter dan metode klasifikasi yang terbaik pada proses validasi sebelumnya, diterapkan pada proses ini. Parameter kombinasi, yaitu LDP orde ke-2 dengan radiusnya bernilai 5 serta *overlapping non-uniform* diterapkan pada seluruh dataset, baik itu data latih maupun data uji. Kemudian diklasifikasi dengan metode SVM kernel RBF menghasilkan performansi *F1-Score* sebesar 99.80% yang menunjukkan sistem telah handal untuk menangani masalah serangan *spoofing* pada citra wajah.

Selain pengujian terhadap performansi, dilakukan juga pengujian terhadap waktu eksekusi sistem yang dipengaruhi oleh pola *uniform* pada metode *Local Derivative Pattern*. Dari pengujian yang telah dilakukan didapat bahwa rata-rata waktu eksekusi pada pola *uniform* adalah 2.09 detik sedangkan pada pola *non-uniform* waktu eksekusinya adalah 5.49 detik. Ini menunjukkan walaupun pola *uniform* tidak memberi performansi yang tinggi tapi dapat mempersingkat waktu eksekusi karena reduksi dimensi yang dilakukannya.

V. Kesimpulan

Setelah proses implementasi sistem Deteksi Serangan *Spoofing* pada Citra Wajah dilakukan, dapat disimpulkan bahwa:

1. Penggunaan metode *Local Derivative Pattern* dalam menangani serangan *spoofing* pada citra wajah terpengaruh oleh beberapa parameter yang berdampak pada performansi serta kehandalan sistem. Setelah dilakukan proses validasi, didapat bahwa kombinasi parameter LDP yang memiliki kinerja paling baik adalah LDP orde ke-2, dengan nilai radiusnya adalah 5, pengambilan matriksnya secara *overlapping* serta pola binernya yaitu *non-uniform*. Ini dibuktikan dengan nilai *F1-Score* yang dihasilkan sebesar 99.74% untuk kombinasi parameter LDP menggunakan metode *Support Vector Machine* kernel *Linear* sebagai metode klasifikasinya.
2. Pada proses validasi didapat bahwa metode *k-Nearest Neighbors* memiliki performansi dan kehandalan terbaik pada nilai K = 1, dimana *F1-Score*nya sebesar 99.71%. Sedangkan, untuk metode *Support Vector Machine* memiliki kinerja terbaik saat menggunakan fungsi kernel *Radial Basis Function* dengan nilai *F1-Score*nya 99.89%. Kedua metode klasifikasi ini kemudian dibandingkan, dan akhirnya metode *Support Vector Machine* dengan fungsi kernel *Radial Basis Function* yang digunakan untuk tahap pengujian karena memiliki performansi dan kehandalan lebih tinggi.
3. Proses pengujian dilakukan untuk seluruh dataset *NUAA Imposter and Photograph Database* dengan mengimplementasikan model ekstraksi ciri serta model klasifikasi sehingga mendapatkan nilai *F1-Score* sebesar 99.80%.
4. Pola *uniform* pada metode *Local Derivative Pattern* dapat mengurangi waktu eksekusi sistem. Ini didapat dari rata-rata waktu eksekusi yang diperlukan untuk pola *uniform* adalah 2.09 detik sedangkan pada pola *non-uniform* waktu yang diperlukan adalah 5.49 detik.

Daftar Pustaka

[1] Q.-T. P. a. D.-T. D.-N. a. G. B. a. F. G. B. D. Natale, "Face Spoofing Detection Using LDP-TOP," *Image Processing (ICIP), 2016,* pp. 404-408, 2016.

[2] J. M. a. A. H. a. M. Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis," *Biometrics, International Joint Conference on,* vol. 00, pp. 1-7, 2011.

[3] H. L. a. S. W. a. A. C.Kot, "Face Spoofing Detection With Image Quality Regression," dalam *Image Processing Theory Tools and Applications (IPTA)*, IEEE, 2016.

[4] G. P. a. L. S. a. Z. Wu, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," 2007.

[5] K. K. a. H. F. a. M. I. F. a. J. Bigun, "Real-Time Face Detection and Motion Analysis With Application in "Liveness" Assessment," *IEEE Transactions on Information Forensics and Security - Part 2,* vol. 2, pp. 548-558, 2007.

[6] W. B. a. H. L. a. N. L. a. W. Jiang, "A Liveness Detection Method For Face Recognition Based on Optical Flow Field," *Image Analysis and Signal Processing,* pp. 233-236, 2009.

[7] Z. B. a. J. K. a. A. Hadid, "Face Spoofing Detection Using Color Texture Analysis," *IEEE Transactions on Information Forensics and Security,* vol. 11, pp. 1818-1830, 2016.

[8] B. Z. a. Y. G. a. S. M. a. S. Z. a. J. L. a. S. Member, "Local Derivative Pattern Versus Local Binary Pattern: Face Recognition with Higher-Order Local Pattern Descriptor," *IEEE Trans. Image Process,* pp. 533-544, 2010.

[9] H. R. a. J. S. a. Y. H. a. X. Y. a. Y. Liu, "Uniform Local Derivative Patterns and Their Application in Face Recognition," *Journal of Signal Processing Systems,* vol. 74, pp. 405-416, 2014.