Jurnal Elektronik Ilmu Komputer Udayana
Volume 13, No 1. August 2024

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Pengembangan Sistem Presensi Anti Spoofing dengan Metode Support Vector Machine

Marselinus Putu Harry Setyawan[a1], I Dewa Made Bayu Atmaja Darmawan[a2], I Gede Santi Astawa[a3], I Wayan Santiyasa[a4]

[a]Program Studi Informatika, Universitas Udayana
Badung, Bali, Indonesia
[1]marselinusphs@gmail.com
[2]dewabayu@unud.ac.id
[3]santi.astawa@unud.ac.id
[4]santiyasa@unud.ac.id

Abstrak

Penelitian ini bertujuan untuk mengembangkan sistem deteksi spoofing menggunakan metode Support Vector Machine (SVM) dengan ekstraksi fitur tekstur Local Binary Patterns (LBP) dan Gray-Level Co-occurrence Matrix (GLCM). Sistem ini ditujukan untuk mengatasi tantangan kehadiran mahasiswa dengan mengintegrasikan teknologi pengenalan wajah dalam manajemen presensi. Spoofing, yang merupakan usaha pemalsuan wajah, menjadi tantangan dalam sistem keamanan berbasis wajah. Oleh karena itu, sistem ini memfokuskan pada deteksi spoofing dengan membandingkan pola tekstur antara wajah asli dan palsu. Model mampu mengidentifikasi upaya pemalsuan wajah (spoofing) dengan tingkat akurasi sebesar 94% setelah melakukan tuning parameter C dan gamma. Selanjutnya, sistem presensi anti spoofing diuji melalui black box testing dan memberikan hasil yang sesuai dengan harapan. Sistem ini mampu memulai kelas, mencatat kehadiran mahasiswa, serta menghasilkan laporan kehadiran yang valid. Seluruh fungsi sistem telah diuji secara menyeluruh dan memperoleh tingkat akurasi 95% dalam pendeteksian spoofing. Dengan demikian, penelitian ini menghadirkan kontribusi penting dalam pengembangan sistem presensi yang lebih akurat dan aman melalui deteksi spoofing.

Kata kunci: *spoofing, attendance system, local binary patterns, gray level co-occurrence matrix, support vector machine, black box testing*

1. Pendahuluan

Untuk memverifikasi catatan kehadiran mahasiswa, kampus harus memiliki sistem yang tepat untuk menyetujui dan memelihara catatan kehadiran secara konsisten. Sistem pencatatan kehadiran mahasiswa umumnya terbagi menjadi Manual Attendance System (MAS) dan Automated Attendance System (AAS). Sistem manual melibatkan dosen memanggil mahasiswa satu per satu atau meminta tanda tangan mahasiswa, yang bisa menjadi sulit dan memakan waktu, terutama di kelas besar. Sebaliknya, sistem absensi otomatis menggunakan pengenalan wajah dapat mengurangi beban administrasi staf kampus [1].

Sistem pengenalan wajah memiliki kerentanan karena tidak membedakan antara gambar wajah nyata dan wajah palsu [2]. Tantangan utama adalah mendeteksi spoofing citra wajah, di mana seseorang mencoba mengakses sistem dengan memalsukan wajah korban untuk mendapatkan akses ilegal. Jenis spoofing yang paling sering digunakan yaitu spoofing cetak dan spoofing presentasi. Spoofing cetak adalah pelaku menggunakan foto korban dengan gambar dicetak, sedangkan spoofing presentasi adalah cara yang lebih canggih yang biasanya menggunakan foto wajah korban dari perangkat elektronik [3]. Deteksi spoofing dapat dilakukan dengan pendekatan fitur tekstur yang membandingkan pola tekstur antara wajah asli dan palsu, memanfaatkan perbedaan pantulan dan permukaan [4].

Penelitian deteksi spoofing wajah telah menggunakan analisis tekstur untuk meningkatkan keamanan sistem pengenalan wajah. Penelitian oleh Kusuma dan Kartika yang menggunakan LBP dan Adaptive

Histogram Equalization dengan KNN [4], serta oleh Alexander *et al* yang menggunakan ekstraksi fitur Local Binary Patterns dalam pengenalan wajah [5]. Penelitian tersebut menunjukkan bahwa kombinasi LBP dan GLCM memberikan akurasi yang lebih tinggi dibandingkan dengan penggunaan algoritma tunggal.

Penelitian ini bertujuan membangun sistem presensi yang dapat mengidentifikasi spoofing wajah menggunakan metode LBP dan GLCM untuk ekstraksi fitur tekstur dan SVM untuk klasifikasi. Metode HOG digunakan untuk deteksi wajah, yang efektif berdasarkan penelitian sebelumnya. Diharapkan sistem ini dapat membantu dalam proses otentikasi untuk mencegah spoofing, sehingga mengurangi akses ilegal.

2. Metode Penelitian

Penelitian ini dimulai dengan mengumpulkan data citra spoofing untuk digunakan dalam model dan melakukan preprocessing pada citra. Kemudian dilakukan analisis kebutuhan dan desain dari sistem yang dibuat berupa UML. Setelah itu membuat model anti-spoofing dan mengimplementasikan desain sistem yang sudah dibuat menjadi sebuah sistem presensi. Terakhir dilakukan pengujian terhadap sistem dan menganalisis keluaran yang dihasilkan dari sistem yang sudah dibuat.

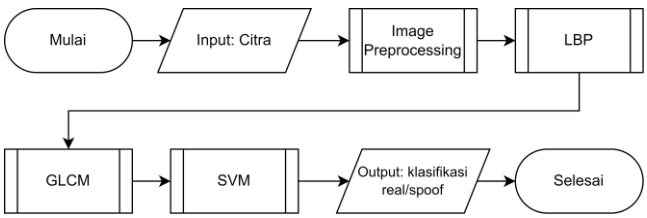
2.1. Pengumpulan Data

CASIA-FASD adalah dataset anti-spoofing wajah yang terdiri dari 50 subjek. Masing-masing subjek memiliki sebuah video wajah asli, spoofing cetak, dan spoofing presentasi menggunakan smartphone. Video direkam menggunakan berbagai jenis kamera: kualitas rendah, kualitas sedang, dan kualitas tinggi. Seluruh video tersimpan dalam format mp4. Video-video tersebut kemudian diubah menjadi serangkaian gambar menggunakan teknik framing. Proses framing ini mengambil setiap frame dari video dan menyimpannya sebagai file gambar dengan format jpg. Contoh gambar pada dataset dapat dilihat pada Gambar 1.

Gambar 1. Contoh Gambar Dataset CASIA-FASD

2.2. Face Spoofing Detection

Face spoofing detection adalah tahapan untuk mengidentifikasikan apakah wajah yang terdeteksi merupakan wajah asli atau spoof. Masukan pada tahap ini adalah citra wajah. Pada tahap ini, pertama data citra akan mendeteksi wajah menggunakan HOG. Kemudian crop area wajah yang terdeteksi menggunakan HOG. Kemudian dilakukan resizing. Resizing dilakukan bertujuan agar seluruh citra memiliki ukuran yang sama, yakni 256x256 piksel. Selanjutnya, data citra akan dilakukan ekstraksi fitur tekstur LBP dan GLCM. Kemudian untuk pengklasifikasiannya menggunakan metode SVM. Adapun parameter yang dilakukan tuning pada SVM yaitu C dan gamma. Keluaran dari tahap face spoofing detection adalah hasil klasifikasi spoofing. Flowchart tahap image preprocessing ditunjukkan pada Gambar 2.

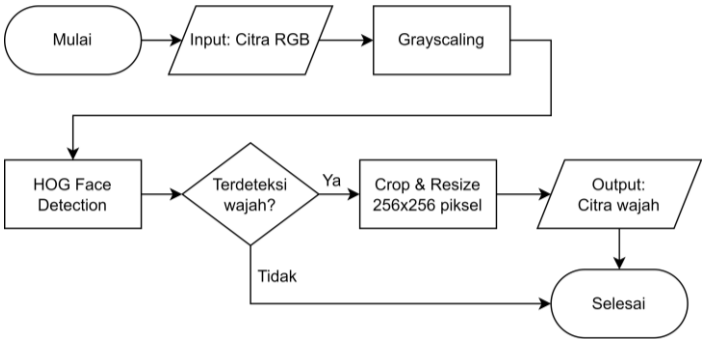


Gambar 2. Flowchart Face Spoofing Detection

p-ISSN: 2301-5373
e-ISSN: 2654-5101

2.2.1.1. Image Preprocessing

Image preprocessing adalah serangkaian teknik yang digunakan untuk mempersiapkan dan memperbaiki kualitas gambar sebelum digunakan dalam analisis atau pemrosesan lebih lanjut. Tujuannya adalah agar gambar lebih mudah dianalisis dan memberikan hasil yang lebih baik. Masukan pada tahap ini adalah data citra berwarna. Pada tahap ini, citra dilakukan grayscaling, yaitu mengubah piksel citra berwarna menjadi citra yang memiliki tingkat warna abu-abu. Kemudian dari citra grayscale tersebut akan dideteksi gambar wajah menggunakan metode Histogram of Oriented Gradients (HOG). Dari wajah yang terdeteksi dilakukan crop pada area wajah. Flowchart tahap image preprocessing ditunjukkan pada Gambar 3.



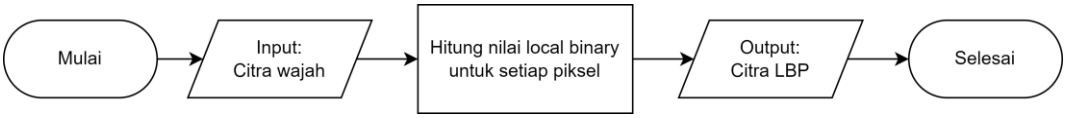
Gambar 3. Flowchart Image Preprocessing

Contoh hasil output pada tahap Image Preprocessing ditunjukkan pada Gambar 4.

Gambar 4. Contoh Hasil Output Image Preprocessing

2.2.1.2. Local Binary Patterns

Local Binary Patterns (LBP) adalah proses ekstraksi fitur pada citra digital yang digunakan dalam pengolahan citra dan pengenalan wajah. Masukan pada tahap ini adalah data citra yang telah dipreprocessing sebelumnya. Proses yang dilakukan pada algoritma LBP adalah dengan mengambil sebuah piksel di citra grayscale, kemudian membandingkan nilai intensitas piksel tersebut dengan nilai intensitas piksel tetangganya. Jika nilai intensitas piksel tetangganya lebih besar dari piksel pusatnya, maka dihasilkan angka 1 pada bit biner. Sebaliknya, jika nilai intensitas piksel tetangganya lebih kecil atau sama dengan piksel pusatnya, maka dihasilkan angka 0 pada bit biner. Dari sini, sebuah pola biner terbentuk pada setiap piksel pada citra. Kemudian bilangan biner tersebut diubah ke bentuk desimal, dan nilai desimal tersebut menjadi nilai baru pada piksel pusat. Keluaran dari tahap ini adalah citra hasil LBP. Flowchart tahapan LBP ditunjukkan pada Gambar 5.



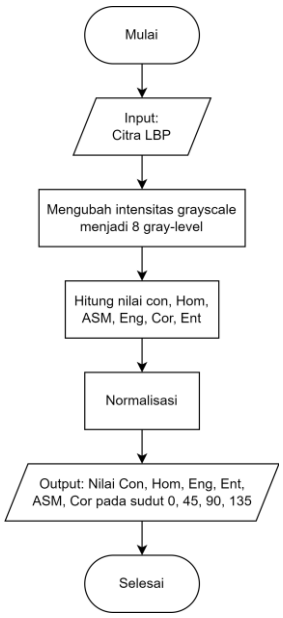
Gambar 5. Flowchart Local Binary Patterns

Contoh hasil output pada tahap Local Binary Patterns ditunjukkan pada Gambar 6.

Gambar 6. Contoh Image Hasil Output Local Binary Patterns

2.2.1.3. Gray-Level Co-occurrence Matrix

Gray-Level Co-occurrence Matrix (GLCM) adalah sebuah metode untuk mengukur tekstur citra dengan menghitung kejadian kemunculan pasangan piksel dengan intensitas tertentu dalam suatu jendela atau area citra. Flowchart tahapan GLCM ditunjukkan pada Gambar 7.

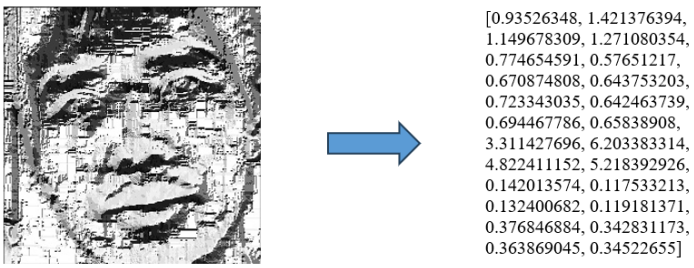


Gambar 7. Flowchart Gray-Level Co-occurrence Matrix

Masukan dari tahap ini adalah citra hasil LBP. Dalam proses pembentukan matriks GLCM, setiap piksel pada citra dianalisis dengan melihat tetangganya. Setiap pasangan tetangga akan dicatat jarak antar piksel dan arah yang dihitung. Selanjutnya, matriks GLCM dibangun dengan menghitung kemunculan relatif dari pasangan piksel dengan level keabuan tertentu. Matriks GLCM kemudian digunakan untuk mengekstraksi fitur-fitur citra, seperti kontras, korelasi, energi, dan homogenitas. Keluaran dari tahap ini adalah nilai kontras, korelasi, energi, dan homogenitas pada sudut 0, 45, 90, 135 pada citra.

Contoh hasil output pada tahap GLCM ditunjukkan pada Gambar 8.

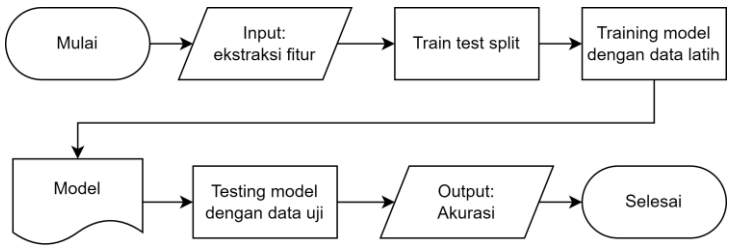
p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 8. Contoh Input dan Output pada Proses Co-occurrence Matrix

2.2.1.4. Support Vector Machine

Support Vector Machine (SVM) adalah algoritma machine learning yang digunakan untuk klasifikasi dan regresi. SVM mencari garis/hyperplane terbaik yang dapat memisahkan data ke dalam kelas-kelas yang berbeda dengan margin maksimal. Masukan pada tahap ini menggunakan data ekstraksi fitur tekstur GLCM. Prosesnya dimulai dengan normalisasi data yang bertujuan untuk mengubah nilai-nilai data menjadi rentang yang serupa. Kemudian, data dibagi menjadi data latih dan data uji dengan perbandingan 80:20. Selanjutnya, data latih digunakan untuk melatih model SVM dan menghasilkan model SVM yang digunakan untuk mengklasifikasikan data uji. Terakhir, dilakukan evaluasi terhadap model SVM dengan menghitung akurasi klasifikasi yang dihasilkan. Keluaran dari tahap ini adalah akurasi dari model. Flowchart tahapan SVM ditunjukkan pada Gambar 9.



Gambar 9. Flowchart Support Vector Machine

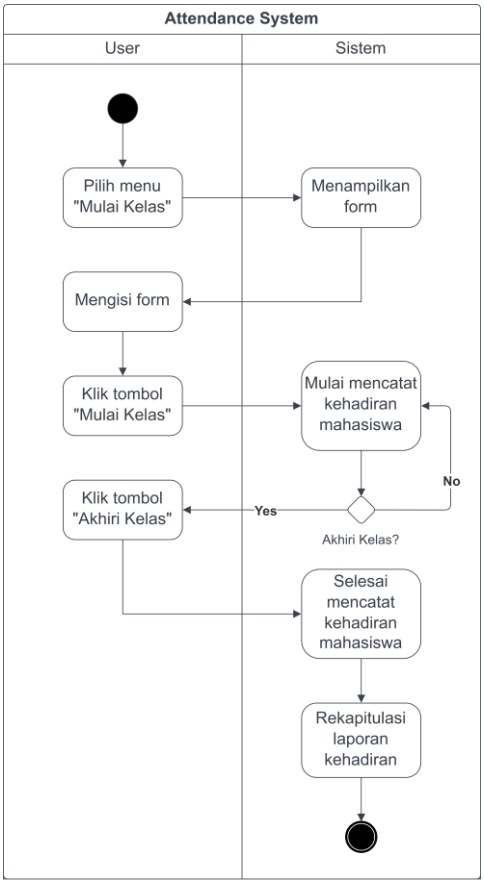
2.3. Sistem Presensi

Sebelum mulai mengembangkan sistem, perlu dilakukan proses analisis kebutuhan pengguna, perancangan sistem, serta pemilihan teknologi yang tepat untuk mengembangkan sistem yang diinginkan. Analisis dapat diterjemahkan dalam bentuk diagram UML untuk memvisualisasikan desain sistem, desain database untuk memodelkan struktur data yang dibutuhkan.

2.3.1.1. Activity Diagram

Activity diagram digunakan untuk merepresentasikan aktivitas atau perilaku suatu sistem, proses bisnis, atau fungsi yang akan dijalankan dalam sebuah sistem. Pada penelitian ini, alur sistem presensi dimulai ketika user memilih menu ‘mulai kelas’, yang merupakan titik awal dari seluruh proses. Sistem kemudian merespon dengan menampilkan form memulai kelas yang memerlukan input kode mata kuliah. Setelah user mengisi dan mengirimkan form tersebut, sistem melakukan proses training face recognition terhadap mahasiswa yang telah melakukan enroll pada mata kuliah tersebut. Proses ini memastikan bahwa sistem dapat mengenali wajah-wajah mahasiswa dengan akurat.

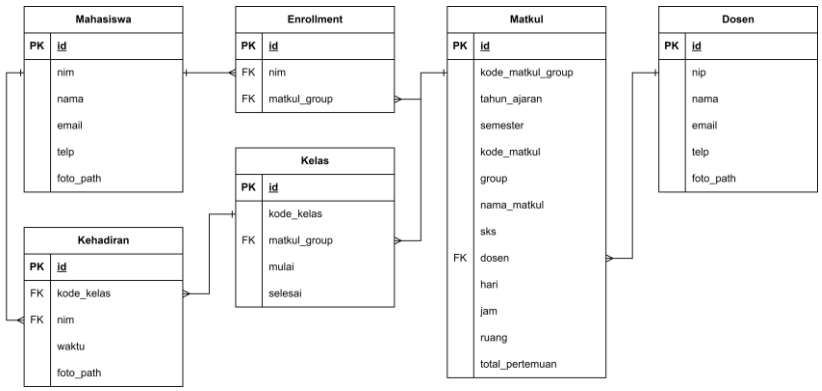
Selanjutnya, sistem secara otomatis mulai merekam kehadiran mahasiswa menggunakan teknologi pengenalan wajah. Proses perekaman ini berlangsung secara terus-menerus hingga dosen memutuskan untuk mengakhiri kelas melalui sistem. Pada tahap akhir, setelah kelas diakhiri, dosen memiliki kemampuan untuk melihat hasil rekapitulasi kehadiran mahasiswa untuk perkuliahan tersebut. Diagram use case yang menggambarkan seluruh proses ini secara lebih rinci dapat dilihat pada Gambar 10. Diagram tersebut memberikan gambaran visual yang membantu dalam memahami bagaimana setiap langkah dalam sistem presensi saling berkaitan dan berinteraksi satu sama lain, sehingga menciptakan sebuah sistem yang efisien dan efektif dalam mencatat kehadiran mahasiswa.



Gambar 10. Activity Diagram

2.3.1.2. Desain Database

Desain database digunakan untuk merancang struktur database untuk memenuhi kebutuhan aplikasi atau sistem informasi. Pada sistem presensi dalam penelitian ini, terdapat enam buah tabel yang masing-masing memiliki peran spesifik untuk memastikan data tersimpan dan dikelola dengan baik. Tabel-tabel tersebut meliputi tabel mahasiswa, dosen, matkul, enrollment, kelas, dan kehadiran. Setiap tabel memiliki atribut-atribut yang saling berhubungan satu sama lain untuk mendukung fungsionalitas sistem. Misalnya, tabel mahasiswa menyimpan data pribadi mahasiswa, tabel dosen menyimpan informasi mengenai dosen, dan tabel matkul menyimpan detail mata kuliah yang diajarkan. Selain itu, tabel enrollment berfungsi untuk mencatat pendaftaran mahasiswa ke dalam mata kuliah tertentu, tabel kelas mencatat informasi mengenai kelas yang diadakan, dan tabel kehadiran mencatat kehadiran mahasiswa dalam setiap sesi perkuliahan. Desain database sistem presensi ini digambarkan secara visual pada Gambar 11, yang memberikan representasi grafis tentang bagaimana tabel-tabel tersebut diatur dan dihubungkan satu sama lain untuk membentuk sebuah sistem yang terpadu dan efisien.



p-ISSN: 2301-5373
e-ISSN: 2654-5101

Gambar 11. Desain Database

2.4. Pengujian Sistem

Pengujian sistem adalah metode untuk memeriksa apakah produk perangkat lunak yang sebenarnya sesuai dengan persyaratan yang diharapkan dan memastikan bahwa produk perangkat lunak bebas dari cacat. Pada tahapan pengujian dibagi menjadi dua, yaitu functional testing dan non functional testing.

2.4.1. Functional Testing

Pada tahap ini dilakukan pengujian functional untuk memverifikasi bahwa setiap fitur aplikasi berfungsi sesuai dengan persyaratan yang telah ditentukan. Pada penelitian ini, functional testing menggunakan metode Black Box Testing.

2.4.2. Non-Functional Testing

Pada tahap ini dilakukan pengujian non-functional untuk memverifikasi pada kebutuhan non-fungsional seperti performa dan kegunaan sebuah aplikasi. Pada penelitian ini, non functional testing menggunakan akurasi deteksi spoofing sebagai penilaiannya. Pengujian dilakukan dengan beberapa skenario uji, di antaranya membandingkan ekstraksi fitur LBP, GLCM, dan LBP-GLCM untuk mengetahui pengaruh penggunaan ekstraksi fitur terhadap akurasi deteksi spoofing dan pengenalan wajah. Untuk menghitung akurasi dapat dilakukan dengan cara membagi jumlah prediksi yang benar dengan jumlah percobaan yang dilakukan. Persamaan menghitung akurasi dapat dilihat pada rumus berikut.

$$Akurasi = \frac{TP+TN}{TP+FN+FP+TN} \times 100\% \qquad (1)$$

Keterangan:

TP = True Positive (sistem benar mengidentifikasi wajah spoofing)

TN = True Negative (sistem benar mengidentifikasi wajah asli)

FP = False Positive (sistem keliru mengidentifikasi wajah asli sebagai spoofing)

FN = False Negative (sistem keliru mengidentifikasi wajah spoofing sebagai wajah asli)

Penelitian ini menggunakan beberapa skenario uji untuk menguji keberhasilan deteksi spoofing. Pengujian dilakukan pada beberapa skenario uji, seperti penggunaan atribut wajah kacamata, rotasi citra wajah, dan pencahayaan indoor/outdoor. Hal ini bertujuan untuk mengetahui sejauh mana kemampuan algoritma dalam mengenali wajah yang memiliki kondisi yang berbeda-beda, sehingga dapat diketahui kehandalan dan kelemahan algoritma dalam berbagai situasi. Hasil pengujian pada scenario uji tersebut kemudian dievaluasi dan dibandingkan dengan hasil pengujian pada scenario uji lainnya untuk mendapatkan pemahaman yang lebih lengkap mengenai kinerja algoritma deteksi spoofing.

3. Hasil dan Pembahasan

3.1. Pengujian Spoofing Detection

Dalam pengujian model deteksi spoofing, dilakukan beberapa skenario pengujian untuk mengevaluasi performa dan karakteristik model. Skenario pengujian meliputi pengujian terhadap nilai C dan gamma, pengaruh penggunaan atribut wajah kaca mata, pengaruh angle wajah, dan pengaruh pencahayaan indoor/outdoor. Pengujian dilakukan dengan tujuan untuk menentukan kombinasi parameter terbaik, menguji kemampuan model dalam mendeteksi spoofing dengan variasi atribut wajah kaca mata dan angle wajah

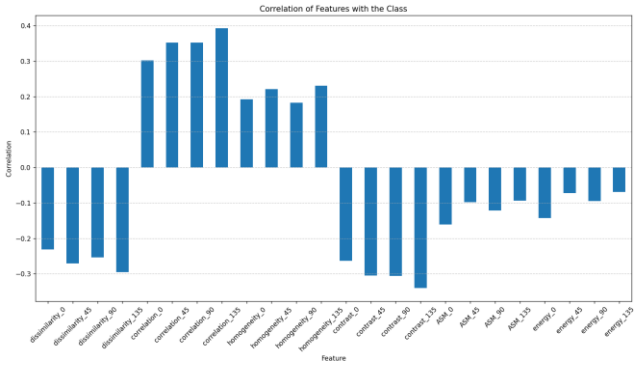
3.1.1. Skenario Pengujian terhadap Nilai C dan Gamma

Dalam skenario pengujian terhadap nilai C dan gamma, dilakukan eksperimen dengan menggunakan beberapa nilai C dan gamma yang berbeda. Rentang nilai C yang diuji meliputi 0.1, 1, 10, 100, 1000, dan 10000, sedangkan untuk gamma diuji dengan nilai 1, 0.1, 0.01, 0.001, dan 0.0001. Hasil pengujian ditunjukkan pada Tabel 1.

Tabel 1. Hasil Akurasi dengan Kombinasi Nilai C dan Gamma

		C					
		0.1	1	10	100	1000	10000
Gamma	1	64%	69%	64%	63%	63%	61%
	0.1	67%	68%	78%	84%	76%	72%
	0.01	63%	66%	66%	84%	94%	86%
	0.001	61%	61%	64%	67%	69%	70%
	0.0001	61%	61%	61%	61%	67%	63%

Setelah melalui pengujian, ditemukan hasil terbaik pada nilai C sebesar 1000 dan gamma sebesar 0.01. Hasil pengujian ini menunjukkan bahwa model SVM dengan konfigurasi parameter tersebut memberikan akurasi sebesar 94% dalam mendeteksi spoofing. Hal ini menunjukkan bahwa kombinasi nilai C dan gamma tersebut mampu memberikan performa terbaik dalam memisahkan kelas-kelas data pada model SVM, sehingga menghasilkan tingkat akurasi yang tinggi dalam deteksi spoofing.



Gambar 12. Korelasi Fitur-Fitur terhadap Kelas Label

Gambar 12 menunjukkan korelasi antara 24 fitur dan 1 kolom kelas. Setiap titik pada grafik mewakili satu fitur, dengan koordinat x menunjukkan nama fitur dan koordinat y menunjukkan nilai koefisien korelasi Pearson antara fitur tersebut dengan kelas. Nilai korelasi dapat berkisar antara -1 hingga 1.

Berdasarkan gambar, terdapat beberapa fitur dengan nilai korelasi tinggi (absolut) terhadap kelas. Fitur-fitur ini kemungkinan besar memiliki pengaruh signifikan terhadap kelas. Contohnya, fitur "dissimilarity_45" memiliki nilai korelasi 0.35, menunjukkan hubungan positif yang cukup kuat dengan kelas. Artinya, semakin tinggi nilai "dissimilarity_45", semakin tinggi kemungkinan data tersebut termasuk dalam kelas tertentu.

Sebaliknya, fitur "homogeneity_90" memiliki nilai korelasi -0.28, menunjukkan hubungan negatif yang cukup kuat dengan kelas. Artinya, semakin tinggi nilai "homogeneity_90", semakin rendah kemungkinan data tersebut termasuk dalam kelas tertentu.

3.1.2. Skenario Pengujian terhadap Pengaruh Penggunaan Atribut Wajah

Pada skenario ini, dilakukan dua kondisi uji coba yang berbeda. Pertama, tanpa atribut kaca mata dan topi, di mana pengujian dilakukan pada wajah asli tanpa perubahan atau penambahan apapun. Kedua, dengan atribut tambahan berupa kaca mata dan topi, di mana pengujian dilakukan untuk menguji kemampuan model dalam mendeteksi spoofing pada wajah yang telah dimodifikasi dengan atribut tersebut.

Tabel 2. Hasil Pengujian Model Terhadap Pengaruh Penggunaan Atribut Wajah

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Skenario	Akurasi
Tanpa Atribut	90%
Dengan Atribut	90%

Pada Tabel 2 menunjukkan bahwa model deteksi spoofing menggunakan metode SVM dengan ekstraksi fitur LBP dan GLCM memiliki tingkat keberhasilan yang sangat baik. Model ini mencapai akurasi sebesar 90% dalam mendeteksi spoofing pada wajah tanpa atribut seperti kacamata dan topi, serta akurasi sebesar 85% dalam mendeteksi spoofing pada wajah dengan atribut tersebut. Hasil ini mengindikasikan bahwa metode tersebut memiliki potensi untuk menjadi solusi yang efektif dalam mendeteksi spoofing pada berbagai kondisi wajah, baik dengan maupun tanpa atribut.

3.1.3. Skenario Pengujian terhadap Pengaruh Angle Wajah

Dalam skenario pengujian terhadap pengaruh angle wajah, dilakukan dua kondisi uji coba yang berbeda. Pertama, kondisi angle wajah lurus di mana pengujian dilakukan menggunakan citra atau data dengan angle wajah tegak lurus terhadap kamera. Kedua, kondisi angle wajah miring, di mana variasi angle wajah dilakukan hingga lebih dari 45 derajat.

Tabel 3. Hasil Pengujian Model Terhadap Pengaruh Angle Wajah

Skenario	Akurasi
Lurus	90%
Miring	90%

Hasil pengujian menunjukkan bahwa model deteksi spoofing menggunakan metode SVM dengan ekstraksi fitur LBP dan GLCM sangat handal dalam mendeteksi spoofing pada berbagai angle wajah. Model ini mencapai akurasi 100% dalam mendeteksi spoofing pada wajah dengan angle lurus dan 90% pada wajah dengan angle miring. Tingkat keberhasilan yang tinggi ini menandakan bahwa metode tersebut efektif dalam berbagai kondisi angle wajah.

3.1.4. Skenario Pengujian terhadap Pengaruh Pencahayaan Indoor/Outdoor

Dalam skenario pengujian pengaruh pencahayaan indoor dan outdoor terhadap model deteksi spoofing, dua kondisi uji coba dilakukan. Pertama, pada kondisi pencahayaan indoor di mana citra atau data diambil di dalam ruangan dengan pencahayaan yang terkendali. Pada kondisi ini, tingkat noise cenderung rendah dengan Signal-to-Noise Ratio (SNR) yang tinggi, umumnya di atas 20 dB. Kedua, pada kondisi pencahayaan outdoor di mana citra atau data diambil di luar ruangan dengan variasi pencahayaan yang lebih bervariasi dan terpengaruh oleh faktor-faktor eksternal seperti sinar matahari, bayangan, dan gangguan lainnya. Pada kondisi outdoor, tingkat noise cenderung tinggi dengan SNR yang rendah, dapat di bawah 10 dB.

Tabel 4. Hasil Pengujian Model Terhadap Pengaruh Pencahayaan Indoor/Outdoor

Skenario	Akurasi
Indoor	90%
Outdoor	75%

Dalam skenario pengujian terhadap pengaruh pencahayaan indoor/outdoor, hasilnya menunjukkan bahwa model memberikan akurasi sebesar 90% dalam mendeteksi spoofing pada dalam ruangan, namun hanya 75% dalam mendeteksi spoofing pada luar ruangan. Hal ini menunjukkan bahwa model kurang bekerja dengan baik dalam kondisi luar ruangan, mungkin karena perubahan pencahayaan yang lebih kompleks dan variabel di luar ruangan.

3.2. Pengujian Sistem Presensi

Pengujian sistem presensi dilakukan dengan pendekatan Black box Testing, di mana sistem presensi dievaluasi berdasarkan input dan output yang dihasilkan, tanpa memperhatikan detail implementasi internalnya. Pada tahap ini, berbagai skenario pengujian dilakukan dengan memberikan berbagai input ke sistem presensi dan mengamati keluaran yang dihasilkan. Tujuan dari pengujian ini adalah untuk memverifikasi bahwa sistem presensi berfungsi sesuai dengan yang diharapkan, mencakup fungsionalitas seperti memulai kelas, pengelolaan data mahasiswa, dan pelaporan.

Tabel 5. Skenario Pengujian Sistem Presensi

No	Skenario Pengujian	Hasil Diharapkan	Hasil Uji
1	Mulai kelas	Menambahkan kelas ke database, menampilkan halaman kelas	Sesuai harapan
2	List kelas yang sedang berlangsung	Menampilkan list kelas sedang berlangsung	Sesuai harapan
3	Masuk ke kelas	Menuju ke halaman kelas.	Sesuai harapan
4	Presensi menggunakan spoofing	Menampilkan bounding box berwarna merah di sekitar wajah	Sesuai harapan
5	Presensi menggunakan citra wajah namun tidak dikenali sebagai peserta mata kuliah	Menampilkan bounding box berwarna biru di sekitar wajah, dan keterangan “Unknown”	Sesuai harapan
6	Presensi menggunakan citra wajah peserta mata kuliah	Menampilkan bounding box berwarna biru di sekitar wajah, dan keterangan NIM peserta. Input data kehadiran ke database.	Sesuai harapan

Hasil positif dari 6 skenario pengujian ini menegaskan bahwa sistem presensi yang telah dikembangkan mampu beroperasi sesuai dengan tujuan awal dan mampu mengatasi berbagai situasi yang beragam. Keberhasilan ini membuktikan bahwa sistem mampu mendukung kehadiran mahasiswa secara efektif, mengelola data mahasiswa dan dosen dengan akurat, serta menghasilkan laporan yang relevan dan sesuai dengan kebutuhan. Dengan demikian, sistem presensi ini memenuhi standar kualitas dan performa yang diharapkan, serta siap digunakan untuk membantu dalam manajemen presensi mahasiswa secara efisien.

Tabel 6. Hasil Pengujian Model Terhadap Pengaruh Pencahayaan Indoor/Outdoor

Skenario	Akurasi
Lurus	90%
Miring	90%

Hasil pengujian ini menunjukkan bahwa model memberikan akurasi sebesar 95% dalam mendeteksi spoofing ketika diimplementasikan dalam sistem presensi, yang menunjukkan tingkat keberhasilan yang sangat baik dalam kondisi tersebut. Hal ini menandakan bahwa metode SVM dengan ekstraksi fitur LBP dan GLCM baik dalam mendeteksi spoofing pada wajah ketika diimplementasikan dalam sistem presensi.

4. Kesimpulan

Berdasarkan rangkaian penelitian dan pengembangan model deteksi spoofing menggunakan metode Support Vector Machine (SVM) dengan ekstraksi fitur tekstur Local Binary Patterns (LBP) dan Gray-Level Co-occurrence Matrix (GLCM), serta pengembangan sistem presensi, dapat diambil beberapa simpulan penting sebagai berikut:

a. Hasil penelitian menunjukkan bahwa deteksi spoofing menggunakan ekstraksi fitur tekstur Local Binary Patterns (LBP) dan Gray-Level Co-occurrence Matrix (GLCM) dengan metode Support Vector Machine (SVM) memberikan hasil akurasi 94%. Dalam penelitian ini, dilakukan tuning parameter C dan gamma. Hasil terbaik diperoleh dengan nilai C sebesar 1000 dan gamma sebesar 0,01. Dengan nilai parameter ini, model SVM berhasil mencapai tingkat akurasi sebesar 94%. Hasil ini menunjukkan bahwa SVM dengan kombinasi fitur LBP dan GLCM dapat efektif dalam mendeteksi spoofing.
b. Peneliti melakukan serangkaian percobaan di berbagai kondisi, termasuk indoor-outdoor, tanpa atribut-dengan atribut kacamata dan topi, dan angle wajah lurus dan miring. Hasil

p-ISSN: 2301-5373
e-ISSN: 2654-5101

percobaan menunjukkan tingkat keberhasilan yang signifikan, dengan akurasi mencapai 90% untuk kondisi tanpa atribut, 85% untuk kondisi dengan atribut, 90% untuk kondisi wajah lurus, dan 90% untuk kondisi wajah miring. Namun, terdapat penurunan akurasi pada kondisi outdoor, dimana akurasi mencapai 75%, yang lebih rendah dibandingkan dengan kondisi indoor. Penurunan ini mungkin disebabkan oleh faktor lingkungan seperti pencahayaan yang lebih bervariasi, gangguan dari sinar matahari, bayangan, dan elemen lainnya yang dapat mempengaruhi kualitas citra wajah.

c. Setelah melakukan non-functional testing dan functional testing pada sistem presensi anti-spoofing, dapat disimpulkan bahwa hasilnya memenuhi harapan. Sistem ini mampu memulai kelas, mencatat kehadiran mahasiswa, serta menghasilkan laporan kehadiran yang valid. Seluruh fungsi sistem telah diuji secara menyeluruh dan memperoleh tingkat akurasi 95% dalam pendeteksian spoofing.

Referensi

[1] M. Surve, et al., "Automatic attendance system using face recognition technique," in International Journal of Recent Technology and Engineering, vol. 9, no. 1, pp. 2134-2138, Jan. 2020.

[2] F. Jiang, P. Liu, and X. Zhou, "Multilevel fusing paired visible light and near-infrared spectral images for face anti-spoofing," Pattern Recognition Letters, vol. 128, pp. 30-37, 2019.

[3] N. Daniel and A. Anitha, "Texture and quality analysis for face spoofing detection," Computers & Electrical Engineering, vol. 94, p. 107293, 2021.

[4] I. B. Kusuma and A. Kartika, "Image spoofing detection using local binary pattern," J. Masy. Inform. Indones., vol. 2, no. 1, pp. 49-54, 2017.

[5] A. D. Alexander, R. Salkiawati, H. Lubis, F. Rahman, H. Herlawati, and R. T. Handayanto, "Local Binary Pattern Histogram for Face Recognition in Student Attendance System," in 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), vol. 152, no. 156, p. 012014, Sept. 2020, IEEE.

This page is intentionally left blank.