Komputika: Jurnal Sistem Komputer
Volume 13, Nomor 1, April 2024, hlm. 139 - 147
Terakreditasi Peringkat 3, SK No. 148/M/KPT/2020
DOI: **10.34010/komputika.v13i1.12217**

ISSN: 2252-9039 (print)
ISSN: 2655-3198 (online)

Prototipe Sederhana Sistem Deteksi Kriminal Berbasis Internet Of Things Menggunakan Teknologi YOLOv5

Afris Nurfal Aziz[1], Hani'atul Khoiriyah[1], Fauzan Abdillah[1], I Gede Wiryawan[2*]

[1)]Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Jember
Jl. Mastrip Nomor 164 Sumbersari, Jember, Indonesia 68121

[2)] Program Studi Teknik Komputer, Jurusan Teknologi Informasi, Politeknik Negeri Jember
Jl. Mastrip Nomor 164 Sumbersari, Jember, Indonesia 68121

**email: wiryawan@polije.ac.id*

(Naskah masuk: *26 Januari 2024*; diterima untuk diterbitkan: *13 Mei 2024*)

ABSTRAK *– Kriminalitas merupakan segala tindakan atau sesuatu yang dilakukan individu, kelompok, maupun komunitas yang melanggar hukum atau suatu tindakan kejahatan, yang mengganggu keseimbangan atau stabilitas sosial dalam masyarakat. Salah satu alat yang digunakan dalam memantau keamanan di berbagai tempat seperti rumah, kantor, dan tempat umum lainnya adalah Closed-Circuit Television (CCTV). Namun, meskipun telah banyak terpasang, permasalahannya masih banyak kejahatan yang terjadi karena keterbatasan dalam pemantauan dan pengawasan oleh petugas keamanan. Oleh karena itu, solusi berupa pengembangan sistem deteksi kriminal menggunakan metode deep learning dianggap penting untuk meningkatkan keamanan dan menurunkan tingkat kriminalitas. Tujuan sistem deteksi kriminal untuk meningkatkan keamanan, mencegah terjadinya tindak kriminal di suatu wilayah atau tempat tertentu. Tahapan utama dalam studi ini dimulai dari pengumpulan data, perancangan sistem, implementasi dan integrasi sistem, serta pengujiannya. Teknologi yang digunakan yaitu YOLOv5 dan didukung perangkat keras berbasis Internet of Things. Sistem berhasil mendeteksi objek violence 92% dan robbery 91% dalam pengujian awal tanpa latar belakang. pengujian kedua dengan latar belakang, sistem berhasil mendeteksi objek violence 93% dan robbery 53%. Sistem berhasil mendeteksi objek violence 91% dan robbery 83% pada pengujian secara real-time. Kontribusi dari studi ini berupa tingkat akurasi tinggi yang didapatkan dalam mendeteksi aktivitas kriminal, seperti kekerasan dan pencurian.*

Kata Kunci *– deteksi; kriminalitas; CCTV; Internet of Things; YOLOv5.*

Simple Prototype of Internet of Things Based Crime Detection System Using YOLOv5 Technology

ABSTRACT – Crime is action or thing carried out by an individual, group or community that violates the law or a criminal act, which disrupts social balance or stability in society. One of the tools used to monitor security in various places i.e. homes, offices and other public places is Closed-Circuit Television (CCTV). However, even though many its have been installed, the problem is that many crimes still occur due to limitations in monitoring and supervision by security officers. Therefore, a solution in the form of developing a crime detection system using deep learning methods is considered important to increase security and reduce crime rates. The aim of a criminal detection system is to increase security, prevent criminal acts in a certain area or place. The main stages in this study start from data collection, system design, implementation and integration, and testing. The technology used is YOLOv5 and is supported by Internet of Things-based hardware. The system succeeded in detecting violence objects 92% of the time and robbery 91% in initial testing without background. In the second background test, the system succeeded in detecting violence objects 93% of the time and robbery 53%. The system succeeded in detecting violence objects 91% and robbery 83% of the time in real-time testing. The contribution of this study is the level of accuracy obtained in

in detecting criminal activity, such as violence and robbery.

Keywords *– detection; crime; CCTV; Internet of Things; YOLOv5*

1. PENDAHULUAN

Kriminalitas secara harfiah berasal dari kata *crimen* yang artinya kejahatan, tindak kriminal, atau juga diartikan suatu tindakan kejahatan, sehingga merupakan tindakan yang bersifat negatif [1]. Tindakan ini akan merugikan banyak pihak dan pelaku tindakannya disebut sebagai seorang kriminal. Sederhananya, kriminalitas merupakan segala tindakan atau sesuatu yang dilakukan individu, kelompok, maupun komunitas yang melanggar hukum atau suatu tindakan kejahatan, yang mengganggu keseimbangan atau stabilitas sosial dalam masyarakat. Kriminalitas merupakan masalah serius yang selalu dihadapi dan sulit dihindari di berbagai negara, baik negara maju maupun negara berkembang [2], dan masih menjadi perhatian utama Indonesia sebagai salah satu negara berkembang di dunia.

Banyak kasus kriminalitas yang terjadi setiap tahun, seperti pencurian, perampokan, dan tindak kekerasan. Kriminalitas ini dipicu oleh beberapa faktor yang diantaranya tingginya jumlah pengangguran [3][4] dan juga kepadatan penduduk [5]. Angka tindak kriminalitas tahun 2022 naik sebesar 7,3 persen dari tahun sebelumnya. Dikutip dari Statistik Kriminal 2023, jumlah kejadian kejahatan di Indonesia sempat mengalami penurunan, dari yang semula sebanyak 247.218 kejadian di tahun 2020 menjadi 239.481 kejadian di tahun 2021. Namun, terjadi peningkatan jumlah kejadian kejahatan yang cukup drastis di tahun 2022 menjadi sebanyak 372.965 kejadian [6]. Jika dirata-ratakan, terdapat 31,6 kejahatan setiap jamnya. Sementara, penyelesaian perkara mengalami penurunan. Dari sumber yang berbeda, Kapolri Listyo Sigit Prabowo merincikan tingkat kejahatan itu meningkat 18,764 kasus menjadi 276.507 perkara dari sebelumnya 257.743 kasus pada 2021. Sebanyak 276.507 perkara itu terjadi dalam setahun. Polri juga mengaku jumlah penyelesaian kasus turut menurun sebanyak 0,9 persen dengan rincian sebanyak 1,877 kasus. Pada tahun 2021, Korps Bhayangkara mencatatkan sebanyak 202.024 kasus berhasil diselesaikan, sementara pada 2022 mereka hanya berhasil menyelesaikan 200.147 kasus. (Sumber: CNN Indonesia).

Salah satu alat yang digunakan dalam memantau keamanan di berbagai tempat seperti rumah, kantor, dan tempat umum lainnya adalah *Closed-Circuit Television* (CCTV). CCTV memiliki peran sebagai kamera pengawas dan pengintai yang dapat memantau situasi dan kondisi secara real time yang juga mampu menekan aksi kejahatan untuk terjadi [7]. Namun, meskipun telah terpasang banyak CCTV, masih banyak kejahatan yang terjadi karena keterbatasan dalam pemantauan dan pengawasan oleh petugas keamanan. Selain itu, jumlah pelaku kejahatan juga semakin meningkat sehingga membutuhkan peran teknologi yang dapat mendeteksi perilaku kriminal. Menurut artikel jurnal *Design of An Intelligent Video Surveillance System For Crime Prevention: Applying Deep Learning Technology* yang diterbitkan oleh Springer Nature pada tahun 2021, disebutkan bahwa untuk pendeteksian dan pencegahan kejahatan yang lebih baik, dibutuhkan sistem pengawasan video yang secara aktif menanggapi insiden dan memproses gambar secara *real-time* tanpa deteksi langsung dari tenaga manusia [8]. Namun, penerapan dari teknologi tersebut belum diterapkan di negara Indonesia. Sebelum diusulkannya studi mengenai sistem pengawasan untuk deteksi dan pencegahan kejahatan, pengawasan dengan video juga telah diusulkan untuk menerapkan *intellegent traffic*. Hasil penilaian dari studi tersebut menetapkan usulan kerja sistem pengawasan video lalu lintas dan identifikasi kecelakaan memberikan tingkat eksekusi yang sangat tinggi dalam hal akurasi, presisi, *recall*, sensitivitas, spesifisitas dan waktu deteksi [9]. Selain itu juga terdapat studi mengusulkan sistem pengawasan video *end-to-end* yang dapat digunakan sebagai titik awal untuk sistem yang lebih kompleks. Berbagai eksperimen juga telah dicoba pada model terlatih dengan observasi yang dijelaskan secara rinci. Studi tersebut menyelesaikannya dengan membahas pendekatan deteksi objek video dan deteksi objek menonjol video yang berpotensi digunakan sebagai perbaikan di masa depan terhadap sistem yang diusulkan [10].

Pemanfaatan perangkat *Internet of Things* sebelumnya sudah banyak dikembangkan. Salah satunya adalah dengan menggunakan sensor *Passive Infrared* (PIR), HC- SR501, dalam mendeteksi gerakan untuk keamanan. Hasilnya adalah pada jarak efektif dari HC- SR501, *passive infrared* sensor, saat mengenai human detektor adalah 0meter sampai 5 meter, ESP32-CAM akan mengirimkan gambar atau video yang artinya ada indikasi pencuri atau orang yang tidak dikenal memasuki rumah. Sedangkan pada jarak 5 meter lebih, HC-SR501 *passive infrared* sensor tidak mengirimkan gambar yang artinya aman [11]. Di samping itu juga terdapat studi yang merancang sebuah sistem pada perangkat CCTV yang mampu memilih citra untuk mengurangi ukuran berkas data

citra yang disimpan dengan pengolahan citra. Pemilihan data dilakukan berbasis pendeteksian objek pada citra dengan metode *adaptive median* pada ruangan tertutup dengan penerangan yang cukup. Pada saat ada objek terdeteksi, maka yang akan disimpan adalah citra masukan sistem. Sebaliknya, jika tidak ada objek terdeteksi maka yang data akan di simpan ke berkas keluaran sistem adalah citra model latar [12].

Oleh karena itu, pengembangan sistem deteksi kriminal pada CCTV menggunakan metode *deep learning* dianggap penting untuk meningkatkan keamanan dan menurunkan tingkat kriminalitas di Indonesia. Metode *deep learning* telah terbukti efektif dalam deteksi objek pada gambar dan video, dan telah banyak digunakan dalam berbagai aplikasi seperti pengenalan wajah dan deteksi objek. Dalam konteks ini, pengembangan prototipe sistem deteksi kriminal pada CCTV dapat membantu petugas keamanan dalam memantau potensi tindak kejahatan, sehingga dapat segera diambil tindakan preventif atau penanggulangan yang cepat dan tepat. Dari prototipe sistem deteksi kriminal pada CCTV tersebut diharapkan dapat meminimalisir angka kejahatan di Indonesia dan menjadikan Indonesia sebagai negara maju pada tahun 2045 dengan tingkat kriminalitas yang rendah.

Tujuan dari sistem deteksi kriminal untuk meningkatkan keamanan dan mencegah terjadinya tindak kriminal di suatu wilayah atau tempat tertentu. Sistem deteksi kriminal untuk membantu mengidentifikasi perilaku yang mencurigakan atau aktivitas kriminal, seperti pencurian, vandalisme, atau tindak kekerasan. Kemudian Sistem deteksi kriminal juga dapat membantu meningkatkan efisiensi operasi dan manajemen keamanan. Sistem deteksi kriminal untuk membantu memonitor dan menganalisis CCTV secara otomatis, sehingga memungkinkan petugas keamanan untuk lebih fokus pada tugas-tugas lainnya, seperti patroli keamanan atau pemantauan lalu lintas. Sistem deteksi kriminal ini juga diharapkan dapat mendeteksi gerakan yang lebih sensitif dari sistem yang dimiliki CCTV. Selain itu, sistem deteksi kriminal pada CCTV untuk membantu penyidik dalam penyelidikan kriminal. Manfaat dengan adanya sistem deteksi kriminal ini Membantu penyidik dalam penyelidikan kriminal karena sistem dapat mengidentifikasi pelaku, kendaraan yang digunakan, atau rute pelaku saat melakukan tindak kriminal. Sistem deteksi kriminal meningkatkan efisiensi operasi dan manajemen keamanan. Sistem dapat membantu memonitor dan menganalisis CCTV secara otomatis, sehingga memungkinkan petugas keamanan untuk lebih fokus pada tugas-tugas lainnya. Hal ini kedepannya dapat meningkatkan efisiensi operasi dan manajemen keamanan.

2. METODE DAN BAHAN

Pada tahap awal pengembangan, inspirasi untuk mengembangkan prototipe sistem deteksi kriminal muncul sebagai tanggapan terhadap meningkatnya kekhawatiran terkait keamanan masyarakat. Faktor-faktor seperti meningkatnya tindak kriminalitas, kendala yang dihadapi oleh penegak hukum, dan perkembangan teknologi deteksi objek menjadi pemicu utama. Tahapan perencanaan awal diperlukan untuk merinci visi dan tujuan pengembangan. Ini melibatkan penentuan area pengujian, jenis teknologi yang akan digunakan yaitu YOLOv5 dan didukung perangkat keras berbasis *Internet of Things*, dan pemilihan anggaran serta sumber daya yang diperlukan. Tahap selanjutnya ialah analisis kebutuhan, dan berikut merupakan komponen perangkat keras dan perangkat lunak yang dibutuhkan untuk prototipe sistem deteksi kriminal untuk meminimalisir tindak kriminalitas di Indonesia diantaranya Perangkat Keras yaitu Kamera Webcam sebagai alternatif dari CCTV, Raspberry Pi 4, Robot, Komputer dengan spesifikasi processor Ryzen 5 3500U, RAM 8 GB, Harddisk 1 TB, dan layar monitor 14 inch. Perangkat lunak bantu yaitu Visual Studio Code, Google Colab dan Firebase.

Pada tahap berikutnya dilakukan pengambilan dataset untuk sistem prototipe deteksi kriminal melibatkan pengumpulan sebanyak 450 gambar yang dibagi menjadi tiga kelas utama. Kelas pertama, "*robbery*", terdiri dari 150 gambar yang mencakup berbagai situasi terkait tindakan menodong senjata [13][14]. Kelas kedua, "*violence*", juga terdiri dari 150 gambar yang menunjukkan berbagai tindakan kekerasan atau perkelahian. Sementara itu, kelas ketiga, "normal,". Kemudian proses pengumpulan data dilanjutkan dengan pengambilan sampel data sekunder, yakni rekaman video yang melibatkan dua robot dalam peragakan aktivitas kejahatan atau perilaku mencurigakan. Penggunaan robot dalam pengambilan sampel ini dipilih karena mereka tidak memiliki emosi atau risiko kesehatan, memungkinkan penggunaan mereka dalam situasi berbahaya tanpa risiko bagi nyawa manusia. Selain itu, robot dapat bekerja secara terus-menerus tanpa perlu istirahat, menjalankan tugas-tugas dengan cepat dan efisien, yang berpotensi menghemat waktu dan sumber daya yang diperlukan untuk pengumpulan data.

Perancangan sistem menjadi tahap selenjutnya dimana dalam tahap desain sistem melibatkan proses perancangan arsitektur sistem, struktur basis data, algoritma, serta antarmuka pengguna (*user interface*) yang akan digunakan oleh pengembang untuk mengimplementasikan solusi atau sistem yang telah direncanakan. Figma merupakan *software* yang

digunakan untuk merancang desain prototipe sistem deteksi kriminal untuk meminimalisir tindak kriminal di Indonesia. Prototipe sistem deteksi kriminal menggunakan YOLOv5 diimplementasikan dalam beberapa langkah-langkah yang diawali *Labeling*, *Training Dataset*, dan Integrasi Sistem. Proses pelabelan menggunakan *platform* Roboflow. Tujuan utama dari pelabelan dataset adalah untuk memperkenalkan dan mengidentifikasi objek-objek kriminal dalam setiap gambar. Proses pelatihan dataset menggunakan *platform* Google Collaboratory, dengan mengatur jumlah iterasi (*epoch*) sebanyak 500 kali.

Langkah terakhir pada tahap implementasi, yaitu integrasi sistem. Dimana sistem diintegrasikan dengan Firebase untuk mengirim data deteksi objek kriminal hanya jika tingkat keyakinan mencapai 80% atau lebih, dengan pengiriman data setiap 10 detik. Hal ini untuk menghindari pengiriman data berlebihan dan memastikan relevansi informasi. Pengujian menjadi tahapan terakhir dari pengembangan prototipe ini. Pengujian (*testing*) adalah tahapan dalam pengembangan sistem di mana prototipe sistem tersebut diperiksa, dievaluasi, dan diuji untuk memastikan bahwa berfungsi sesuai dengan spesifikasi yang telah ditentukan.

3. HASIL DAN PEMBAHASAN

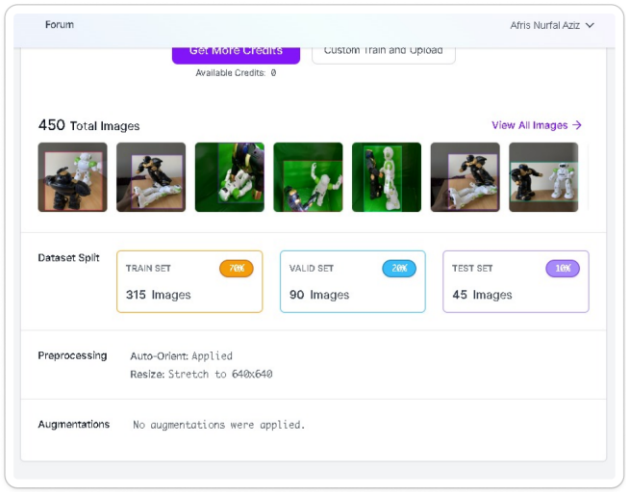
1. Pengambilan Dataset

Pengambilan dataset untuk sistem prototipe deteksi kriminal dilakukan dengan mengumpulkan sebanyak 450 gambar yang terbagi dalam tiga kelas utama. Setiap kelas mewakili jenis tindakan atau situasi tertentu yang relevan dengan tugas deteksi kriminal. Dataset ini mencakup berbagai kondisi, seperti posisi objek dan latar belakang yang berbeda-beda. Pembagian kelas tersebut antara lain 150 gambar untuk kelas "*robbery*", yang mencakup berbagai gambar terkait tindakan menodong senjata [13][14]. 150 gambar untuk kelas "*violence*", yang mencakup berbagai gambar yang menunjukkan tindakan kekerasan atau perkelahian, 150 gambar untuk kelas "normal," yang mencakup gambar-gambar situasi atau tindakan yang tidak terkait dengan tindakan kriminal. Pengambilan dataset ini merupakan langkah awal yang penting dalam pengembangan sistem prototipe deteksi kriminal, karena dataset yang representatif dan seimbang akan membantu model dalam belajar dan mengenali pola-pola yang berhubungan dengan aktivitas kriminal.

2. Pelabelan

Setelah berhasil mengumpulkan dataset sebanyak 450 gambar yang terdiri dari tiga kelas berbeda, langkah berikutnya adalah melakukan proses pelabelan menggunakan *platform* Roboflow. Pelabelan dataset ini adalah tahap krusial dalam persiapan data untuk pelatihan model deteksi kriminal. Dengan bantuan Roboflow, pelabelan dataset dapat dilakukan dengan cepat menambahkan anotasi atau label yang diperlukan pada setiap gambar. Tujuan utama dari pelabelan dataset adalah untuk memperkenalkan dan mengidentifikasi objek-objek kriminal dalam setiap gambar. Dengan melakukan pelabelan yang teliti, dataset akan mengandung informasi penting mengenai pola dari objek-objek tersebut. Hal ini sangat penting dalam proses pelatihan model deteksi kriminal, karena model akan menggunakan dataset yang sudah diberi label untuk memahami ciri-ciri objek kriminal. Dengan kata lain, pelabelan dataset bertujuan untuk "mengajarkan" sistem agar dapat mengenali dan membedakan objek-objek yang relevan dalam konteks deteksi kriminal.

Setelah proses pelabelan selesai, hasilnya akan membagi gambar-gambar tersebut ke dalam tiga lapisan (*layer*) yang berbeda, yaitu *layer* untuk pelatihan (*training*), validasi, dan pengujian (*testing*). Hasil dari pembagian dataset ini, sebanyak 315 gambar akan digunakan sebagai *train-set*, 90 gambar menjadi *valid-set*, dan sisanya yaitu 45 gambar akan ditetapkan sebagai *test-set*. Hasil dapat dilihat pada gambar 1 di bawah.



Gambar 1. Hasil dari Tahap Pelabelan

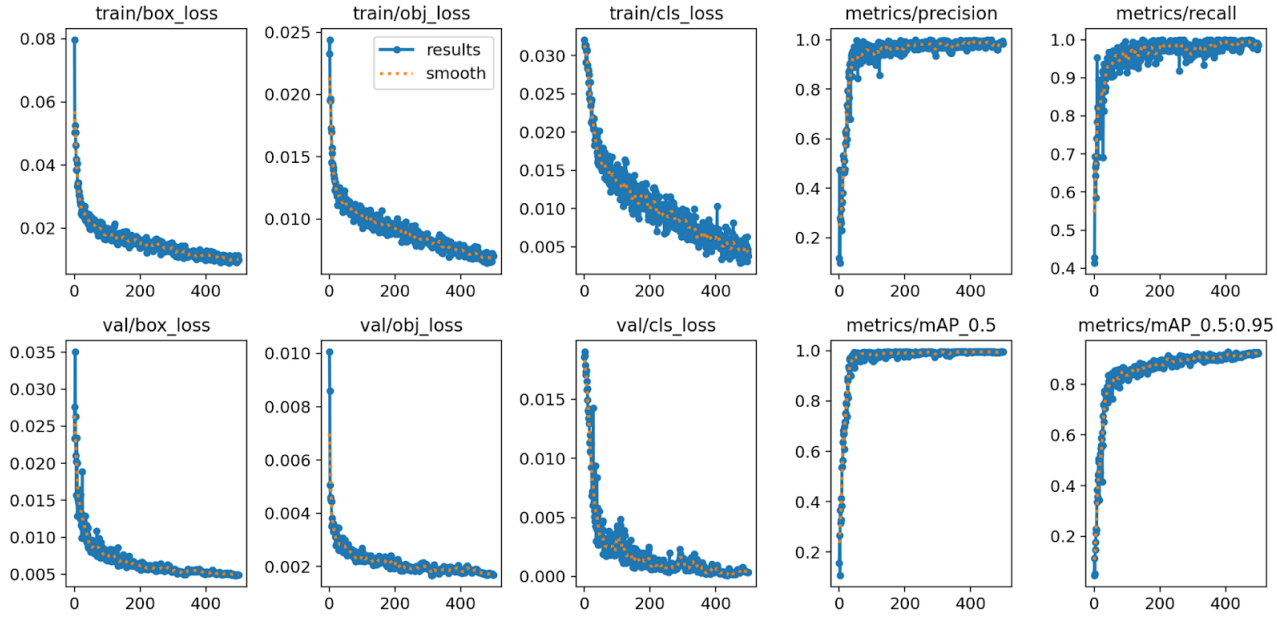
Pembagian dataset ini adalah langkah penting dalam pengembangan model deteksi kriminal. *Train-set* digunakan untuk melatih model, sehingga model dapat memahami dan mengenali pola-pola yang terdapat dalam data pelatihan. *Valid-set* digunakan untuk mengatur parameter-parameter model dan memantau kinerjanya selama proses pelatihan. Sedangkan *test-set* berfungsi untuk menguji sejauh mana model yang telah dilatih mampu mengenali objek kriminal secara obyektif.

Setelah dataset telah dilabeli dengan benar, selanjutnya dilakukan pengunggahan dataset tersebut ke Google Drive. Platform ini digunakan

sebagai penyimpanan awan yang aman dan dapat diakses secara mudah, memungkinkan kolaborator tim untuk mengakses, membagikan, dan mengelola dataset dengan lebih efisien. Dengan dataset yang sudah terlabeli dan disimpan, tahap berikutnya siap untuk dilanjutkan ke proses pelatihan model deteksi kriminal.

3. Training Dataset

Tahap selanjutnya ialah dengan menjalankan proses pelatihan dataset menggunakan *platform* Google Collaboratory, dengan mengatur jumlah iterasi (*epoch*) sebanyak 500 kali. Pemilihan jumlah *epoch* ini bertujuan untuk memberikan model pelatihan kesempatan yang cukup untuk memahami dengan baik pola-pola yang ada dalam dataset deteksi kriminal. Pelatihan pada sejumlah besar *epoch* diharapkan model akan menjadi lebih tajam dalam mengenali objek-objek kriminalitas dalam gambar yang sangat bervariasi. Hasil pelatihan model YOLOv5 pada dataset ini sangat memuaskan. Dengan melakukan pelatihan sebanyak 500 kali epoch, model yang didapatkan berhasil mencapai tingkat akurasi yang sangat tinggi dalam mengenali kelas "normal," "*robbery*", dan "*violence*" seperti pada gambar 2.



Gambar 2. Hasil dari Training Model Data

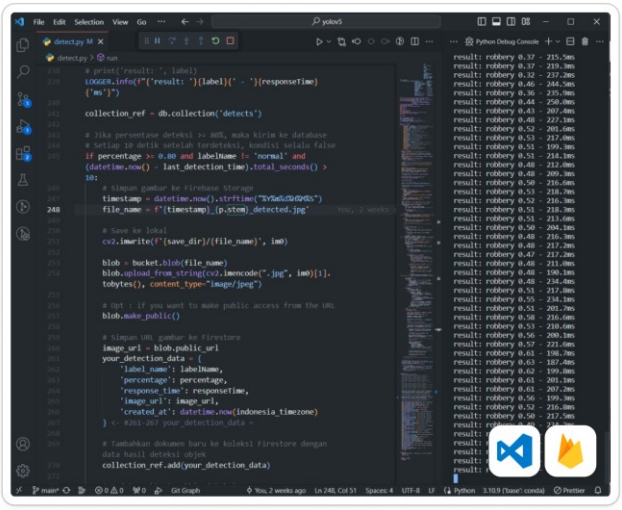
Hasil dari *training data* ini selanjutnya dievaluasi dengan menggunakan metrik-metrik seperti *recall*, *precision*, dan lainnya untuk mengukur kinerja model. *Recall* mengukur kemampuan model untuk mendeteksi sebanyak mungkin objek kriminal yang sebenarnya, sedangkan *precision* mengukur seberapa akurat model dalam mengidentifikasi objek-objek tersebut [15]. Penggunaan metrik ini sebelumnya juga telah dilakukan pada studi yang menggunakan teknologi serupa, yaitu TOLOv5 [16]. Tujuan dengan menggunakan 500 *epoch* ini adalah untuk mencapai keseimbangan yang optimal antara kinerja model dalam mendeteksi objek kriminal dan mengurangi jumlah kesalahan deteksi. Dengan demikian, harapannya dapat menghasilkan model prototipe deteksi kriminal yang andal dan efektif dalam mengidentifikasi situasi berpotensi berbahaya untuk keamanan masyarakat. Dengan jumlah *epoch* yang cukup banyak dapat diyakini bahwa model ini telah mengalami konvergensi yang baik, sehingga mampu menghasilkan hasil deteksi yang akurat dan andal.

Output dari *training dataset* yang berupa file dengan ekstensi .pt memiliki peran penting dalam pengintegrasian model deteksi kriminal ke perangkat seperti Raspberry Pi 4. File tersebut adalah berkas yang berisi parameter-parameter yang telah diatur selama proses pelatihan, termasuk bobot-bobot (*weights*) dari model deteksi.

4. Integrasi Sistem

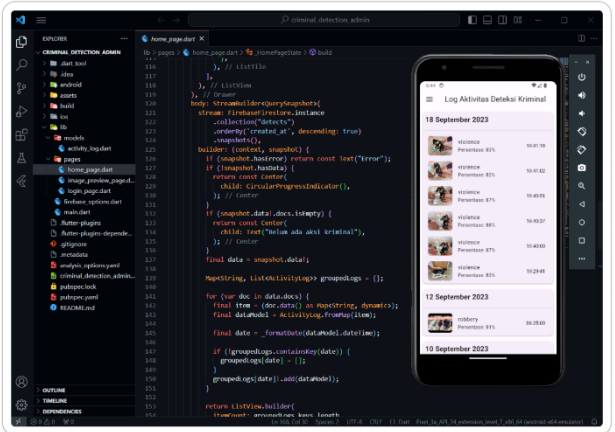
Proses integrasi ke Raspberry Pi 4 melibatkan instalasi perangkat lunak yang sesuai, serta konfigurasi sistem untuk menjalankan model dengan efisien. Integrasi pertama yang dilakukan adalah menghubungkan sistem dengan Firebase, dengan parameter bahwa data akan dikirimkan hanya jika tingkat keyakinan (*confidence*) deteksi objek kriminal mencapai 80% atau lebih. Selain itu, pengaturan sistem telah dilakukan untuk mengirimkan data secara berkala dengan jeda waktu 10 detik antara pengiriman data. Tujuan dari pengaturan ini adalah untuk mencegah pengiriman data yang berlebihan

dan memastikan bahwa informasi yang dikirimkan ke Firebase terkait dengan deteksi objek kriminal hanya dikirimkan ketika cukup relevan dan signifikan. Hal ini akan membantu dalam mengelola data dengan lebih efisien dan menghindari kelebihan beban pada jaringan atau penyimpanan Firebase. Gambar 3 menunjukan proses dan hasil dari integrasi sistem.



Gambar 3. Proses dan Hasil Integrasi Sistem

Sistem yang dikembangkan sudah berhasil terintegrasi dengan Raspberry Pi 4, memungkinkan pemantauan secara *real-time* yang efektif. Selain itu, Firebase juga dimanfaatkan sebagai *database* untuk menyimpan data relevan. Data ini akan tersedia melalui aplikasi *mobile* yang telah dirancang, seperti pada gambar 4 di bawah.



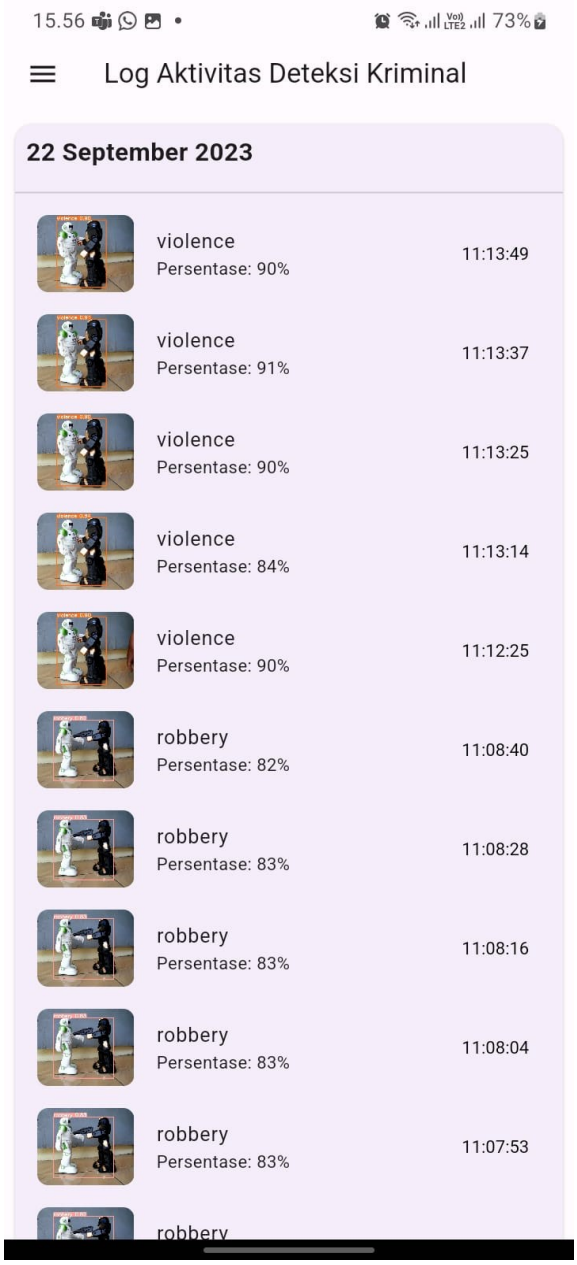
Gambar 4. Hasil Integrasi Sistem dengan Aplikasi Mobile

Kombinasi antara Raspberry Pi 4 sebagai platform pemantauan dan Firebase sebagai *database* memberikan kemampuan yang sangat efisien dalam mengumpulkan, menyimpan, dan mengakses data deteksi kriminalitas. Dengan adanya ambang batas sebesar 80% untuk indikasi kriminal, sistem ini dapat secara akurat mengidentifikasi situasi yang memerlukan tindakan lebih lanjut dan merekam data ini dengan cepat dan andal. Data yang tersedia di Firebase dapat diakses melalui aplikasi *mobile* yang dapat digunakan oleh pihak berwenang untuk mengambil tindakan yang sesuai dalam menjaga keamanan dan penegakan hukum. Dengan integrasi ini, menunjukan bahwa sistem ini telah memberikan solusi yang efektif untuk pemantauan dan respons terhadap situasi kriminalitas secara *real-time*.

5. Pengujian Sistem

Proses pengujian sistem deteksi kriminal yang mencakup berbagai konteks dan kondisi berbeda sangat penting untuk memastikan keandalan dan keefektifan sistem. Langkah-langkah pengujian yang telah dilakukan antara lain pengujian dengan *background* gambar yang polos, pengujian dengan gambar yang memiliki *background*, pengujian secara *real-time* menggunakan kamera, dan pengujian output pada aplikasi *mobile* berbasis Android.

Pengujian awal dilakukan dengan menggunakan gambar yang polos, di mana objek kriminal ditampilkan tanpa adanya latar belakang yang kompleks. Hal ini digunakan untuk mengukur kemampuan dasar sistem dalam mendeteksi objek kriminal tanpa gangguan dari latar belakang. Sistem berhasil mendeteksi objek *violence* sebanyak 460 interasi dari 500 kali iterasi yang dilakukan atau sebesar 92% dan *robbery* terdeteksi sebesar 91% dari 500 epoch dalam pengujian awal tanpa latar belakang ini. Selanjutnya, pengujian dilakukan dengan menggunakan gambar yang memiliki latar belakang yang beragam dan kompleks. Pengujian ini membantu evaluasi kemampuan sistem untuk membedakan objek kriminal dalam konteks yang lebih nyata. Pada pengujian kedua, sistem berhasil mendeteksi objek *violence* 93% atau 465 epoch dari 500 iterasi dan objek *robbery* terdetaksi sebanyak 265 kali iterasi dari 500 iterasi atau sebesar 53%. Setelah terintegrasi dengan Raspberry Pi 4, sistem diuji secara *real-time* dengan menggunakan kamera. Hal ini memungkinkan pengujian dalam situasi yang lebih mendekati kondisi kehidupan nyata, seperti pengawasan keamanan di lokasi tertentu atau area publik. Sistem berhasil mendeteksi objek *violence* sebesar 91% atau 460 epoch dari 500 kali iterasi dan *robbery* sebanyak 415 kali iterasi dari 500 epoch yang dilakukan atau sebesar 83% pada pengujian secara *real-time*.



Gambar 5. Log aktivitas kriminal pada aplikasi mobile

Hasil pengujian terakhir ini menunjukan bahwa objek yang berhasil terdeteksi oleh sistem, dan jika indikasi tindakan kriminal terpenuhi dengan tingkat keyakinan yang memadai, maka data log aktivitas kriminal akan ditampilkan dalam aplikasi mobile seperti pada gambar 5 di atas. Pengujian yang komprehensif seperti ini membantu memvalidasi kinerja sistem dalam berbagai situasi dan kondisi. Hasil dari pengujian ini akan memberikan pemahaman yang lebih baik tentang sejauh mana sistem dapat digunakan secara efektif untuk mendeteksi tindakan kriminal dalam berbagai konteks yang berbeda. Selain itu, temuan dari pengujian dapat digunakan untuk perbaikan dan peningkatan sistem agar lebih andal dan akurat.

6. Pembahasan

Potensi khusus dari sistem deteksi kriminal yang telah dijelaskan sebelumnya antara lain respons cepat terhadap aktivitas kriminal, dimana sistem ini memberikan petugas keamanan alat yang dapat membantu mereka merespons dengan cepat terhadap situasi kriminal yang terdeteksi. Mereka dapat mengambil tindakan pencegahan atau menghubungi penegak hukum yang berwenang sesuai dengan informasi yang tersedia. Kemudian juga meningkatkan keamanan dan respons, yang berarti sistem ini dapat membantu meningkatkan tingkat keamanan di lokasi yang dipantau dan meningkatkan respons terhadap situasi berpotensi berbahaya. Ini dapat digunakan dalam berbagai konteks, seperti pemantauan area publik, keamanan perusahaan, atau pengawasan perbatasan.

Guna mencapai potensi khusus tersebut, pengembangan sistem deteksi kriminal memerlukan upaya lebih lanjut, termasuk perbaikan dataset yang lebih besar dan memiliki konteks background yang beragam. Beberapa langkah yang dapat diambil untuk meningkatkan sistem yaitu dengan pengumpulan dataset yang lebih besar, pengambilan dataset dari berbagai konteks dan latar belakang yang lebih padat, pelatihan model yang lebih lanjut, dan pengembangan antarmuka pengguna yang lebih baik.

Jumlah dataset yang lebih besar dengan variasi yang lebih tinggi dalam objek kriminal dan latar belakang akan membantu sistem memahami berbagai situasi dan kondisi dengan lebih baik. Data dari berbagai lokasi dan lingkungan juga dapat meningkatkan akurasi sistem dalam mendeteksi tindakan kriminal. Di samping itu, sistem deteksi kriminal harus mengumpulkan dataset dari berbagai konteks dan latar belakang yang lebih padat. Ini termasuk pengambilan data dari lingkungan perkotaan, pedesaan, dalam ruangan, luar ruangan, siang hari, malam hari, dan dalam cuaca berbeda. Dengan melakukan ini, sistem akan lebih adaptif terhadap berbagai situasi dan latar belakang yang mungkin dihadapi dalam kehidupan nyata. Dataset yang lebih beragam akan membantu melatih model untuk mengenali objek kriminal dengan lebih baik, terlepas dari kondisi atau konteksnya.

Dengan dataset yang jauh lebih besar, model dapat dilatih lebih lanjut untuk mengenali objek dan situasi yang lebih beragam. Ini dapat meningkatkan tingkat kepercayaan dan akurasi dalam mendeteksi aktivitas kriminal. Serta aplikasi mobile untuk petugas keamanan juga perlu terus diperbarui dan ditingkatkan agar dapat menyajikan informasi dengan lebih baik dan lebih cepat kepada petugas. Melalui langkah-langkah ini, sistem deteksi kriminal dapat mengoptimalkan potensi khususnya dalam memberikan respons cepat terhadap aktivitas

kriminal dan meningkatkan tingkat keamanan dan respons terhadap situasi berpotensi berbahaya.

4. KESIMPULAN

Sistem deteksi kriminal yang menjadi tujuan dari studi ini untuk meningkatkan keamanan dan mencegah terjadinya tindak kriminal di suatu wilayah atau tempat tertentu, telah dikembangkan dengan berbasis Internet of Things dan menggunakan teknologi YOLOv5. Melalui tahapan pengambilan dataset sejumlah 450 gambar, kemudian pelabelan dengan hasil 315 gambar digunakan sebagai *train-set*, 90 gambar menjadi *valid-set*, dan sisanya yaitu 45 gambar ditetapkan sebagai *test-set*. Tahapan *training dataset* diatur jumlah iterasi (*epoch*) sebanyak 500 kali sehingga menghasilkan model *training*. Setelah *training* data, tahapan studi ini dilanjutkan ke integrasi sistem dengan aplikasi *mobile*. Terakhir pada tahap pengujian sistem berhasil mendeteksi objek *violence* 92% dan *robbery* 91% dalam pengujian awal tanpa latar belakang. Pada pengujian kedua dengan latar belakang, sistem berhasil mendeteksi objek *violence* 93% dan *robbery* 53%. Sistem berhasil mendeteksi objek *violence* 91% dan *robbery* 83% pada pengujian secara *real-time*. Potensi khusus dan kontribusi dari sistem deteksi kriminal yang telah dijelaskan sebelumnya antara lain respons cepat dari pihak berwajib terhadap aktivitas kriminal, dimana sistem ini memberikan informasi mengenai tingkat akurasi yang baik dalam mendeteksi aktivitas kriminal, seperti kekerasan dan pencurian.

DAFTAR PUSTAKA

[1] R. Khairani and Y. Ariesa, "Analisis Faktor-Faktor Yang Mempengaruhi Tingkat Kriminalitas Sumatera Utara (Pendekatan Ekonomi)," *J. Kaji. Ekon. dan Kebijak. Publik*, vol. 4, no. 2, pp. 99–110, 2019.

[2] S. Rahmalia, Ariusni, and M. Triani, "Pengaruh Tingkat Pendidikan, Pengangguran, dan Kemiskinan Terhadap Kriminalitas di Indonesia," *J. Kaji. Ekon. dan Pembang.*, vol. 1, no. 1, pp. 21–36, 2019.

[3] R. I. Sari, "Hubungan Pengangguran, Pendidikan dan Distribusi Pendapatan terhadap Angka Kriminalitas di Sulawesi Selatan Menggunakan Analisis Regresi Data Panel," 2018, [Online]. Available: http://repositori.uin-alauddin.ac.id/12500/1/HUBUNGAN PENGANGGURAN%2C PENDIDIKAN DAN DISTRIBUSI PENDAPATAN TERHADAP ANGKA KRIMINALITAS DI SULAWESI SELATAN MENGGUNAKAN A~1.pdf.

[4] R. M. Sabiq and N. C. Apsari, "Dampak Pengangguran Terhadap Tindakan Kriminal Ditinjau Dari Perspektif Konflik," *J. Kolaborasi Resolusi Konflik*, vol. 3, no. 1, pp. 51–64, 2021, doi: 10.24198/jkrk.v3i1.31973.

[5] R. M. Sabiq and N. Nurwati, "Pengaruh Kepadatan Penduduk Terhadap Tindakan Kriminal," *J. Kolaborasi Resolusi Konflik*, vol. 3, no. 2, pp. 161–167, 2021, doi: 10.24198/jkrk.v3i2.35149.

[6] Badan Pusat Statistik, "Statistik Kriminal Tahun 2023," *Badan Pus. Stat.*, vol. 14, p. 209, 2023, [Online]. Available: https://www.bps.go.id/id/publication/2023/12/12/5edba2b0fe5429a0f232c736/statistik-kriminal-2023.html.

[7] Gega Ryani Cahya Kurnia B. P, "Peran Kamera Pengawas Closed-Circuit Television (CCTV) Dalam Kontra Terorisme," *J. Lemb. Ketahanan Nas. Republik Indones.*, vol. 9, no. 4, pp. 100–116, 2020.

[8] C. S. Sung and J. Y. Park, "Design of an intelligent video surveillance system for crime prevention: applying deep learning technology," *Multimed. Tools Appl.*, vol. 80, no. 26–27, pp. 34297–34309, 2021, doi: 10.1007/s11042-021-10809-z.

[9] V. C. Maha Vishnu, M. Rajalakshmi, and R. Nedunchezhian, "Intelligent traffic video surveillance and accident detection system with dynamic traffic signal control," *Cluster Comput.*, vol. 21, no. 1, pp. 135–147, 2018, doi: 10.1007/s10586-017-0974-5.

[10] J. Xu, "A deep learning approach to building an intelligent video surveillance system," *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5495–5515, 2021.

[11] A. Setiawan and A. Irma Purnamasari, "Pengembangan Passive Infrared Sensor (PIR) HC-SR501 dengan Microcontrollers ESP32-CAM Berbasiskan Internet of Things (IoT) dan Smart Home sebagai Deteksi Gerak untuk Keamanan Perumahan," *Prosisiding Semin. Nas. SISFOTEK (Sistem Inf. dan Teknol. Informasi)*, vol. 3, no. 1, pp. 148–154, 2019, [Online]. Available: http://seminar.iaii.or.id/index.php/SISFOTEK/article/view/118.

[12] J. P. Sagala, I. Candradewi, and A. Harjoko, "Penggunaan Deteksi Gerak untuk Pengurangan Ukuran Data Rekaman Video Kamera CCTV," *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 10, no. 1, p. 99, 2020, doi: 10.22146/ijeis.35983.

[13] S. Ahmed, M. T. Bhatti, M. G. Khan, B. Lövström, and M. Shahid, "Development and Optimization of Deep Learning Models for Weapon Detection in Surveillance Videos,"

Appl. Sci., vol. 12, no. 12, 2022, doi: 10.3390/app12125772.

[14] A. Castillo, S. Tabik, F. Pérez, R. Olmos, and F. Herrera, "Brightness guided preprocessing for automatic cold steel weapon detection in surveillance videos with deep learning," *Neurocomputing*, vol. 330, pp. 151–161, 2019, doi: 10.1016/j.neucom.2018.10.076.

[15] T. A. Kumar, R. Rajmohan, M. Pavithra, S. A. Ajagbe, R. Hodhod, and T. Gaber, "Automatic Face Mask Detection System in Public Transportation in Smart Cities Using IoT and Deep Learning," *Electron.*, vol. 11, no. 6, 2022, doi: 10.3390/electronics11060904.

[16] J. Ieamsaard, S. N. Charoensook, and S. Yammen, "Deep Learning-based Face Mask Detection Using YoloV5," *Proceeding 2021 9th Int. Electr. Eng. Congr. iEECON 2021*, pp. 428–431, 2021, doi: 10.1109/iEECON51072.2021.9440346.