Identifikasi *Source Image* Menggunakan Pendekatan *Forensic Similarity* pada *Image* Forensik

AHMAD RIDHA KELREY

18917103

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2022

Lembar Pengesahan Pembimbing

Identifikasi *Source Image* Menggunakan Pendekatan *Forensic Similarity* pada *Image Forensik*

Ahmad Ridha Kelrey
18917103

Yogyakarta, Juni 2022

Pembimbing

Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

Identifikasi Source Image Menggunakan Pendekatan Forensic Similarity pada Image Forensik

Ahmad Ridha Kelrey

18917103

Yogyakarta, Juni 2022

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom.
Ketua

Ahmad Luthfi, S.Kom., M.Kom. Ph.D.
Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

Abstrak

Identifikasi Source Image Menggunakan Pendekatan Forensic Similarity pada Image Forensik

Dengan perkembangan teknologi digital, gambar digital bisa didapat kapan dan dimana saja melalui kamera dan telepon genggam. Orang dapat memperoleh gambar dengan mudah dan dapat juga memanipulasi sumber informasi pada konten dan bahkan dapat melakukan manipulasi gambar. Sehingga perlu melakukan verifikasi sumber gambar yang merupakan pekerjaan utama di bidang image forensik. Identifikasi sumber kamera adalah proses menentukan perangkat kamera mana yang telah digunakan untuk mengambil gambar. Pendekatan Forensic Similarity yang berbasis Convolutional Neural Network menentukan jika dua patch gambar diambil oleh kamera yang berbeda atau dari kamera yang sama. Pendekatan ini berbeda dari identifikasi kamera pada umumnya karena tidak menentukan kamera yang tepat yang digunakan untuk menangkap salah satu patch. Kekuatan pendekatan ini adalah kemampuan untuk membandingkan kamera yang tidak digunakan untuk melatih sistem. Ini memungkinkan penyidik mempelajari informasi penting tentang gambar yang diambil dengan kamera apa pun, dan tidak dibatasi oleh kumpulan model kamera di database penyidik. Meskipun informasi model kamera, tanggal dan waktu, dan informasi lainnya dapat ditemukan di EXIF atau di header JPEG, secara umum tidak mungkin untuk menganggap informasi tersebut benar karena metadata gambar dapat dengan mudah dimodifikasi. Proses identifikasi kamera sumber menggunakan identifikasi pada gambar untuk mengetahui sumber kamera yang diperoleh dari gambar tersebut. Dengan menggunakan pendekatan forensic similarity dapat mendukung informasi pada metadata sehingga dapat menjamin keaslian dari informasi yang diperoleh.

Kata kunci

Image Forensik, *Forensic Similarity*, Identifikasi Source Model Camera, Metadata

Abstract

Identify Source Image Using Forensic Similarity Approach in Image Forensics

With the development of digital technology, digital images can be obtained anytime and anywhere through cameras and cell phones. People can get images easily and can also manipulate the sources of information in the content and can even manipulate images. So it is necessary to verify the source of the image which is the main job in the field of image forensics. Camera source identification is the process of determining which camera device was used to take the image. Forensic Similarity approach based on Convolutional Neural Network determines if two image patches are taken by different cameras or from the same camera. This approach differs from typical camera identification in that it does not specify the exact camera used to capture any of the patches. The strength of this approach is the ability to compare cameras that were not used to train the system. This allows investigators to learn important information about images taken with any camera, and is not limited by the set of camera models in the investigator database. Although camera model information, date and time, and other information can be found in the EXIF or in the JPEG header, it is generally impossible to assume the information is correct because image metadata can be easily modified. The source camera identification process uses identification on the image to find out the camera source obtained from the image. By using a forensic similarity approach, it can support information in metadata so that it can guarantee the authenticity of the information obtained.

Keywords

Image Forensic, Forensic Similarity, Source Camera Identification, Metadata

Pernyataan KeaslianTulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni 2022

Ahmad Ridha Kelrey, S.Kom.

Daftar Publikasi

Publikasi yang dihasilkan:

(Ahmad Ridha Kelrey, Yudi Prayudi, Erika Ramadhani, 2022), Identifikasi Source Image Menggunakan Pendekatan Forensic Similarity Pada Image Forensik).

Kontributor	Jenis Kontribusi
Ahmad Ridha Kelrey	Mendesain eksperimen (60%) Menulis *paper* (70%)
Yudi Prayudi	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)
Erika Ramadhani	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (15%)

Halaman Persembahan

Alhamdulillahi Robbil 'Alamin. Segala puji dan syukur atas kehadirat Allah *Subhana Wa Ta'ala* yang telah memberikan rahmat, ridho, dan karunia-Nya kepada saya. Shalawat serta salam kepada Nabi Muhammad *Shallallahu 'Alaihi Wasallam*, sebagai pembawa risalah Allah terakhir dan penyempurna seluruh risalah-Nya. Tesis ini kupersembahkan kepada:

1. **Allah SWT** yang telah memberiku nikmat iman dan islam, serta sang guru besarku **Rasulullah Muhammad SAW** yang mengajarkanku ilmu akan arti kehidupan.
2. **Kedua Orang tua** tersayang yang selalu mengiringi doa, motivasi, serta nasihat dalam hidupku. Tiada kata yang dapat ku tulis untuk menggambarkan segala pengorbanan dan kasih sayang kalian. Namun hanya doa yang dapat ku persembahkan semoga kasih sayang dan rahmat Allah SWT senantiasa tercurahkan.
3. **Dosen dan Seluruh pengurus Akademik MI UII** yang berjasa serta bersedia memberikan waktu dan ilmu pengetahuan selama menempuh masa studi magister.
4. **Teman, Sahabat MI UII 2018 khususnya Konsentrasi Forensika Digital** yang selalu memberikan semangat, motivasi, dan pengertian menempuh masa studi magister.
5. Teman-teman yang tidak dapat penulis sebutkan satu-persatu yang ikut mendukung penulis dalam penyusunan Laporan Tesis ini, maupun dalam menempuh masa studi magister.

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur penulis sampaikan kehadirat Allah SWT., Tuhan Yang Maha Pemurah lagi Maha Penyayang. Berkat rahmat, hidayah, dan inayah-Nya, akhirnya penulis dapat menyelesaikan laporan tesis yang berjudul "Identifikasi *Source Image* Menggunakan Pendekatan *Forensic Similarity* pada Image Forensik".

Tesis ini merupakan syarat wajib yang harus ditempuh dalam mencapai Magister Strata-2 pada Program Studi Magister Informatika. Penulisan laporan tesis ini terselesaikan karena bantuan dari berbagai pihak. Untuk itu, penulis menyampaikan terima kasih kepada semua pihak yang telah membantu penulis dalam menyelesaikan laporan tesis ini.

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Selaku Rektor Universitas Islam Indonesia.
2. Bapak Hari Purnomo, Prof., Dr., Ir., M.T., Selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Ibu Izzati Muhimmah, S.T., M.Sc., Ph.D., Selaku Ketua Program Studi Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Dr. Yudi Prayudi, S. Si., M. Kom., Selaku Dosen Pembimbing 1 yang berkenan membimbing dan mengarahkan penulis, sehingga Penelitian Tesis ini dapat selesai.
5. Ibu Erika Ramadhani, S.T., M.Eng., Selaku Dosen Pembimbing 2 yang berkenan membimbing dan mengarahkan penulis, sehingga Penelitian Tesis ini dapat selesai.
6. Semua pihak yang tidak dapat penulis sebutkan satu persatu, baik secara langsung maupun tidak langsung membantu dalam penulisan tesis ini.

Semoga atas bantuan dan kerja sama yang telah diberikan menjadi amal baik dan mendapat balasan dari Allah SWT. Penulis menyadari bahwa penelitian ini jauh dari sempurna, untuk itu diperlukan saran dan masukan demi sempurnanya penyusunan laporan tesis ini. Akhir kata, penulis berharap semoga laporan tesis ini dapat bermanfaat bagi semua yang membutuhkan.

Wassalamu'alaikum Wr. Wb

Yogyakarta, Juni 2022

Ahmad Ridha Kelrey

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

CCTV	- Closed Circuit Television
CFA	- Color Filter Array
CMOS	- Complementary metal–oxide–semiconductor
CNN	- Convolutional Neural Network
EXIF	- Exchangeable Image Format
JPG	- Joint Photographic Group
JPEG	- Joint Photographic Experts Group

BAB 1
Pendahuluan

1.1 Latar Belakang

Dengan perkembangan teknologi digital, gambar digital bisa didapat kapan dan di mana saja melalui berbagai kamera dan telepon genggam. Pada saat yang sama, teknologi forensik gambar digital telah mendapat perhatian cukup karena dapat digunakan untuk gambar identifikasi sumber, deteksi pemalsuan gambar, dan pelacakan riwayat operasi gambar (Xu, Wang, Zhou, Xi, & Wang, 2016). Gambar, tidak seperti teks, merupakan media komunikasi yang efektif dan alami bagi manusia, karena kedekatannya dan cara mudah untuk memahami isi gambar. Secara historis dan tradisional, ada kepercayaan pada integritas data visual, sehingga gambar yang dicetak di surat kabar secara umum diterima sebagai sertifikasi kebenaran berita, atau rekaman video CCTV diusulkan sebagai barang bukti di depan pengadilan. Dengan cepatnya penyebaran penggunaan perangkat yang memungkinkan akuisisi data visual, hampir setiap orang saat ini memiliki kemungkinan untuk merekam, menyimpan, dan berbagi gambar digital. Pada saat yang sama, ketersediaan perangkat lunak pengedit gambar membuat sangat mudah untuk mengubah konten gambar, atau membuat yang baru, sehingga kemungkinan merusak dan memalsukan konten visual tidak lagi terbatas pada para ahli. Akhirnya, perangkat lunak saat ini memungkinkan untuk membuat grafik komputer foto realistik yang menurut masyarakat tidak dapat dibedakan dari gambar fotografi (Piva, 2013). Tugas image forensik adalah untuk mengekspos jejak yang tersisa dalam konten multimedia dengan memanfaatkan pengetahuan yang ada tentang pencitraan digital. Kegiatan penelitian dalam domain ini dimulai beberapa tahun yang lalu dan meningkat pesat dalam beberapa waktu terakhir, sehingga perlunya tinjauan komprehensif tentang state of the art pada image forensik. Image forensik bertujuan untuk menemukan riwayat pemrosesan suatu konten. Asumsi dasarnya adalah bahwa setiap operasi yang telah diterapkan pada gambar akan meninggalkan jejak dalam statistik gambar. Sejauh jejak tersebut dapat dideteksi, mereka dapat digunakan sebagai bukti (Dang-Nguyen, Pasquini, Conotter, & Boato, 2015).

Orang dapat memperoleh gambar dengan mudah dan dapat juga memanipulasi sumber informasi pada konten dan bahkan dapat melakukan manipulasi gambar. Sehingga perlu melakukan verifikasi sumber dan keaslian gambar yang merupakan pekerjaan utama

di bidang forensik gambar. Sebagai salah satu bidang utama forensik gambar, identifikasi sumber kamera memiliki dua cabang. Salah satunya adalah mencocokkan gambar dengan satu kamera dan yang lainnya adalah mencocokkannya dengan model kamera tertentu. Proses akuisisi gambar melibatkan beberapa tahapan yang masing-masing dapat diimplementasikan secara berbeda di kamera yang berbeda (Wang, Yin, Tan, Li, & Li, 2018). Identifikasi kamera sumber adalah proses menentukan perangkat kamera mana yang telah digunakan untuk mengambil gambar. Ini sering digunakan dalam masalah keamanan dan hukum sebagai barang bukti digital. Identifikasi model kamera menggolongkan teknik identifikasi sumber forensik yang bertujuan untuk menentukan model kamera yang digunakan untuk memperoleh gambar yang asalnya tidak diketahui. Identifikasi model kamera berusaha menjawab pertanyaan (1) Dari model mana kamera yang (kemungkinan besar) mengambil gambar ini? atau (2) Apakah gambar ini diambil dengan kamera merek dan model tertentu (Kirchner & Gloe, 2015). Perangkat pencitraan meninggalkan beberapa jejak dalam suatu gambar selama proses pembuatannya. Jejak ini disebabkan oleh karakteristik perangkat fisik, karena beberapa karakteristik perangkat memiliki keunikan perangkat yang sulit dihilangkan. Kita dapat menggunakan karakteristik perangkat seperti sidik jari suatu perangkat. Saat ini, identifikasi sumber kamera digital dapat dibagi menjadi dua kategori: identifikasi sumber berdasarkan deteksi korelasi dan identifikasi sumber berdasarkan klasifikasi pola (Cai, Shao, Tomioka, Liu, & Li, 2019).

Pendekatan Forensic Similarity yang berbasis CNN menentukan jika dua patch gambar diambil oleh model kamera yang berbeda atau dari model kamera yang sama. Pendekatan ini berbeda dari identifikasi model kamera karena tidak menentukan model kamera yang tepat yang digunakan untuk menangkap salah satu patch. Kekuatan pendekatan ini adalah kemampuan untuk membandingkan model kamera yang tidak digunakan untuk melatih sistem (Mayer & Stamm, 2019).

Tantangan untuk memverifikasi keaslian suatu gambar dapat diatasi dari berbagai perspektif. Salah satunya didekati dengan menjawab pertanyaan berikut: apakah mungkin untuk mengetahui model kamera yang digunakan untuk mengambil gambar meskipun model kamera, tanggal dan waktu, dan informasi lainnya dapat ditemukan di EXIF atau di header JPEG, secara umum tidak mungkin untuk menganggap informasi tersebut dapat diandalkan dan sah karena metadata gambar dapat dengan mudah dimodifikasi (Camacho & Wang, 2021). Metadata adalah data tentang data. Metadata adalah data yang memberikan beberapa informasi penting tentang data yang dapat digunakan untuk menganalisis bukti, kepemilikan, dan kualitas data tersebut. Metadata pada gambar dapat terdiri dari dua jenis yaitu, metadata

yang dihasilkan secara otomatis dan metadata yang disisipkan atau dimanipulasi oleh manusia. Metadata yang dihasilkan secara otomatis yang memberikan informasi tentang ID perangkat, perangkat lunak yang digunakan, tanggal dan waktu pembuatan, dll. (P, Srikanth, & Sailaja, 2016). Proses investigasi dapat menggunakan metadata dari header gambar, meskipun kita ketahui bahwa metadata dapat dengan relatif mudah dimodifikasi. Oleh karena itu, metadata gambar sering diabaikan karena dianggap hampir tidak memiliki nilai pembuktian (Mullan, Riess, & Freiling, 2019).

Pada penelitian ini akan dilakukan proses identifikasi sumber kamera menggunakan pendekatan forensic similarity dengan melakukan identifikasi pada gambar untuk mengetahui sumber kamera yang diperoleh dari gambar tersebut. Dengan menggunakan pendekatan forensic similarity dapat mendukung informasi pada metadata sehingga dapat menjamin keaslian dari informasi yang diperoleh.

1.2 Rumusan Masalah

Rumusan masalah berikut akan dijawab oleh penelitian ini:

1. Bagaimana melakukan identifikasi *source image* pada gambar menggunakan pendekatan *forensic similarity*.
2. Bagaimana menggunakan pendekatan *forensic similarity* untuk mendukung informasi perangkat yang terdapat pada metadata gambar tersebut.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya menerapkan pendekatan forensic similarity untuk mencari kemiripan pada gambar berdasarkan perangkat dari gambar itu diambil.
2. File yang diuji dan dianalisis adalah file gambar yang diperoleh dari perangkat asli bukan dari media sosial.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Untuk identifikasi *source image* pada gambar menggunakan pendekatan *forensic similarity*.
2. Untuk mengetahui bagaimana pendekatan forensic similarity bisa mendukung informasi pada metadata gambar asli atau metadata gambar yang telah dimodifikasi atau dihapus.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi dalam kehidupan manusia dan dapat diterapkan di dunia nyata, khususnya membantu pembuktian barang bukti digital di persidangan. Adapun manfaat penelitian ini antara lain:

1. Mengetahui metode image forensik yang relevan untuk melakukan perbandingan dan analisis kemiripan sumber perangkat pada gambar yang menjadi barang bukti.
2. Membantu penegak hukum untuk mengetahui keaslian pada gambar tersebut diambil menggunakan perangkat apa yang bisa dipertanggungjawabkan.

1.6 Review Penelitian

Perkembangan penelitian membuat banyak para peneliti melakukan beragam penelitian, penelitian terkait multimedia forensik atau identifikasi kamera sumber tentunya bukan menjadi sebuah hal yang baru. Penelitian-penelitian tersebut, tentu menjadi sebuah sumber referensi untuk mendapatkan informasi yang dapat dijadikan sebagai acuan penelitian selanjutnya.

Menurut (Mayer & Stamm, 2019) Pada penelitian mereka mengusulkan teknik forensik gambar digital baru yang disebut Forensic Similarity untuk menentukan apakah dua Image Patch mengandung jejak forensik yang sama atau berbeda. Manfaat utama dari pendekatan ini adalah pengetahuan sebelumnya, misalnya sampel pelatihan, dari jejak forensik tidak diperlukan untuk membuat keputusan kesamaan forensik di atasnya. Untuk melakukan ini, mereka mengusulkan dua bagian sistem deep learning yang terdiri dari Feature Extractor berbasis Convolutional Neural Network (CNN) dan jaringan saraf tiga lapis, yang disebut jaringan kesamaan, yang memetakan image patch ke skor yang menunjukkan apakah mereka mengandung jejak forensik yang sama atau berbeda.

Menurut (Bondi et al., 2015) Pada penelitian mereka mendeteksi model kamera yang digunakan untuk memotret gambar yang memungkinkan untuk memecahkan masalah forensik, dari pelanggaran hak cipta hingga atribut kepemilikan. Untuk alasan ini, komunitas forensik telah mengembangkan seperangkat algoritma identifikasi model kamera yang memanfaatkan jejak karakteristik yang tertinggal pada gambar yang diperoleh oleh pipeline pemrosesan yang spesifik dari setiap model kamera. Pada penelitian ini peneliti menyelidiki pendekatan baru untuk memecahkan masalah identifikasi model kamera. Mereka mengusulkan algoritma data-driven berdasarkan convolutional neural network, yang mempelajari fitur yang mencirikan setiap model kamera langsung dari gambar yang diperoleh. Hasil pada set data yang terkenal dari 18 model kamera menunjukkan bahwa: (1)

metode yang diusulkan mengungguli algoritme mutakhir dalam klasifikasi image patch berwarna 64x64; (2) fitur yang dipelajari oleh jaringan yang diusulkan ke model kamera yang tidak pernah digunakan untuk pelatihan.

Menurut (Cai et al., 2019) Pada penelitian mereka mengusulkan pendekatan klasifikasi model berbasis CNN yang menggunakan Frequency Domain Feature dari noise gambar yang diekstraksi sebagai input. Mereka mengevaluasi efisiensi penggunaan fitur domain frekuensi secara efektif mengklasifikasikan model kamera. Hasil menunjukkan bahwa fitur dalam domain frekuensi cocok untuk klasifikasi model berbasis CNN. Gambar penuh diklasifikasikan menggunakan voting mayoritas patch gambar, dan akurasi rata-rata mencapai 100% untuk 12 model dan 99,32% untuk 14 model. Selain itu, peneliti mencapai akurasi 100% untuk klasifikasi 10 merek. Pendekatan yang peneliti usulkan efektif tidak hanya untuk klasifikasi model tetapi juga untuk klasifikasi merek. Peneliti mengabaikan informasi fase dan hanya menggunakan informasi magnitudo dari spektrum Fourier. Dari hasil percobaan, peneliti dapat melihat bahwa magnitude memiliki informasi yang signifikan untuk klasifikasi model kamera.

Menurut (Tuama, Comby, & Chaumont, 2016) Pada penelitian mereka mengevaluasi efisiensi penggunaan CNN untuk identifikasi model kamera sumber berdasarkan deep learning dan convolutional neural network. Mereka mencoba jaringan kecil dengan menyetel model AlexNet. Namun demikian, jaringan kecil ini sedikit kurang efisien (1% hingga 3%) daripada model GoogleNet. Hasil yang bervariasi dengan dua filter preprocessing yang berbeda menunjukkan peran penting yang dimainkan preprocessing dalam akurasi klasifikasi keseluruhan. Skalabilitas juga telah dievaluasi dan peningkatan jumlah model mengurangi keakuratan tidak terlalu drastis.

Menurut (Huang et al., 2018) Penelitian ini mengusulkan deep convolutional neural network baru yang melibatkan tiga lapisan convolutional, dua lapisan yang sepenuhnya terhubung dan classifier Softmax untuk mengidentifikasi kamera sumber gambar. Untuk proses pelatihan, mereka menerapkan berbagai kombinasi ukuran mini-batch, max-epoch, dan basic-learning-rate dan akhirnya mencapai kinerja pelatihan dan pengujian terbaik dengan serangkaian parameter pelatihan. Metode yang diusulkan memiliki keuntungan sebagai berikut untuk mengidentifikasi kamera sumber gambar: (1) lapisan input dapat menerima image patch berukuran kecil 36x36x3, menyelesaikan masalah kurangnya gambar sampel yang cukup dalam kasus forensik melalui pemotongan gambar asli ke memperoleh data pelatihan yang memadai; (2) dibandingkan dengan beberapa pekerjaan yang ada, jaringan yang diusulkan lebih dalam konvolusi dengan lapisan yang terhubung sepenuhnya

dihapus, yang ditunjukkan untuk meningkatkan representasi dan efisiensi. Hasil eksperimen mendukung kesimpulan bahwa metode yang diusulkan memang dapat mencapai kinerja yang lebih baik.

Tabel 1.1 Rangkuman Review Penelitian

Judul/ Peneliti	**Tujuan**	**Metode/ Pendekatan**	**Hasil**
Forensic Similarity for Digital Images (Mayer & Stamm, 2019)	Mengusulkan teknik forensik gambar digital baru yang disebut *Forensic Similarity* untuk menentukan apakah dua *Image Patch* mengandung jejak forensik yang sama atau berbeda	*CNN-based Feature Extractor* dan *Three-Layer Neural Network*	Penggabungan *Feature Extractor* berbasis *Convolutional Neural Network* (CNN) dan *Three-Layer Neural Network* memetakan *image patch* ke skor yang menunjukkan apakah mereka mengandung jejak forensik yang sama atau berbeda
First Steps Toward Camera Model Identification with (Bondi et al., 2015)	Mengusulkan pendekatan baru untuk memecahkan masalah identifikasi model kamera. Mereka mengusulkan algoritma *data-driven* berdasarkan	*Data-Driven* berbasis *Convolutional Neural Network*	(1) metode yang diusulkan mengungguli algoritme mutakhir dalam klasifikasi *image patch* berwarna 64x64; (2) fitur yang dipelajari oleh jaringan yang diusulkan ke model kamera yang tidak pernah digunakan untuk pelatihan.

	convolutional neural network		
CNN-based Camera Model Identification Using Image Noise in Frequency Domain (Cai et al., 2019)	Mengusulkan pendekatan klasifikasi model berbasis CNN yang menggunakan *Frequency Domain Feature* dari *noise* gambar yang diekstraksi sebagai input	*Convolutional Neural Network (CNN)* dan *AlexNet*	Hasil yang bervariasi dengan dua filter *preprocessing* yang berbeda menunjukkan peran penting yang dimainkan *preprocessing* dalam akurasi klasifikasi keseluruhan
Camera Model Identification With The Use of Deep Convolutional Neural Networks (Tuama et al., 2016)	Mengevaluasi efisiensi penggunaan CNN untuk identifikasi model kamera sumber berdasarkan *deep learning* dan *convolutional neural network*	*Deep-Learning dan Convolutional Neural Network*	Hasil yang bervariasi dengan dua filter *preprocessing* yang berbeda menunjukkan peran penting yang dimainkan *preprocessing* dalam akurasi klasifikasi keseluruhan.

Identification of The Source Camera of Images based on Convolutional Neural Network (Huang et al., 2018)	Mengusulkan *deep convolutional neural network* baru yang melibatkan tiga lapisan convolutional, dua lapisan yang sepenuhnya terhubung dan classifier *Softmax* untuk mengidentifikasi kamera sumber gambar	*Deep Convolutional Neural Network*	Hasil eksperimen mendukung kesimpulan bahwa metode yang diusulkan memang dapat mencapai kinerja yang lebih baik

1.7 Metode Penelitian

Penelitian ini perlu disusun langkah-langkah penyelesaian secara sistematik, adapun sistematika metodologi yang digunakan pada penelitian ini adalah sebagai berikut:

1. Tinjauan Pustaka

Tahap tinjauan pustaka dilakukan guna mencari bahan materi secara teori dan literatur dari penelitian-penelitian terdahulu, sehingga penelitian ini tidak terjadi perulangan pembahasan, dan menjadikan penelitian yang efektif ataupun bernilai.

2. Teknik Pengambilan Sampel Data

Selanjutnya dari berbagai penelitian yang telah ada dirumuskan hal-hal yang penting pada image forensik. Cara pengambilan sampel data gambar sesuai dengan prosedur dan parameter yang ada, sehingga memperoleh pemahaman yang komprehensif mengenai metode yang diangkat.

3. Implementasi Metode

Indikator dan parameter yang ditemukan dilakukan uji coba perumusan perbandingan dari masing-masing komponen yang telah ditentukan.

4. Analisis Data

Hasil dari implementasi metode tersebut akan dianalisis dan diolah sehingga menghasilkan nilai keakuratan dari implementasi metode tersebut.

5. Laporan

Semua kegiatan yang dilakukan dalam penelitian ini dibuat laporan dan didokumentasi dari kesimpulan analisis, baik kelebihan atau kekurangan metode yang digunakan. Sehingga bisa digunakan sebagai karya ilmiah untuk dijadikan bahan acuan dan referensi penelitian berikutnya.

1.8 Sistematika Penelitian

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas, di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang teori-teori dari berbagai bahan referensi yang terkait guna memecahkan masalah dalam penelitian ini.

BAB III METODOLOGI PENELITIAN

Pada bab ini membahas tentang langkah-langkah atau prosedur penelitian, sehingga mampu menyelesaikan masalah secara sistematik.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis, dan evaluasi dari penelitian yang diangkat.

BAB V PENUTUP

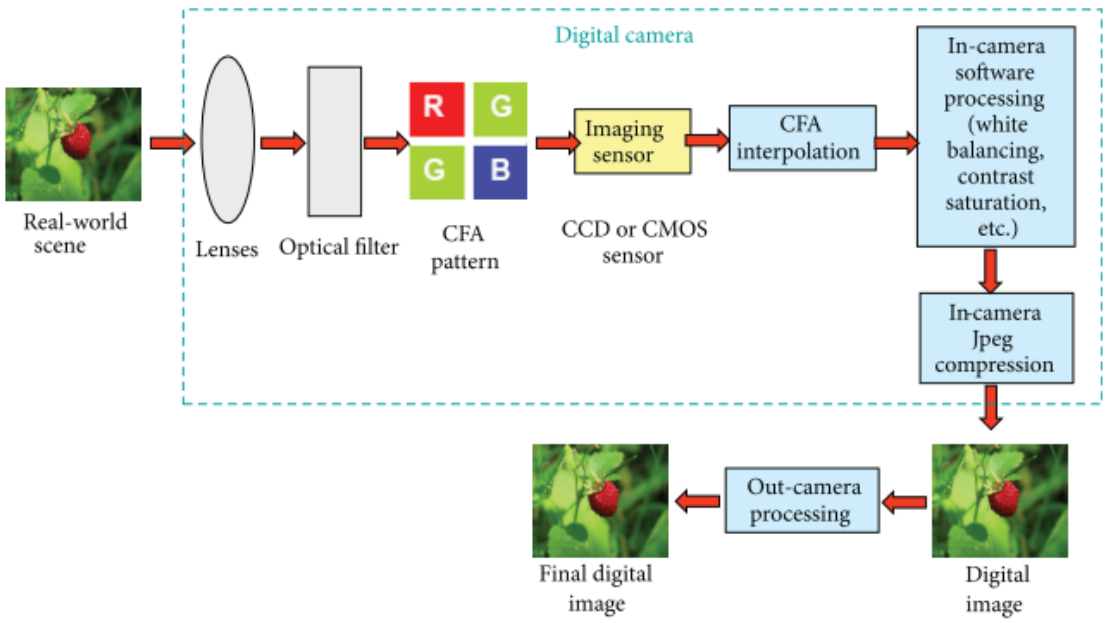
Bab ini merupakan bab terakhir yang memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan.

BAB 2

Tinjauan Pustaka

2.1 Gambar

Gambar, tidak seperti teks, merupakan media komunikasi yang efektif dan alami bagi manusia, karena kedekatannya dan cara mudah untuk memahami isi gambar. Secara historis dan tradisional, ada kepercayaan pada integritas data visual, sehingga gambar yang dicetak di surat kabar secara umum diterima sebagai sertifikasi kebenaran berita, atau rekaman video CCTV diusulkan sebagai barang bukti di depan pengadilan. Dengan cepatnya penyebaran penggunaan perangkat murah dan mudah yang memungkinkan akuisisi data visual, hampir setiap orang saat ini memiliki kemungkinan untuk merekam, menyimpan, dan berbagi gambar digital. Pada saat yang sama, ketersediaan perangkat lunak pengedit gambar membuat sangat mudah untuk mengubah konten gambar, atau membuat yang baru, sehingga kemungkinan merusak dan memalsukan konten visual tidak lagi terbatas pada para ahli. Akhirnya, perangkat lunak saat ini memungkinkan untuk membuat grafik komputer foto realistik yang menurut masyarakat tidak dapat dibedakan dari gambar fotografi atau juga menghasilkan konten visual yang dihasilkan secara *hybrid*.



Gambar 2.1 Digital Image Life Cycle

Seperti yang ditunjukkan pada Gambar 2.1, sejarah gambar digital dapat direpresentasikan sebagai komposisi dari beberapa langkah, dikumpulkan ke dalam tiga fase utama: *acquisition*, *coding*, dan *editing*. Selama akuisisi, cahaya yang datang dari *real scene* yang dibingkai oleh kamera digital difokuskan oleh lensa pada sensor kamera (CCD atau CMOS), di mana sinyal gambar digital dihasilkan. Namun, sebelum mencapai sensor, cahaya biasanya disaring oleh CFA (*Color Filter Array*), lapisan tipis pada sensor yang secara selektif memungkinkan komponen cahaya tertentu melewatinya ke sensor. Dalam praktiknya, untuk setiap piksel, hanya satu warna utama tertentu (Merah, Hijau, atau Biru) yang dikumpulkan. Keluaran sensor secara berurutan diinterpolasi untuk mendapatkan ketiga warna utama untuk setiap piksel, melalui proses yang disebut *demosaicing* untuk mendapatkan citra warna digital. Sinyal yang diperoleh mengalami pemrosesan tambahan dalam kamera yang dapat mencakup *white balancing*, *color processing*, *image sharpening*, *contrast enhancement*, dan *gamma correction*.

Dengan pengkodean, sinyal yang diproses disimpan ke memori kamera untuk menghemat penyimpanan. Di sebagian besar kamera, gambar dikompresi secara *lossy* dan untuk perangkat komersial, format JPEG biasanya lebih disukai. Akhirnya, gambar yang dihasilkan dapat diproses lebih lanjut, misalnya, untuk meningkatkan atau memodifikasi kontennya. Pengeditan gambar apa pun dapat diterapkan pada gambar selama masa pakainya, yang paling sering digunakan adalah transformasi geometris (*rotation*, *scaling*, dll.), *blurring*, *sharpening*, *contrast adjustment*, *image splicing* (komposisi dari gambar menggunakan bagian dari satu atau lebih bagian gambar), dan *cloning* (atau *copy-move*, replikasi bagian dari gambar yang sama). Terakhir, setelah diedit, seringkali gambar disimpan dalam format JPEG, sehingga akan terjadi kompresi ulang (Piva, 2013).

2.2 Digital Forensik

Forensik secara umum adalah suatu proses ilmiah untuk mengumpulkan, menganalisis dan menyajikan bukti pada pengadilan. Pada umumnya, sebuah tahap forensik dilakukan dengan asumsi bahwa data-data yang telah dikumpulkan akan digunakan sebagai bukti di pengadilan. Oleh karena itu, setelah pengumpulan barang bukti, para praktisi forensik menjaga dan mengontrol bukti tersebut untuk mencegah terjadinya modifikasi (Firdaus, 2016).

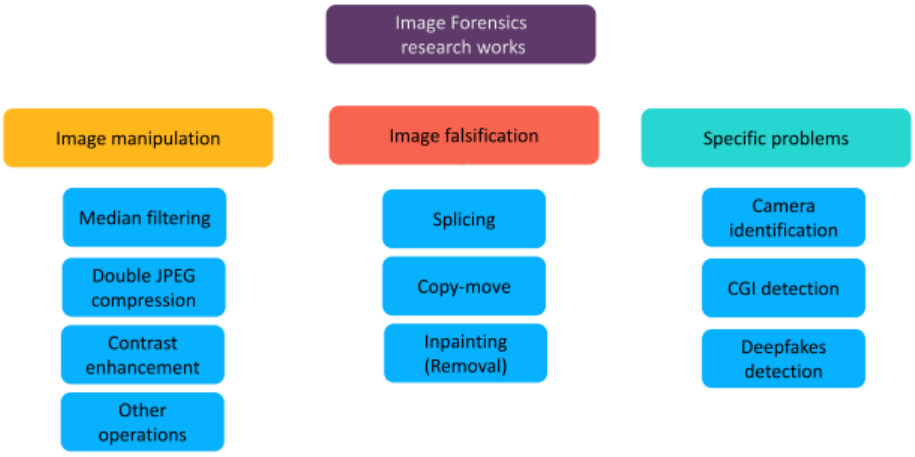
Forensik digital merupakan bagian dari ilmu forensik yang melingkup penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Sebagai ilmu yang masih baru, masih dibutuhkan pemahaman dan kemampuan untuk menguasai disiplin ilmu

tersebut. Penguasaan ilmu ini tidak hanya ditujukan pada kemampuan teknis semata tetapi juga terkait bidang lain seperti hukum (Rahardjo, 2013).

2.3 Image Forensik

Forensik multimedia merupakan turunan dari ilmu forensik klasik yang mempelajari penggunaan metode ilmiah untuk mendapatkan fakta pembuktian dari bukti fisik atau digital. Tugas alat forensik multimedia adalah untuk mengekspos jejak yang tersisa dalam konten multimedia dengan memanfaatkan pengetahuan yang ada tentang pencitraan digital dan dalam penelitian keamanan multimedia. Kegiatan penelitian dalam domain ini dimulai beberapa tahun yang lalu dan meningkat pesat dalam beberapa waktu terakhir, sehingga perlunya tinjauan komprehensif tentang *state of the art* pada forensik citra digital untuk memungkinkan orang baru masuk ke bidang ini.

Forensik citra digital bertujuan untuk menemukan riwayat pemrosesan suatu konten. Asumsi dasarnya adalah bahwa setiap operasi yang telah diterapkan pada gambar akan meninggalkan jejak halus dalam statistik gambar. Sejauh jejak tersebut dapat dideteksi, mereka dapat digunakan sebagai bukti pemalsuan gambar. (Dang-Nguyen et al., 2015).



Gambar 2.2 Diagram klasifikasi untuk karya forensik gambar berbasis deep-learning.

Image forensik diklasifikasikan ke dalam tiga kelompok besar: deteksi manipulasi gambar (yaitu, operasi pemrosesan gambar seperti *median filtering* dan *contrast enhancement*), deteksi pemalsuan gambar yang dengan sengaja mengubah makna semantik gambar (misalnya *copy-move*, *splicing* dan *inpainting*) dan masalah forensik spesifik lainnya (Camacho & Wang, 2021).

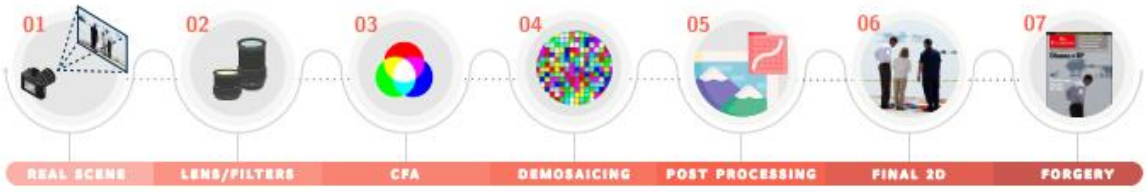
2.3.1 Manipulation Detection

Manipulasi gambar sebagai operasi rutin yang memodifikasi atau meningkatkan gambar digital dengan pemrosesan gambar dasar seperti *median filtering*, JPEG *compression*, atau *contrast enhancement*. Operasi ini dapat digunakan untuk meningkatkan kualitas visual dari gambar yang diubah atau untuk menyembunyikan jejak operasi pemalsuan yang mungkin meninggalkan sidik jari yang jelas jika digunakan sendiri.

2.3.2 *Falsification Detection*

Image falsification merupakan pembuatan konten palsu di beberapa bagian gambar untuk menipu manusia tentang fakta yang terjadi di masa lalu. Berbeda dengan manipulasi gambar biasa, *image falsification* dilakukan dengan sengaja untuk mengubah makna semantik gambar, seringkali dengan menyisipkan atau menghapus konten tertentu. Teknik pemalsuan gambar yang paling umum dapat dibagi menjadi tiga kategori besar: *copy-move forgery* di mana satu bagian dari gambar disalin dan ditempelkan ke dalam gambar yang sama dengan bagian palsu; *splicing forgery* di mana wilayah yang dirusak dalam gambar berasal dari gambar yang berbeda; dan *inpainting forgery* yang kadang-kadang dianggap sebagai subkelompok *copy-move* dengan perbedaan bahwa daerah palsu dalam *inpainting forgery* sering dibangun dengan menggunakan dan menggabungkan bagian kecil di lokasi yang berbeda dari gambar yang sama. Perlu disebutkan bahwa teknik *inpainting* secara tradisional digunakan untuk merekonstruksi bagian gambar yang hilang atau rusak dan bahwa pemalsuan lukisan sering diterapkan untuk melakukan penghapusan objek dalam gambar .

2.3.3 Camera Identification



Gambar 2.3 Ilustrasi jalur dari *image acquisition* dan *forgery creation*.

Proses perolehan gambar ditunjukkan pada Gambar 2.4. Pertama, sinar cahaya diarahkan oleh lensa, kemudian filter yang berbeda seperti *anti-aliasing* dapat diterapkan sebelum *Color Filter Array* (CFA) membagi cahaya menjadi merah (R), komponen hijau (G) dan biru (B) per piksel. Langkah *demosaicing* dilakukan setelahnya untuk merekonstruksi

seluruh warna dari sampel *input* yang diambil oleh langkah sebelumnya. Tergantung pada model kamera dan perangkat lunak, beberapa operasi pasca-pemrosesan seperti *white balancing*, *gamma correction* dan JPEG *compression* dapat dilakukan. Langkah-langkah pasca-pemrosesan ini berkontribusi sebagai petunjuk penting untuk bidang image forensik. Ketika gambar keluaran akhir kamera dipalsukan untuk membuat pemalsuan, jejak tambahan yang unik untuk setiap pemalsuan biasanya tertinggal.

2.4 Source Model Camera

Identifikasi model kamera menggolongkan teknik identifikasi sumber forensik yang bertujuan untuk menentukan model kamera yang digunakan untuk memperoleh gambar yang asalnya tidak diketahui. Identifikasi model kamera berusaha menjawab pertanyaan

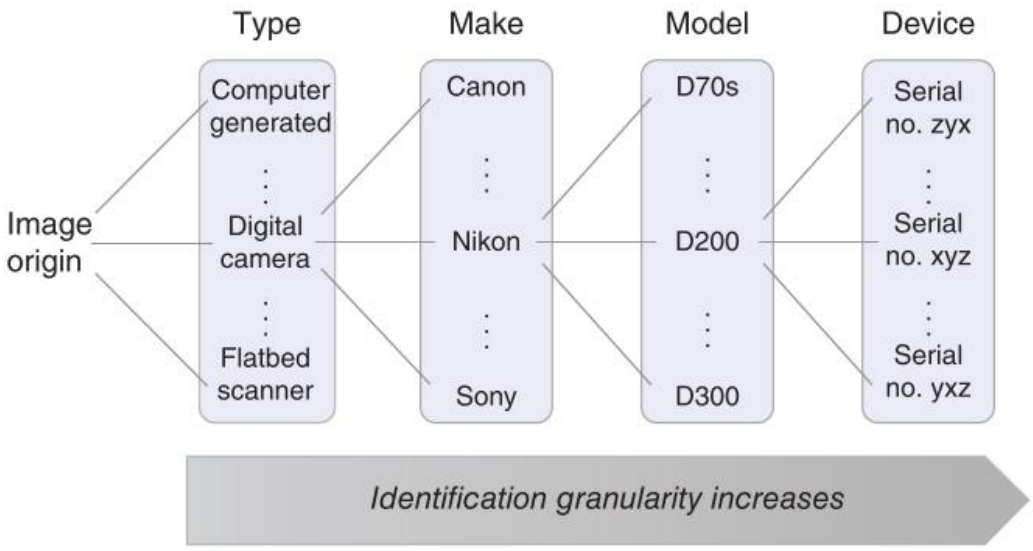
- 'Dari model mana kamera yang (kemungkinan besar) mengambil gambar ini?', atau
- 'Apakah gambar ini diambil dengan kamera merek dan model tertentu?',

Jika keyakinan sebelumnya berlaku. Premis identifikasi model kamera adalah bahwa gambar yang diperoleh dengan model kamera yang sama memiliki karakteristik yang sama, yang dapat dimanfaatkan untuk inferensi tentang sumber gambar. Produsen kamera bebas untuk menyempurnakan model mereka untuk menciptakan gambar yang bagus secara visual sesuai dengan preferensi mereka. Akibatnya, sejumlah besar varian berbeda dari komponen internal kamera, algoritma pemrosesan, dan kombinasinya menghasilkan gambar yang bervariasi di berbagai karakteristik gambar model-spesifik yang berbeda. Setiap gambar diperoleh dengan model kamera yang berbeda, menunjukkan bahwa perbedaan besar seringkali sudah terlihat dari inspeksi visual komparatif.

Identifikasi sumber forensik menghubungkan konten multimedia ke kelas dari perangkat akuisisi tertentu. Asumsi utama dari identifikasi sumber forensik adalah bahwa perangkat akuisisi meninggalkan jejak pada konten yang diperoleh, dan contoh dari jejak ini khusus untuk kelas dari perangkat masing-masing. Identifikasi sumber bekerja dengan mengekstraksi karakteristik akuisisi dari konten asal yang tidak diketahui dan membandingkannya dengan database referensi dari karakteristik yang diketahui. Data referensi dikompilasi dari konten berlabel dari perangkat akuisisi yang berpotensi relevan dalam fase pelatihan. Hal ini membuat identifikasi sumber menjadi masalah klasifikasi yang khas, dengan ruang kelas yang ditentukan untuk mewakili contoh karakteristik akuisisi yang berbeda (Böhme & Kirchner, 2013).

Secara intuitif, identifikasi sumber forensik harus berusaha untuk mengidentifikasi perangkat akuisisi yang digunakan untuk membuat konten yang dipertanyakan. Namun tidak selalu mungkin (atau diinginkan sejak awal) karena alasan praktis untuk bekerja pada tingkat *granularitas* yang tinggi ini. Mengkompilasi contoh karakteristik untuk *database* referensi memerlukan akses terkontrol ke konten yang diperoleh dengan perangkat kandidat masing-masing. Ini umumnya merupakan tugas yang memakan banyak sumber daya dan waktu. Pra-klasifikasi dengan perincian yang lebih rendah dapat membantu memilih subset perangkat akuisisi yang relevan untuk menjalankan algoritme identifikasi yang lebih bertarget di tahap berikutnya. Dalam kerja kasus nyata, kami mungkin juga menghadapi situasi di mana tidak ada konten tambahan dari perangkat akuisisi yang sebenarnya tersedia. Maka berguna untuk mempersempit sumber ke kelompok perangkat tertentu setidaknya. Untuk tujuan ini, biasanya cukup untuk memiliki akses ke perwakilan lain dari kelas perangkat yang sama.

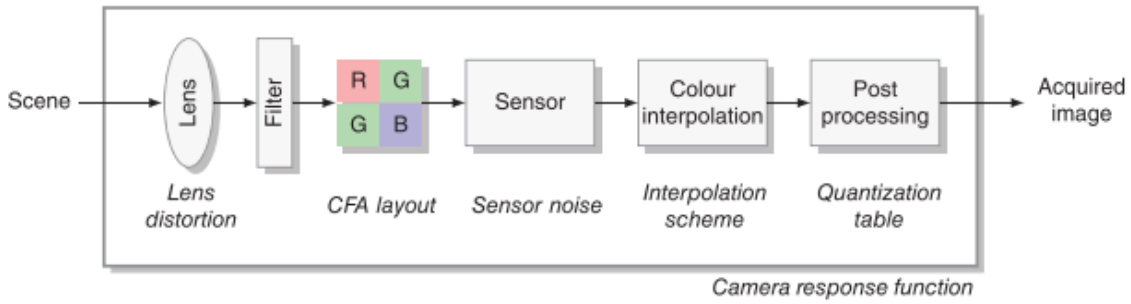
Tergantung pada kasus spesifik dan informasi referensi yang tersedia, identifikasi sumber forensik dapat didekati pada berbagai tingkat perincian identifikasi. Gambar 2.2 sebagai contoh menggambarkan analisis citra digital bahwa kita dapat membedakan antara metode untuk menentukan jenis perangkat akuisisi, merek atau modelnya, dan pada akhirnya juga perangkat itu sendiri.



Gambar 2.4 Tingkat *granularitas* dalam identifikasi sumber forensik

Perangkat akuisisi dan/atau metode akuisisi yang ditumpuk secara vertikal mengacu pada kemungkinan ruang kelas dari masing-masing tingkat perincian yang diatur secara horizontal. *Granularitas* meningkat dari kiri ke kanan: pada tingkat terendah memisahkan antara materi yang dipindai dan difoto, sedangkan identifikasi tingkat perangkat bertujuan

untuk membedakan kamera digital individu (atau *scanner*, dll.). Tingkat menengah sewenang-wenang dapat dibayangkan, misalnya untuk membedakan kamera *point-and-shoot* tingkat konsumen dari kamera DSLR profesional.



Gambar 2.5 Jalur pemrosesan kamera digital.

2.5 Metadata

Informasi elektronik sering kali berisi *metadata* yang tidak dapat dilihat saat melihat informasi menggunakan aplikasi dan alat yang secara konvensional terkait dengan jenis file. Metadata dapat, bagaimanapun, memberikan banyak informasi kepada penyelidik digital, juga, dapat digunakan untuk memberatkan (atau membebaskan) penulis, resensi, pemilik atau penerbit dokumen file.

Metadata dapat memberikan penyelidik dengan kekayaan informasi tentang file yang sedang diselidiki. Selanjutnya, penyidik forensik dapat menggunakan metadata untuk memperoleh informasi, misalnya, pembuat file, tanggal dan waktu pembuatan, berapa kali file telah dimodifikasi, termasuk kapan modifikasi dilakukan. Metadata Sistem File yang termasuk dalam kategori metadata sistem file adalah informasi tentang ukuran file, unit data spesifik yang dialokasikan dan akses ke cap tanggal atau waktu di dalam file. Metadata terkandung dalam file media seperti format pertukaran grafik (GIF), JPEG, dan dalam musik: MP3 dan AAC dan format file gambar yang ditandai. Dengan demikian, metadata dapat bermanfaat dalam penyelesaian sengketa hukum, karena dapat digunakan sebagai alat bukti untuk membuktikan atau menyanggah alat bukti lain yang diajukan dalam suatu perkara di pengadilan. Selain itu, metadata dapat disimpan di berbagai situs di dalam file. Penyelidik dapat mengumpulkan informasi dari metadata ini yang berhubungan dengan kepemilikan dan pemilik potensial (Alanazi, Lebh, & Jones, 2015). Metadata dapat menghasilkan bukti yang tidak selalu mudah terlihat dan penyidik harus memastikan pengumpulan data tersebut dan validasinya untuk presentasi di pengadilan. Praktisi hukum

yang menangani kasus-kasus yang melibatkan metadata harus diberi tahu tentang sifat dan nilai metadata untuk membantu proses penuntutan.

2.6 Pendekatan Forensic Similarity

Pendekatan forensik multimedia sebelumnya untuk gambar digital telah berfokus pada mengidentifikasi atau mengklasifikasikan jejak forensik tertentu (misalnya model kamera sumber, riwayat pemrosesan) dalam gambar atau patch gambar. Pendekatan ini mempunyai kelebihan utama yaitu 1) sampel pelatihan dari jejak tertentu diperlukan untuk mengidentifikasinya, dan 2) tidak semua analisis forensik memerlukan identifikasi jejak. Misalnya, untuk mengekspos pemalsuan penyambungan, cukup untuk mengidentifikasi bahwa gambar yang dipalsukan hanyalah konten komposit dari sumber yang berbeda, tanpa perlu mengidentifikasi sumber tersebut secara eksplisit. Forensic similarity adalah pendekatan yang menentukan apakah dua patch gambar memiliki jejak forensik yang sama atau berbeda. Tidak seperti pendekatan forensik sebelumnya, itu tidak mengidentifikasi jejak tertentu, tetapi masih memberikan informasi forensik penting kepada penyidik. Manfaat utama dari jenis pendekatan ini adalah dapat diimplementasikan secara praktis dalam skenario open-set. Artinya, sistem berbasis kesamaan forensik tidak secara inheren memerlukan sampel pelatihan dari jejak forensik untuk membuat keputusan kesamaan forensik.

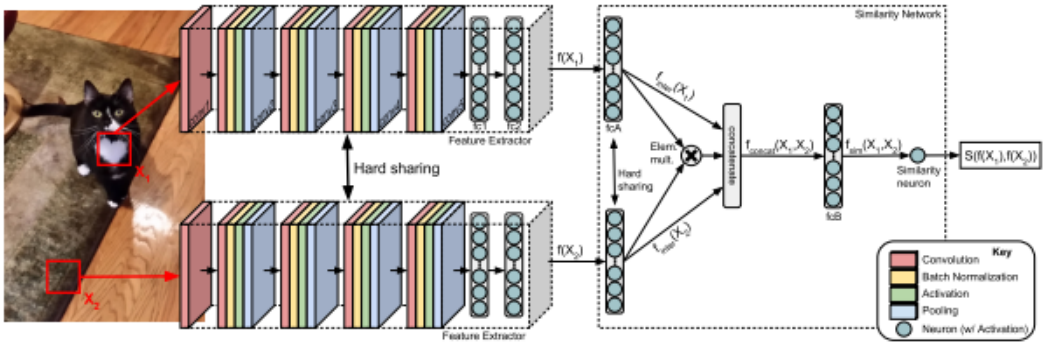
(a) Reference Image (Google Pixel 1) (b) Google Pixel 1 Image (c) Asus Zenfone 3 Image (d) Forensic Similarity Distribution

Gambar 2.6 Forensic similarity score

Contoh skor kesamaan forensik ditunjukkan pada Gambar 2. 5. Dalam contoh ini, perhitungan skor forensic similarity antara *patch* kecil yang dipilih secara acak dari tiga gambar berbeda: dua diambil oleh Google Pixel 1, dan satu diambil oleh Asus Zenfone 3. Tak satu pun dari model kamera ini digunakan untuk melatih sistem. Ketika kedua tambalan

ditangkap oleh model kamera yang sama, skor kesamaan forensik tinggi dan mendekati satu, seperti yang ditunjukkan oleh distribusi biru pada Gambar. 2.5 (d). Ketika kedua patch ditangkap oleh model kamera yang berbeda, skor forensic similarity rendah dan mendekati nol, seperti yang ditunjukkan oleh kurva oranye. Kualitas penting yang perlu diperhatikan adalah forensic similarity tidak berubah terhadap konten semantik yang digambarkan dalam gambar. Misalnya, meskipun gambar (a) dan gambar (c) menggambarkan pemandangan yang sangat mirip, skor forensic similarity rendah karena diambil oleh model kamera yang berbeda.

Pendekatan ini mendefinisikan jejak forensik sebagai sinyal yang tertanam dalam gambar yang diinduksi oleh, dan menangkap informasi tentang, operasi pemrosesan sinyal tertentu yang dilakukan pada gambar. Jejak forensik secara inheren tidak terkait dengan konten persepsi gambar; dua gambar yang menggambarkan adegan yang berbeda mungkin berisi jejak forensik yang sama, dan dua gambar yang menggambarkan adegan yang sama mungkin berisi jejak forensik yang berbeda. Mekanisme umum yang menyebabkan jejak forensik dalam suatu gambar adalah: model kamera yang menangkap gambar, situs web media sosial tempat gambar diunduh, dan riwayat pemrosesan gambar. Sejumlah pendekatan telah diteliti untuk mengekstrak dan mengidentifikasi jejak forensik yang terkait dengan mekanisme ini. Arsitektur forensic similarity berbasis CNN yang ditujukan untuk mengekstraksi fitur forensik yang kuat dari gambar dan secara akurat menentukan kesamaan forensik antara dua patch gambar.



Gambar 2.7 Arsitektur Forensic similarity

Pendekatan sebelumnya ini, bagaimanapun, mengasumsikan serangkaian jejak forensik yang tertutup. Mereka dirancang untuk melakukan pemetaan X → Y di mana X adalah ruang tambalan gambar dan Y adalah ruang jejak forensik yang diketahui yang digunakan untuk melatih sistem, misalnya model kamera atau operasi pengeditan. Namun ketika *patch* gambar *input* memiliki jejak forensik y /∈ Y, sistem identifikasi masih dipaksa

untuk memetakan ke ruang Y, yang mengarah ke hasil yang salah. Artinya, sistem akan salah mengklasifikasikan jejak "*unknown*" baru ini sebagai jejak "*known*" di Y.

Ini bermasalah karena dalam praktiknya penyidik forensik sering disajikan dengan gambar atau tambalan gambar yang berisi jejak forensik yang penyidiknya tidak memiliki contoh pelatihan. Kami menyebutnya jejak forensik yang tidak diketahui. Ini mungkin model kamera yang tidak ada di *database* penyidik, atau operasi pengeditan yang sebelumnya tidak diketahui. Dalam skenario ini, masih penting untuk mengumpulkan forensik penting tentang gambar atau *patch* gambar.

Untuk mengatasi ini, kami mengusulkan sistem yang mampu beroperasi pada jejak forensik yang tidak diketahui. Alih-alih membangun sistem untuk mengidentifikasi jejak forensik tertentu, kami mengajukan pertanyaan "apakah kedua tambalan gambar ini berisi jejak forensik yang sama?" Meskipun sistem kesamaan forensik mungkin belum pernah melihat jejak forensik tertentu sebelumnya, ia masih dapat membedakan apakah mereka sama atau berbeda di dua tambalan. Jenis pertanyaan ini analog dengan masalah pengambilan gambar berbasis konten, dan masalah verifikasi pembicara.

Forensic similarity didefinisikan sebagai fungsi

$$C : \mathbb{X} \times \mathbb{X} \rightarrow \{0,1\} \tag{2.1}$$

yang membandingkan dua tambalan gambar. Hal ini dilakukan dengan memetakan dua tambalan gambar input X1, X2 ∈ X ke skor yang menunjukkan apakah kedua tambalan gambar tersebut memiliki jejak forensik yang sama atau berbeda. Skor 0 menunjukkan dua tambalan gambar berisi jejak forensik yang berbeda, dan skor 1 menunjukkan bahwa mereka mengandung jejak forensik yang sama. Dengan kata lain

$$C(X_1, X_2) = \begin{Bmatrix} 0 \text{ jika } X_1, X_2 \text{ berbeda jejak forensik} \\ 1 \text{ jika } X_1, X_2 \text{ sama jejak forensik} \end{Bmatrix} \tag{2.2}$$

Untuk membangun sistem ini, kami mengusulkan sistem kesamaan forensik yang terdiri dari dua bagian konseptual utama, yang ditunjukkan pada gambaran umum sistem pada Gambar.2 1. Bagian konseptual pertama disebut *ekstraktor* fitur.

$$f : \mathbb{X} \rightarrow \mathbb{R}^N \tag{2.3}$$

yang memetakan *patch* gambar *input* X ke ruang fitur dimensi-N yang bernilai nyata. Ruang fitur ini mengkodekan informasi forensik tingkat tinggi tentang tambalan gambar X. Penelitian terbaru dalam forensik multimedia telah menunjukkan bahwa *convolutional neural network* (CNN) adalah alat yang ampuh untuk mengekstraksi informasi forensik umum tingkat tinggi dari *patch* gambar [23]. Kami menentukan bagaimana ini dilakukan di

Sec. III, di mana kami menjelaskan implementasi yang kami usulkan dari sistem forensic similarity.

Selanjutnya kita mendefinisikan bagian konseptual kedua, fungsi kesamaan

$$S : RN \times RN \rightarrow [0,1] \quad (2.4)$$

yang memetakan pasangan vektor fitur forensik ke skor kesamaan yang mengambil nilai dari 0 hingga 1. Skor kesamaan yang rendah menunjukkan bahwa kedua patch gambar X1 dan X2 memiliki jejak forensik yang berbeda, dan skor kesamaan yang tinggi menunjukkan bahwa kedua jejak forensik sangat serupa.

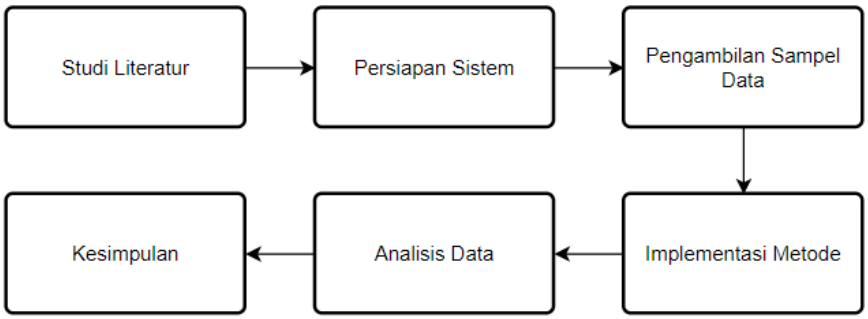
Terakhir, kami membandingkan skor kesamaan S(f(X1), f(X2)) dari dua *patch* gambar X1 dan X2 dengan ambang batas η sedemikian rupa sehingga

$$C(X_1, X_2) = \begin{cases} 0 & \text{jika } S(f(X_1), f(X_2)) \leq \eta \\ 1 & \text{jika } S(f(X_1), f(X_2)) > \eta \end{cases} \quad (2.5)$$

Dengan kata lain, sistem kesamaan forensik yang diusulkan mengambil dua tambalan gambar X1 dan X2 sebagai masukan. *Ekstraktor* fitur memetakan dua tambalan gambar input ini ke sepasang vektor fitur f(X1) dan f(X2), yang mengkodekan informasi forensik tingkat tinggi tentang tambalan gambar. Kemudian, fungsi kesamaan memetakan kedua vektor fitur ini ke skor kesamaan, yang kemudian dibandingkan dengan ambang batas. Skor kesamaan di atas ambang batas menunjukkan bahwa X1 dan X2 memiliki jejak forensik yang sama (misalnya riwayat pemrosesan atau model kamera sumber), dan skor kesamaan di bawah ambang batas menunjukkan bahwa mereka memiliki jejak forensik yang berbeda.

BAB 3
Metodologi

Proses penelitian ini dilakukan dengan metodologi, sehingga dapat diketahui urutan langkah-langkah secara sistematis yang dapat dijadikan pedoman untuk menyelesaikan masalah, membuat analisis, serta kendala-kendala yang dihadapi. Adapun langkah-langkah yang ditempuh untuk melakukan penelitian ini adalah sebagai berikut:



Gambar 3.1 Alur Metodologi Penelitian

Pada gambar 3.1 menjelaskan alur metodologi penelitian yang digunakan untuk melakukan identifikasi source model camera pada gambar yang menjadi barang bukti dan melakukan pengujian pada gambar yang telah dilakukan manipulasi pada metadata dari gambar tersebut.

3.1 Studi Literatur

Tahap ini dilakukan untuk mengumpulkan referensi yang terkait dengan penelitian, misalnya jurnal, paper, buku, makalah dan sumber lain yang membahas tentang *Source Model Camera* serta referensi lainnya.

3.2 Persiapan Sistem

Penelitian ini menggunakan beberapa alat dan bahan untuk menguji dan mengimplementasikan penelitian yang mendukung perolehan informasi yang dibutuhkan> Perangkat yang digunakan dalam penelitian ini adalah komputer dan smartphone yang disajikan pada Tabel 3.1.

Tabel 3.1 Hardware

No	Nama	Spesifikasi
1.	Asus ROG GL503GE	• Processor Intel Core i7-8750H • RAM 8GB • Storage 1TB
2.	Xiaomi MI5	• Android • Storage 64GB • RAM 3GB
3.	Samsung Galaxy S6	• Android • Storage 64GB • RAM 3GB

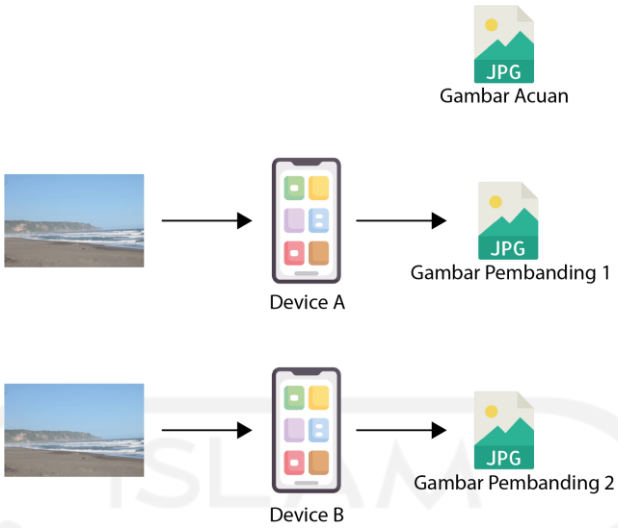
Sementara itu, Tabel 3.2 menyajikan perangkat lunak yang digunakan pada penelitian ini.

Tabel 3.2 Software

No	Nama Perangkat Lunak
1.	Windows 10 Home 64-bit
2.	Jupiter Notebook

3.3 Pengambilan Sampel Data

Sesuai dengan prosedur forensika digital diperlukan tahapan dalam pengambilan barang bukti digital. Hal itu agar dapat menunjukkan kemiripan barang bukti. Barang bukti digital tersebut selanjutnya dijadikan parameter pada metode yang akan dianalisis. Tahapan penanganan barang bukti digital untuk pengambilan sampel data dilakukan pada tahap *acquisition*. *Acquisition* adalah langkah yang meliputi pembuatan citra forensik (*imaging*) dari barang bukti. Ini harus dilakukan untuk menghindari gangguan terhadap bukti asli. Pencitraan seperti menyalin bukti, namun, selain menangkap semua data bukti, seperti file dan folder, pencitraan menangkap informasi penting, seperti *metadata*. Proses menghasilkan salinan yang identik dengan melakukan proses *copy bit per bit* yang akan menghasilkan file DD *image*.



Gambar 3.2 Proses Pengumpulan Data

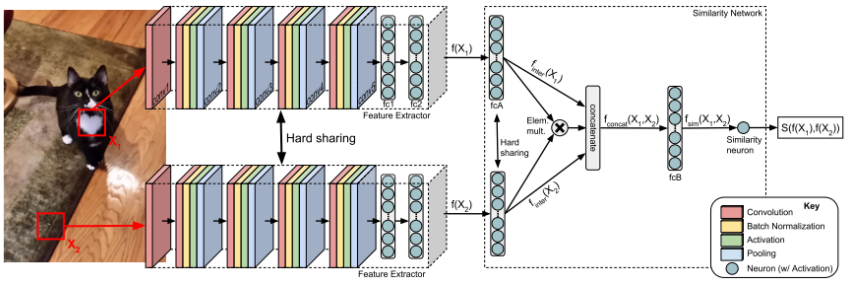
Berdasarkan gambar di atas, proses pengumpulan data berupa gambar diambil dari beberapa perangkat yang berbeda. Setiap perangkat diambil beberapa gambar untuk menjadi data acuan dan data pengujian pada proses implementasi pendekatan *forensic similarity* yang berbasiskan CNN.

3.4 Analisis Metadata

Pada tahap ini dilakukan analisis metadata pada gambar dengan menggunakan *tool* EXIF untuk memperoleh *metadata* dari gambar yang diujikan berupa merek perangkat, model perangkat, software perangkat, serta tanggal gambar tersebut diambil.

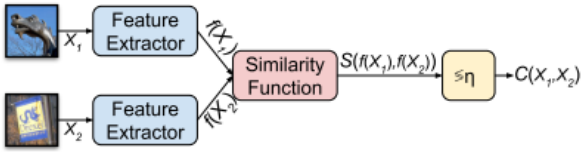
3.5 Implementasi Metode

Pada tahap ini mulai dilakukan implementasi pendekatan *forensic similarity* berbasiskan *convolutional neural network* berdasarkan parameter-parameter yang telah dirumuskan.



Gambar 3.3 Arsitektur *Forensic Similarity*

Forensic similarity adalah pendekatan yang menentukan apakah dua *patch* gambar memiliki jejak forensik yang sama atau berbeda. Tidak seperti pendekatan forensik lainnya, pendekatan ini tidak mengidentifikasi jejak tertentu, tetapi tetap memberikan informasi forensik penting kepada penyidik. Manfaat utama dari jenis pendekatan ini adalah dapat diterapkan secara praktis dalam skenario set terbuka. Artinya, sistem berbasis kesamaan forensik tidak secara inheren memerlukan sampel pelatihan dari jejak forensik untuk membuat keputusan.



Gambar 3.4 Sistem Forensic Similarity

Forensic similarity terdiri dari dua elemen konseptual: 1) *feature extractor* berbasis CNN yang memetakan gambar yang menjadi input ke *low-dimensional feature*, dan 2) *three-layer neural network*, yang memetakan pasangan fitur ini ke skor yang menunjukkan apakah dua patch gambar berisi jejak forensik yang sama.

3.6 Analisis Data

Tahapan ini adalah proses analisis data dari hasil pengujian dengan menggunakan pendekatan *forensic similarity* yang menghasilkan nilai kemiripan dalam perbandingan gambar dari perangkat yang sama.

3.7 Kesimpulan

Berdasarkan semua proses yang telah dilakukan selama penelitian ini akan didokumentasikan dalam laporan, sehingga dapat diperoleh kesimpulan yang menjadi landasan dari penerapan metode beserta kelebihan dan kekurangan dari metode tersebut. Hasil laporan dari kesimpulan tersebut berguna sebagai referensi bagi penelitian selanjutnya.

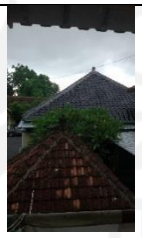
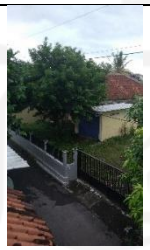
BAB 4
Hasil dan Pembahasan

Bab ini membahas hasil penelitian yang dijelaskan proses identifikasi *source camera* berdasarkan flowchart metodologi penelitian pada bab tiga, dimulai dari studi literatur, pengumpulan data, implementasi metode, analisis data, serta mendapatkan kesimpulan dari penelitian ini.

4.1 Pengambilan Sampel Data

Pada tahapan ini dilakukan proses pengumpulan data berupa data tiga gambar dari 2 perangkat yang berbeda.

Tabel 4.1 Data Gambar

Perangkat	**Nama File**	**Gambar**
Xiaomi Mi5	xiaomi_mi5_a.jpg	
Realme 9 Pro	realme_9_pro_a.jpg	
Xiaomi Mi5	xiaomi_mi5_b.jpg	

Data Gambar yang digunakan dalam penelitian merupakan gambar yang diambil langsung menggunakan menggunakan 2 perangkat yaitu Xiaomi Mi5 dan Realme 9 Pro dengan rincian gambar acuan diambil dengan Xiaomi Mi5 yang kemudian kita sebut dengan gambar (a), gambar yang kita ambil dengan Realme 9 Pro dan memiliki latar foto yang sama dengan gambar (a) yang kemudian kita sebut dengan gambar (b), serta gambar yang kita

ambil dengan Xiaomi Mi5 dan memiliki latar foto yang berbeda dengan gambar (a) yang kemudian kita sebut sebagai gambar (c).

4.2 Analisis Metadata Gambar

Metadata adalah data yang memberikan beberapa informasi penting tentang data yang dapat digunakan untuk menganalisis bukti, kepemilikan, dan kualitas data tersebut. Dari metadata file gambar jpeg banyak informasi seperti ukuran gambar, merek & model kamera, resolusi, tanggal dan waktu asli dan diedit, dll.

Tabel 4.2 Metadata Gambar

Nama File	**Metadata**
xiaomi_mi5_a.jpg	Make: Xiaomi Model: MI 5 Software: gemini-user 8.0.0 OPR1.170623.032 V10.2.2.0.OAAMIXM release-keys DateTime (Original): 2021:10:31 16:53:04
realme_9_pro_a.jpg	Make: realme Model: realme 9 Pro 5G Software: None DateTime (Original): 2022:06:18 14:27:19
xiaomi_mi5_b.jpg	Make: Xiaomi Model: MI 5 Software: gemini-user 8.0.0 OPR1.170623.032 V10.2.2.0.OAAMIXM release-keys DateTime (Original): 2021:10:31 16:52:20

Berdasarkan tabel di atas, penulis menggunakan *tool* EXIF untuk memperoleh *metadata* dari gambar yang diujikan berupa merek perangkat, model perangkat, software perangkat, serta tanggal gambar tersebut diambil.

Metadata yang diperoleh bisa menjadi alat bantu untuk mengetahui gambar tersebut diambil menggunakan perangkat apa. Namun informasi yang didapat tersebut benar atau asli, karena saat ini sangat mudah untuk melakukan manipulasi atau modifikasi metadata pada gambar tertentu. Apakah mungkin untuk mengetahui model kamera yang digunakan untuk mengambil gambar meskipun model kamera, tanggal dan waktu, dan informasi

lainnya dapat ditemukan di EXIF atau di *header* JPEG. Diharapkan dengan menggunakan pendekatan *forensic similarity* bisa membantu kita sebagai penyidik ketika ingin melakukan identifikasi sumber kamera dari gambar tertentu pada proses image forensik. Karena kamera merupakan sumber informasi penting yang dapat digunakan untuk melakukan *autentikasi* asal gambar di bidang image forensik.

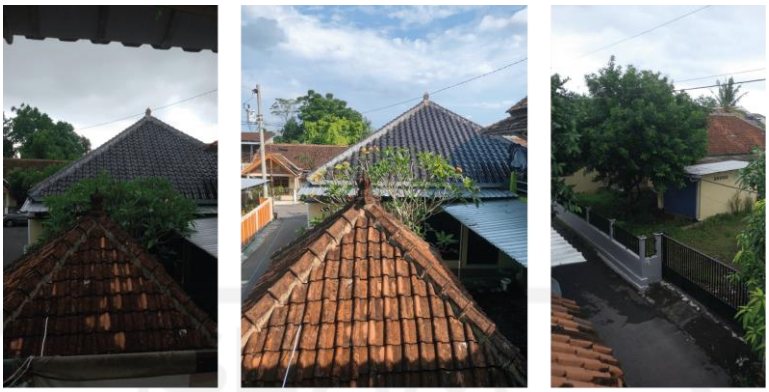
4.3 Implementasi Pendekatan *Forensic Similarity*

Gambar 4.1 Alur Implementasi Metode

Pendekatan *Forensic similarity*, menentukan apakah dua *image patch* mengandung jejak forensik yang sama atau berbeda. Pendekatan ini berbeda dari pendekatan forensik lainnya karena tidak secara eksplisit mengidentifikasi jejak forensik tertentu yang terkandung dalam *image patch*, hanya apakah mereka konsisten di dua *image patch*.

Pendekatan ini mendefinisikan jejak forensik sebagai sinyal yang tertanam dalam gambar dan menangkap informasi tentang, operasi pemrosesan sinyal tertentu yang dilakukan pada gambar. Jejak forensik secara inheren tidak terkait dengan konten persepsi gambar; dua gambar yang menggambarkan adegan yang berbeda mungkin berisi jejak forensik yang sama, dan dua gambar yang menggambarkan adegan yang sama mungkin berisi jejak forensik yang berbeda. Mekanisme umum yang menyebabkan jejak forensik dalam suatu gambar adalah: model kamera yang menangkap gambar, situs web media sosial tempat gambar diunduh, dan riwayat pemrosesan gambar.

Pada implementasi identifikasi *source image* menggunakan pendekatan *forensic similarity* menggunakan 2 perangkat yaitu Xiaomi Mi5 dan Realme 9 Pro dengan rincian gambar acuan diambil dengan Xiaomi Mi5 yang kemudian kita sebut dengan gambar (a), gambar yang kita ambil dengan Realme 9 Pro dan mempunyai latar foto yang sama dengan gambar (a) yang kemudian kita sebut dengan gambar (b), serta gambar yang kita ambil dengan Xiaomi Mi5 dan memiliki latar foto yang berbeda dengan gambar (a) yang kemudian kita sebut sebagai gambar (c).



Gambar 4.2 Gambar A (Xiaomi Mi5), Gambar B (Realme 9 Pro), Gambar C (Xiaomi Mi5)

Dengan skenario bahwa (a) yang menjadi barang bukti diambil dengan menggunakan Xiaomi Mi5 yang akan dibandingkan dengan gambar (b) dan (c) yang diambil dari perangkat Realme 9 Pro dan Xiaomi Mi5. Dimana gambar (a) dan (b) memiliki latar foto, sedangkan gambar (c) memiliki latar foto yang berbeda.

4.3.1 Identifikasi Patch Gambar

Forensic similarity menjelaskan metode untuk memilih *patch* gambar yang sesuai untuk analisis forensik menggunakan metode seleksi berbasis entropi untuk menyaring *patch* gambar sebelum menganalisis kesamaan forensiknya. Melihat jejak forensik sebagai sejumlah informasi yang dikodekan dalam gambar yang telah diinduksi oleh beberapa operasi pemrosesan. *Patch* gambar adalah saluran yang mengomunikasikan informasi ini. Dari saluran ini akan diekstrak informasi forensik menggunakan fitur ekstraktor dan kemudian membandingkan *patch* gambar menggunakan *similarity network*.

```
# import library
import sys
sys.path.append('../')
import forensic_similarity as forsim
from utils.blockimage import tile_image

import matplotlib.pyplot as plt
import matplotlib.cm as cm
import numpy as np
```

Gambar 4.3 Proses *import library/package*

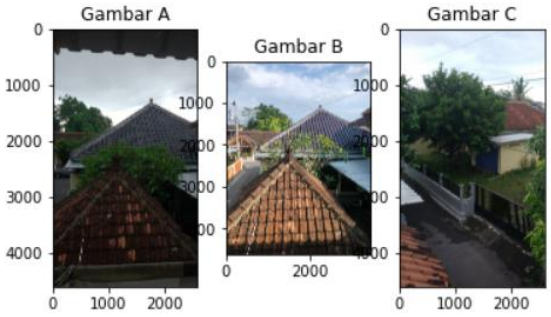
Proses yang pertama ketika melakukan implementasi pendekatan *forensic similarity* adalah melakukan *import library/package* yang diperlukan untuk menjalankan jupiter notebook untuk keperluan *image processing* termasuk *package* pendekatan *forensic similarity*.

```
# load gambar
I0 = plt.imread('./images/xiaomi_mi5_a.jpg')
I1 = plt.imread('./images/realme_9_pro_a.jpg')
I2 = plt.imread('./images/xiaomi_mi5_b.jpg')
```

Gambar 4.4 Proses load data gambar

Kemudian melakukan *load* data gambar yaitu gambar (a) yang menjadi gambar acuan dan gambar (b) dan (c) yang menjadi gambar pembanding. Gambar yang berhasil di *load* kemudian ditampilkan seperti pada gambar di bawah, terlihat gambar (a) dan gambar (b) mempunyai latar belakang foto yang sama sedangkan gambar (c) mempunyai latar foto yang berbeda.

```
#SHOW IMAGES
fig,ax = plt.subplots(1,3)
ax[0].imshow(I0); ax[1].imshow(I1); ax[2].imshow(I2)
ax[0].set_title('Gambar A'); ax[1].set_title('Gambar B'); ax[2].set_title('Gambar C')
plt.show()
```



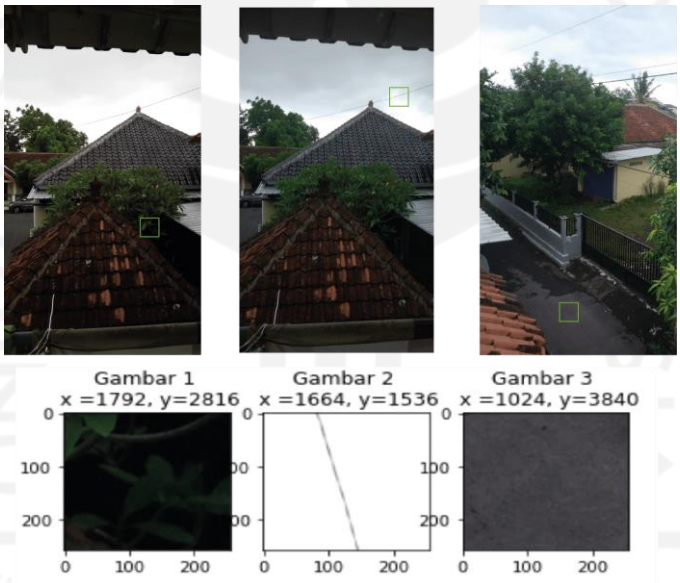
Gambar 4.5 Proses show gambar (a), (b), dan (c)

Tahap selanjutnya adalah memasukkan parameter *patch size* atau ukuran *patch* yang menjadi ukuran untuk *patch* yang akan dipilih nanti dan parameter *overlap*. Kemudian mengambil setiap *tile* dari setiap gambar sesuai dengan *patch size* yaitu 256 x 256 piksel setiap *tile* pada gambar (a), (b), dan (c).

```
#Get tiles/patches from images
patch_size = 256
overlap = 128

T0,xy0 = tile_image(I0,width=patch_size,height=patch_size,
                x_overlap=overlap,y_overlap=overlap)

T1,xy1 = tile_image(I1,width=patch_size,height=patch_size,
                x_overlap=overlap,y_overlap=overlap)

T2,xy2 = tile_image(I2,width=patch_size,height=patch_size,
                x_overlap=overlap,y_overlap=overlap)
```

Gambar 4.6 Proses mengambil *tile* atau *patch* dari setiap gambar

Selanjutnya dipilih *patch* pada *tile* dari setiap gambar secara acak atau *random* yang kemudian *patch* itu yang akan digunakan untuk melakukan perbandingan pada gambar (a) dan (b) serta gambar (a) dan (c).



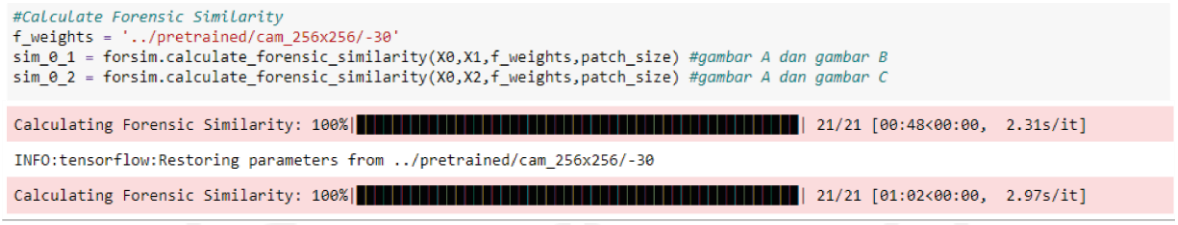
Gambar 4.7 Patch Gambar

Berdasarkan gambar di atas, Pendekatan *forensic similarity* memilih *patch* gambar 256x256 piksel secara acak dari ketiga gambar tersebut dan kemudian membandingkan *patch* gambar menggunakan *similarity network*.

4.3.2 Perhitungan Nilai Forensic Similarity

Tahap selanjutnya adalah melakukan perhitungan nilai *forensic similarity* antara gambar (a) dengan (b) dan gambar (a) dengan (c). Perhitungan dilakukan dengan membandingkan *image patch* antara gambar (a) dengan (b) dan *image patch* gambar (a) dengan (b)

menggunakan *image patch* dengan ukuran 256 x 256 piksel yang dipilih secara acak dari *tile* pada setiap gambar yang diproses yaitu gambar (a), (b), dan (c). Proses perhitungan ini menggunakan model yang sudah terdapat pada pendekatan *forensic similarity* yaitu model yang berbasis pada data *training* MISLNet dan CompareNet. Sehingga pendekatan ini tidak memerlukan data *training* baru untuk mengidentifikasi persamaan forensik dari dua patch pada gambar yang berbeda.



Gambar 4.8 Proses perhitungan *forensic similarity*

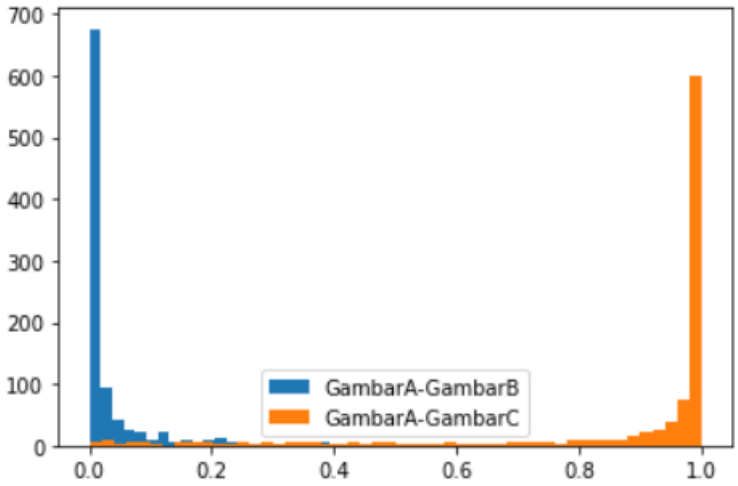
Proses perhitungan menggunakan pendekatan *forensic similarity* ini terdiri dari tahap *feature extractor* untuk mendapatkan *high level forensic feature vector* yang akan digunakan pada *similarity network*. Dimana *similarity network* ini adalah jaringan saraf yang memetakan *feature vector* dari dua patch gambar untuk memperoleh nilai *forensic similarity* yang akan menunjukkan apakah kedua *patch* tersebut mengandung jejak forensik yang sama atau berbeda.

```
#histogram graph
fig,ax = plt.subplots(1)
ax.hist(sim_0_1,50,label='GambarA-GambarB')
ax.hist(sim_0_2,50,label='GambarA-GambarC')
ax.legend()
plt.show()
```

Gambar 4.9 Proses menampilkan grafik histogram

Tahap terakhir adalah menampilkan *output* berupa nilai *forensic similarity* dan nilai *density* antara gambar (a) dengan gambar (b) dan gambar (a) dengan gambar (c) dalam bentuk grafik histogram sehingga lebih mudah dilihat. Dimana kurva biru menjelaskan gambar (a) dengan gambar (b) dan kurva orange menjelaskan gambar (a) dengan gambar (c). Sumbu x menjelaskan nilai *forensic similarity*, jika nilai mendekati nol maka perangkat berbeda dan jika mendekati satu maka perangkat sama. Sedangkan sumbu y menjelaskan nilai *density* atau tingkat kerapatan/persebaran piksel pada gambar dimana semakin tinggi nilai *density* akan membantu untuk memperoleh nilai *forensic similarity*. Hasil perhitungan

nilai *forensic similarity* tersebut kemudian ditampilkan dalam bentuk grafik, seperti gambar 4.10.



Gambar 4.10 Grafik Nilai *Forensic Similarity*

Berdasarkan grafik histogram pada gambar 4.10 di atas, dari proses *forensic similarity* diperoleh nilai kemiripan dengan melakukan perbandingan pada gambar (a) dengan gambar (b) dan gambar (a) dengan (c). Dimana gambar (a) dan (c) diambil menggunakan perangkat Xiaomi Mi5, dan gambar (b) diambil menggunakan Realme 9 Pro, ketika kedua patch diambil dari kamera yang sama maka nilai *forensic similarity* tinggi dan mendekati satu, seperti yang ditunjukkan oleh kurva orange. Ketika kedua patch diambil dari kamera yang berbeda maka nilai *forensic similarity* rendah dan mendekati nol, seperti yang ditunjukkan oleh kurva biru. Meskipun gambar (a) dan gambar (b) memiliki latar pemandangan yang sangat mirip seperti pada gambar 6, tapi nilai *forensic similarity* rendah karena diambil dari perangkat kamera yang berbeda.

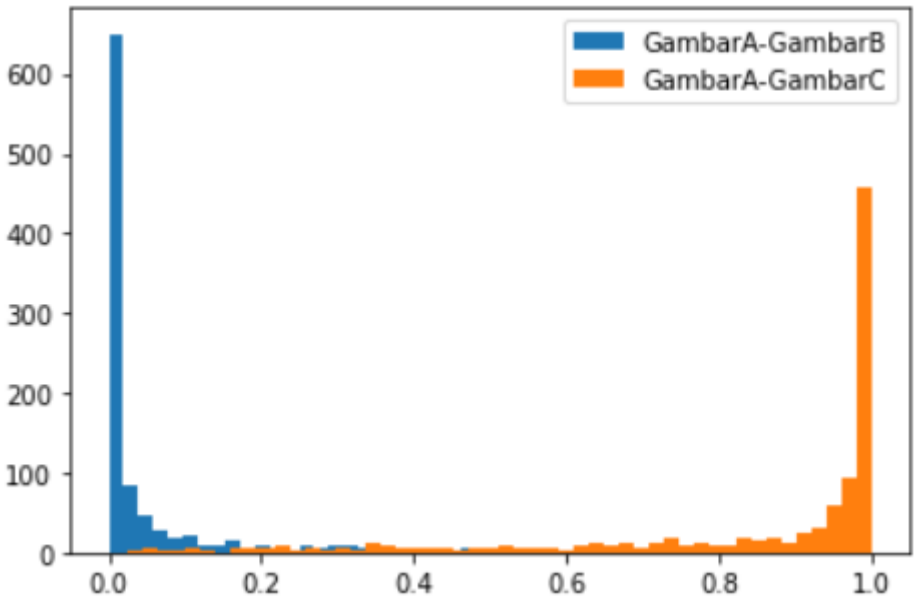
4.4 Analisis Gambar Non-Metadata

Pada proses ini penulis melakukan pengujian pada gambar acuan (Oppo Reno 6) yang tidak memiliki *metadata* atau sudah dimanipulasi metadatanya dan akan dibandingkan dengan gambar pembanding (Xiaomi Mi5 dan Oppo Reno 6). Dengan asumsi gambar acuan yang akan dibandingkan dengan gambar pembanding tidak mempunyai atribut *metadata* yang memberikan informasi terkait sumber kamera yang digunakan untuk mengambil gambar tersebut. Untuk membuat simulasi tersebut, penulis akan menggunakan *tool* EXIF untuk menghapus atribut metadata pada gambar tersebut misalnya, *make*, *model*, *software*, dan *datetime* dan lainnya.

```
Make: OPPO
Model: OPPO Reno6
Software: None
Artist: None
DateTime (Original): 2022:04:07 17:03:03
Flash Details: Flash(flash_fired=False, flash_return=FlashReturn.NO_STROBE_RETU
RN_DETECTION_FUNCTION, flash_mode=FlashMode.COMPULSORY_FLASH_SUPPRESSION, flash
_function_not_present=False, red_eye_reduction_supported=False, reserved=0)
pixel_x_dimension: 0
pixel_y_dimension: 0
compression: None

Make: None
Model: None
Software: None
Artist: None
DateTime (Original): None
Flash Details: None
pixel_x_dimension: 0
pixel_y_dimension: 0
compression: None
```

Gambar 4.11 Metadata gambar sebelum dan sesudah dihapus

Berdasarkan gambar di atas, semua atribut yang menjelaskan informasi terkait sumber kamera yang menjelaskan gambar tersebut diambil menggunakan perangkat tertentu tidak dijelaskan. Sehingga diperlukan proses identifikasi sumber kamera menggunakan pendekatan *forensic similarity* sehingga bisa dibandingkan dengan perangkat yang diduga sama dengan perangkat yang menjadi sumber gambar tersebut diambil.



Gambar 4.12 Grafik Nilai *Forensic Similarity* pada gambar *non-metadata*

Berdasarkan grafik pada gambar 4.5, diketahui dari proses *forensic similarity* diperoleh nilai kemiripan dengan melakukan perbandingan pada gambar A (Oppo Reno 6) dengan gambar B (Xiaomi Mi5) dan gambar A (Oppo Reno 6) dengan C (Oppo Reno 6). Diperoleh gambar (a) dan gambar (c) mempunyai nilai *forensic similarity* yang lebih tinggi

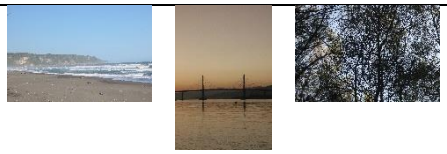
dan mendekati satu, seperti yang ditunjukkan oleh kurva *orange*. dibandingkan gambar A dan gambar B yang rendah dan mendekati nol, seperti yang ditunjukkan oleh kurva biru. Meskipun pada gambar (a) yang menjadi gambar acuan tidak memiliki atribut *metadata* yang menjelaskan informasi terkait sumber kamera.

Diketahui bahwa gambar acuan (Gambar A) setelah melalui proses menghapus atribut metadata menggunakan tool EXIF, meskipun berdasarkan grafik pada gambar 8 tetap diperoleh hasil yang sama yaitu ketika kedua patch diambil dari kamera yang sama maka nilai *forensic similarity* tinggi dan mendekati satu meskipun pada gambar non-metadata.

4.5 Pengujian Forensic Similarity

Pada pengujian implementasi pendekatan *forensic similarity*, penulis menggunakan 6 perangkat yang terdiri dari 5 perangkat *smartphone* dan 1 perangkat kamera DSLR dengan 3 data gambar untuk masing-masing perangkat, sehingga untuk pengujian ini menggunakan total 18 *file* gambar, seperti pada tabel berikut.

Tabel 4.3 Perangkat Pengujian

Perangkat	**Nama File**	**Gambar**
Xiaomi Mi 5	xiaomi_mi5_a.jpg xiaomi_mi5_b.jpg xiaomi_mi5_c.jpg	
Xiaomi Mi A1	xiaomi_mi_a1_a.jpg xiaomi_mi_a1_b.jpg xiaomi_mi_a1_c.jpg	
Oppo F7	oppo_f7_a.jpg oppo_f7_b.jpg oppo_f7_c.jpg	
Oppo Reno 6	oppo_reno_6_a.jpg oppo_reno_6_b.jpg oppo_reno_6_c.jpg	
Canon EOS 750D	canon_750d_a.jpg canon_750d_b.jpg canon_750d_c.jpg	

Realme 9 Pro	realme_9_pro_a.jpg realme_9_pro_b.jpg realme_9_pro_c.jpg	  

Skenario pada pengujian kali ini adalah setiap perangkat dibandingkan dengan perangkat yang lain untuk memperoleh nilai rata-rata *forensic similarity* dari 3 gambar setiap perangkatnya.

Tabel 4.4 Hasil Pengujian Gambar

Perangkat Acuan	**Perangkat Pembanding**											
	Xiaomi Mi5		Xiaomi Mi A1		Oppo F7		Oppo Reno 6		Canon EOS 750D		Realme 9 Pro	
	Density	Forensic Similarity	Density	Forensic Similarity	Density	Forensic Similarity	Density	Forensic Similarity	Density	Forensic Similarity	Density	Forensic Similarity
Xiaomi Mi5	610.0	0.99	459.0	0.89	902.0	0.11	635.0	0.10	757.0	0.10	953.0	0.24
Xiaomi Mi A1	478.0	0.90	965.0	0.99	737.0	0.19	658.0	0.20	977.0	0.06	974.0	0.21
Oppo F7	983.0	0.15	828.0	0.20	994.0	0.99	784.0	0.79	996.0	0.11	677.0	0.20
Oppo Reno 6	926.0	0.20	641.0	0.19	740.0	0.89	969.0	0.99	997.0	0.005	691.0	0.99
Canon EOS 750D	941.0	0.12	992.0	0.10	998.0	0.06	993.0	0.003	998.0	0.99	987.0	0.002
Realme 9 Pro	963.0	0.18	976.0	0.19	749.0	0.20	655.0	0.89	989.0	0.001	987.0	0.99

Berdasarkan tabel di atas, diketahui bahwa ketika kedua *patch* gambar diambil dari kamera yang sama maka nilai *forensic similarity* tinggi dan mendekati satu. Ketika kedua patch diambil dari kamera yang berbeda maka nilai *forensic similarity* rendah dan mendekati nol. Berdasarkan pengujian juga diperoleh bahwa perangkat dengan merek yang sama ketika dibandingkan memiliki nilai *forensic similarity* yang cukup tinggi atau mendekati 1 (satu) sehingga perlu juga dilihat nilai kerapatan piksel (*density*) yang bisa menjadi acuan pendukung jika perangkat tersebut memiliki nilai *forensic similarity* yang tinggi.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Pada penelitian ini menunjukkan bahwa pendekatan *forensic similarity* yang berbasis *convolutional neural network* (CNN) sebagai salah satu pendekatan yang dapat digunakan untuk melakukan identifikasi *source image* atau sumber kamera yang menjelaskan gambar tersebut diambil menggunakan perangkat yang diduga. Meskipun informasi terkait sumber kamera dapat diperoleh dari *metadata* pada *header* gambar tersebut menggunakan *tool* EXIF, namun informasi *metadata* yang diperoleh tidak secara langsung dianggap benar karena dapat dengan mudah dimanipulasi informasi pada *atribut metadata*. Dengan menggunakan pendekatan *forensic similarity* harapannya dengan teknik ini dapat mendukung informasi pada *metadata* sehingga dapat menjadi validasi apakah gambar tersebut diambil dari perangkat yang sama atau tidak serta menjamin keaslian dari informasi yang diperoleh.

5.2 Saran

Diketahui bahwa sampel file gambar yang diuji dan dianalisis adalah file gambar yang diperoleh secara langsung dari perangkat atau device tersebut bukan dari media sosial. Sehingga kedepannya bisa dikembangkan untuk file gambar yang berasal dari media sosial serta gambar yang telah dimodifikasi.

Daftar Pustaka

Alanazi, F., Lebh, L., & Jones, A. (2015). The Value of Metadata in Digital Forensics, *8*(2011), 161174. https://doi.org/10.1109/EISIC.2015.26

Böhme, R., & Kirchner, M. (2013). *Counter-Forensics : Attacking Image Forensics*. https://doi.org/10.1007/978-1-4614-0757-7

Bondi, L., Member, S., Baroffio, L., David, G., Bestagini, P., Delp, E. J., … Member, S. (2015). First Steps Toward Camera Model Identification with Convolutional Neural Networks, *14*(8), 1–5.

Cai, T., Shao, Z., Tomioka, Y., Liu, Y., & Li, Z. (2019). CNN-based Camera Model Identification Using Image Noise in Frequency Domain. *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, (1), 3518–3524. https://doi.org/10.1109/SMC.2019.8914375

Camacho, I. C., & Wang, K. (2021). A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. *Journal of Imaging*, *7*(69). https://doi.org/https://doi.org/10.3390/jimaging7040069

Dang-Nguyen, D.-T., Pasquini, C., Conotter, V., & Boato, G. (2015). RAISE - A Raw Images Dataset for Digital Image Forensics. In *MMSys '15: Proceedings of the 6th ACM Multimedia Systems Conference* (pp. 219–224). https://doi.org/https://doi.org/10.1145/2713168.2713194

Firdaus, V. A. H. (2016). Forensik Audio Pada Rekaman Suara. *School of Electrical Engineering and Informatics Institute Technology of Bandung Bandung, Indonesia*. Bandung.

Huang, N., He, J., Zhu, N., Xuan, X., Liu, G., & Chang, C. (2018). Identification of the Source Camera of Images Based on. *Digital Investigation*. https://doi.org/10.1016/j.diin.2018.08.001

Kirchner, M., & Gloe, T. (2015). Forensic Camera Model Identification. In *Handbook of Digital Forensics of Multimedia Data and Devices* (First Edit). Wiley-IEEE Press.

Mayer, O., & Stamm, M. C. (2019). Forensic Similarity for Digital Images. *IEEE Transactions on Information Forensics and Security*, *15*(1553610), 1331–1346. https://doi.org/10.1109/TIFS.2019.2924552

Mullan, P., Riess, C., & Freiling, F. (2019). Forensic source identification using JPEG

image headers: The case of smartphones. *Digital Investigation*, *28*, S68–S76. https://doi.org/10.1016/j.diin.2019.01.016

P, R. K., Srikanth, C., & Sailaja, K. L. (2016). Location Identification of the Individual based on Image Metadata. *Procedia - Procedia Computer Science*, *85*(Cms), 451–454. https://doi.org/10.1016/j.procs.2016.05.191

Piva, A. (2013). An Overview on Image Forensics. *International Scholarly Research Notices*, *2013*, 22. https://doi.org/https://doi.org/10.1155/2013/496701

Rahardjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi*, *12*(29), 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

Tuama, A., Comby, F., & Chaumont, M. (2016). Camera Model Identification With The Use of Deep Convolutional Neural Networks. *IEEE International Workshop on Information Forensics and Security (WIFS)*. https://doi.org/10.1109/WIFS.2016.7823908

Wang, B., Yin, J., Tan, S., Li, Y., & Li, M. (2018). Source Camera Model Identification Based on Convolutional Neural Networks with Local Binary Patterns Coding. *Signal Processing: Image Communication*. https://doi.org/10.1016/j.image.2018.08.001

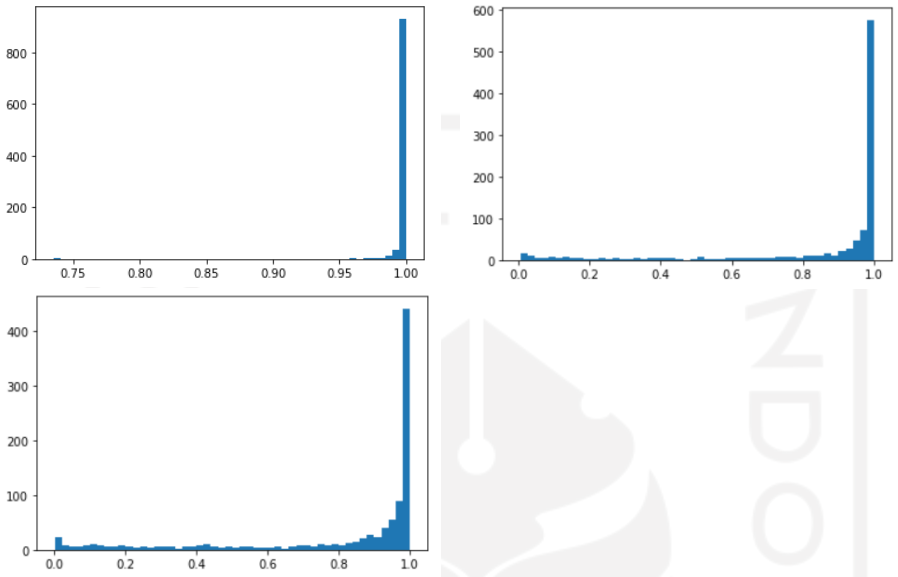
Xu, B., Wang, X., Zhou, X., Xi, J., & Wang, S. (2016). Source camera identification from image texture features. *Neurocomputing*, 1–10. https://doi.org/10.1016/j.neucom.2016.05.012

LAMPIRAN

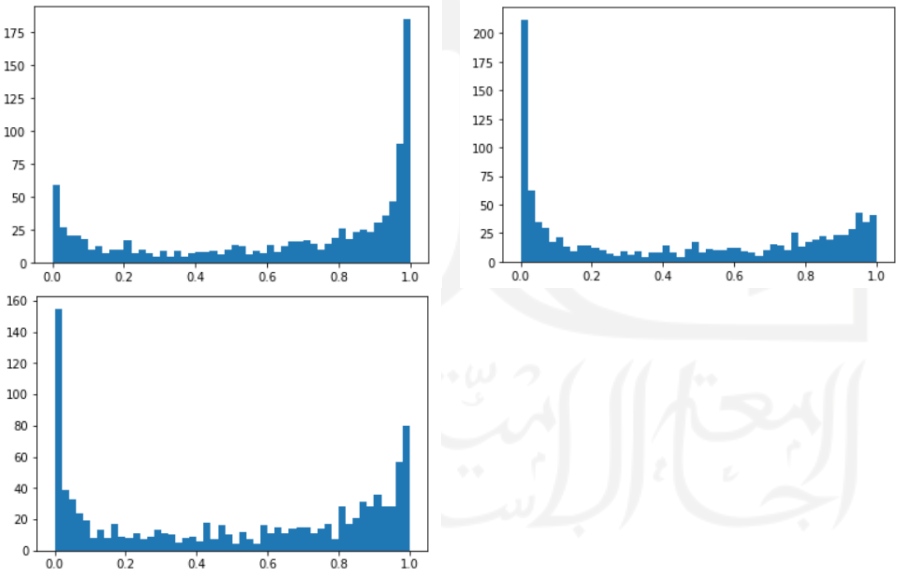
Visualisasi Hasil Pengujian Implementasi Pendekatan Forensic Similarity Pada Beberapa Perangkat:

1. Gambar Acuan Xiaomi Mi5

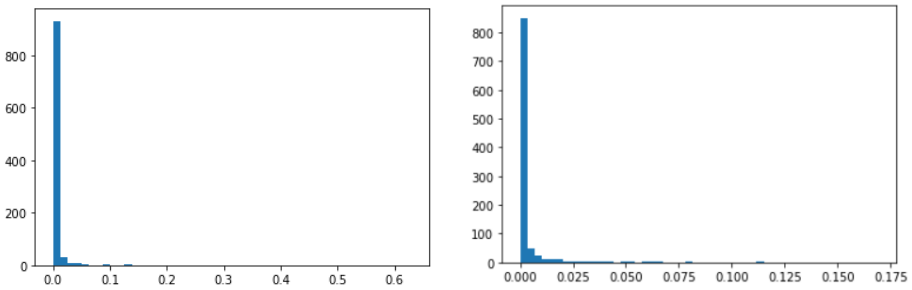
- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Xiaomi Mi 5:

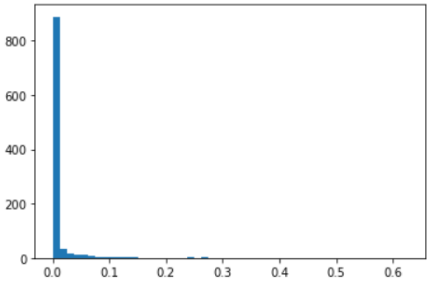


- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Xiaomi Mi A1:

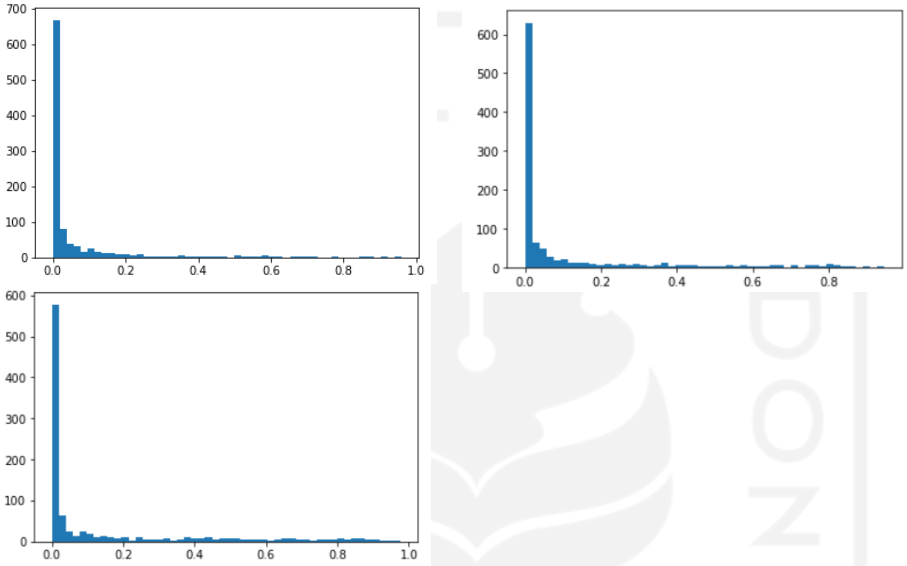


- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Oppo F7:

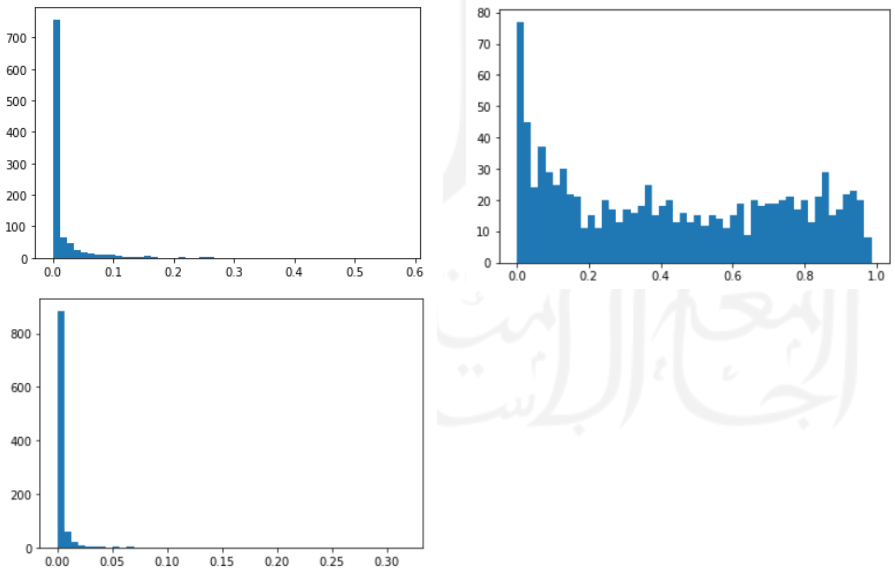




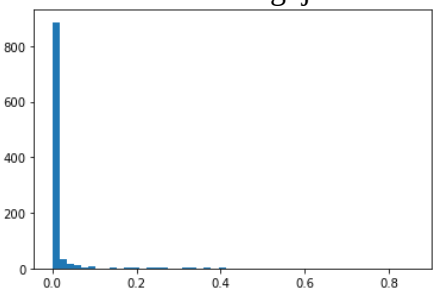
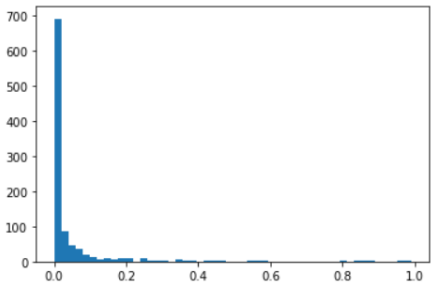
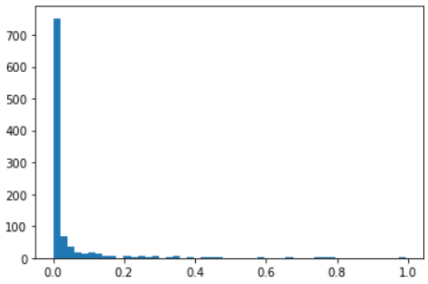
- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Oppo Reno 6:



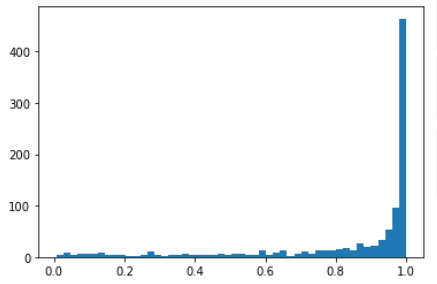
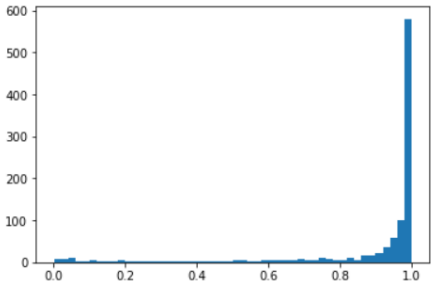
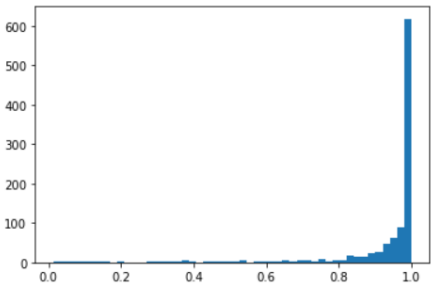
- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Canon EOS 750D:



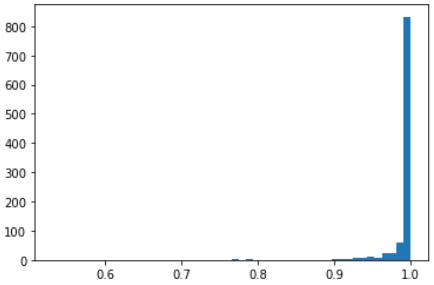
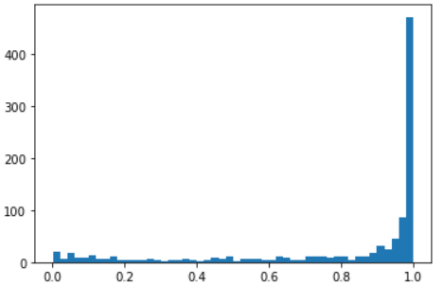
- Hasil Visualisasi Pengujian Xiaomi Mi 5 dan Realme 9 Pro:

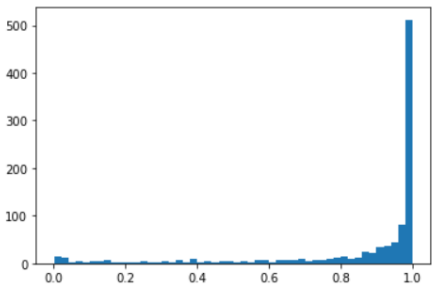




2. Gambar Acuan Xiaomi Mi A1:
   - Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Xiaomi Mi 5:

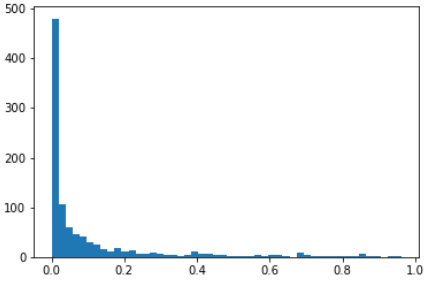




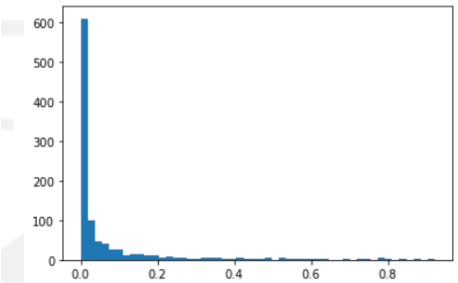
   - Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Xiaomi Mi A1:

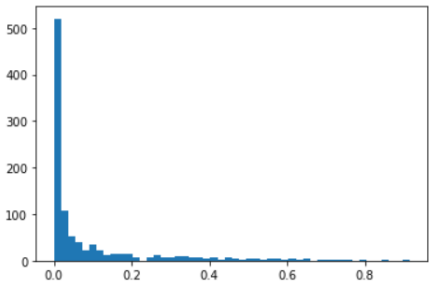





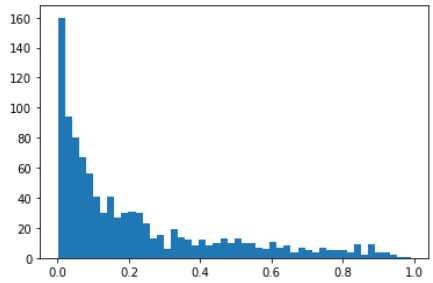
- Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Oppo F7:

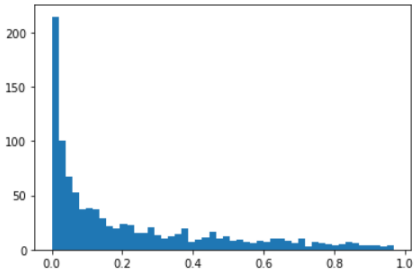


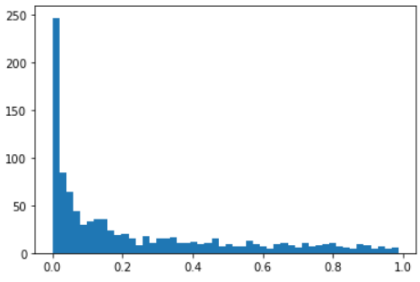




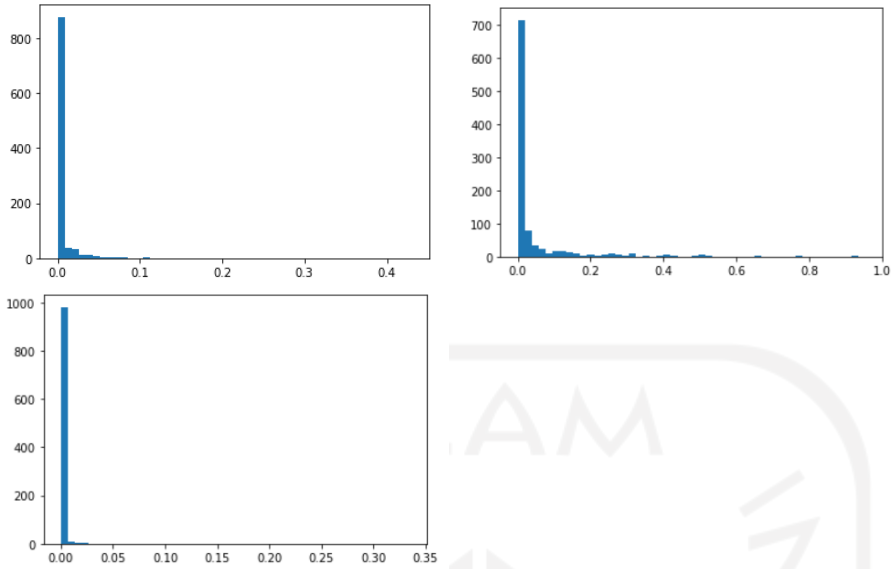
- Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Oppo Reno 6:



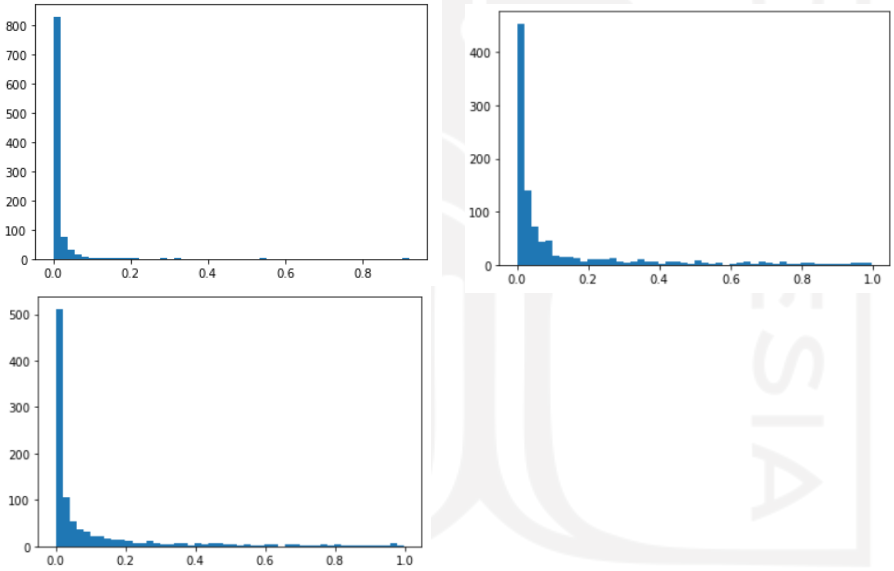




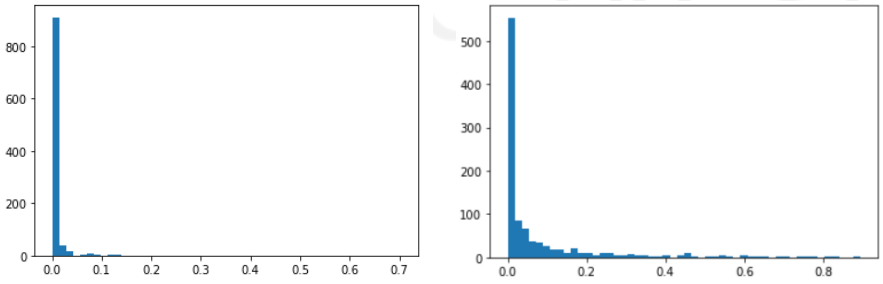
- Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Canon EOS 750D:

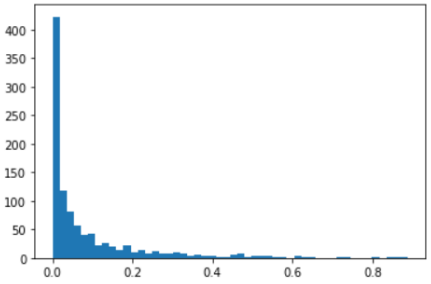


- Hasil Visualisasi Pengujian Xiaomi Mi A1 dan Realme 9 Pro:

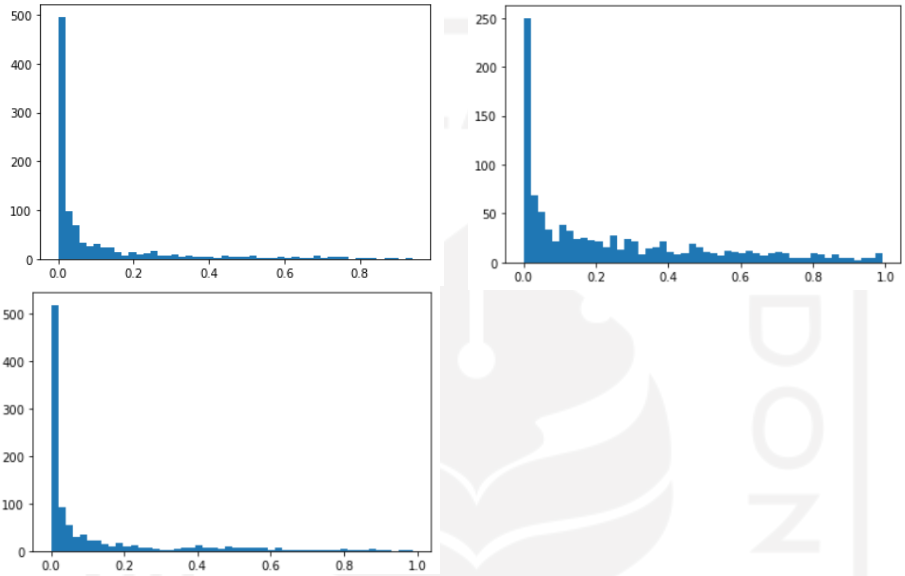


3. Gambar Acuan Oppo F7:
   - Hasil Visualisasi Pengujian Oppo F7 dan Xiaomi Mi 5:

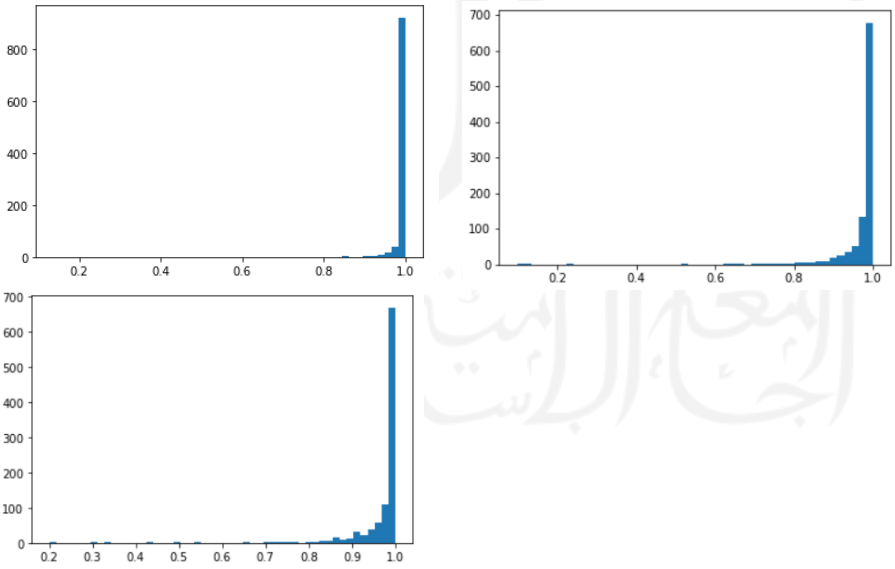




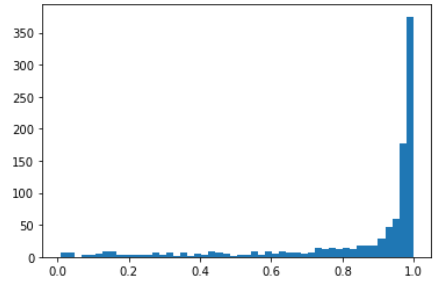
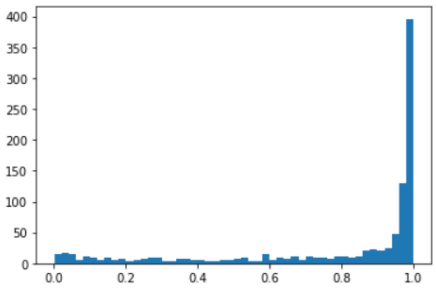
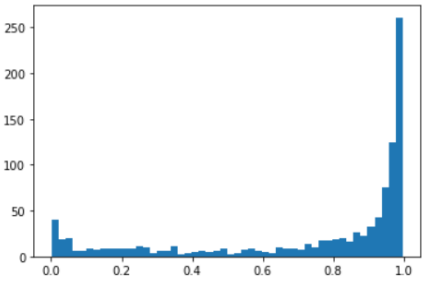
- Hasil Visualisasi Pengujian Oppo F7 dan Xiaomi Mi A1:



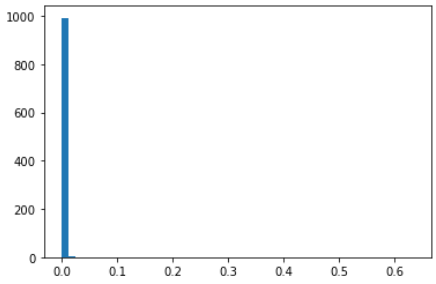
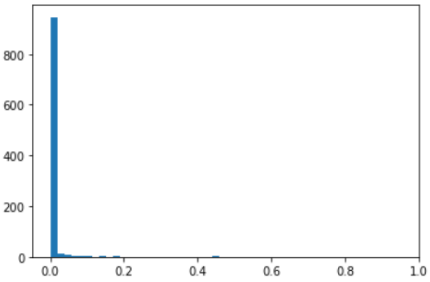
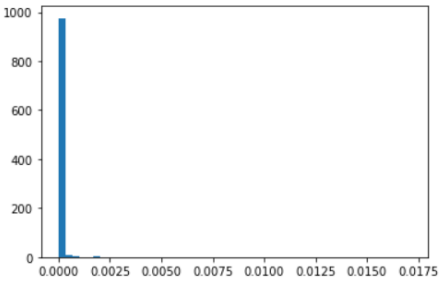
- Hasil Visualisasi Pengujian Oppo F7 dan Oppo F7:



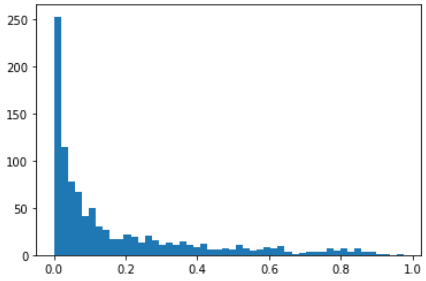
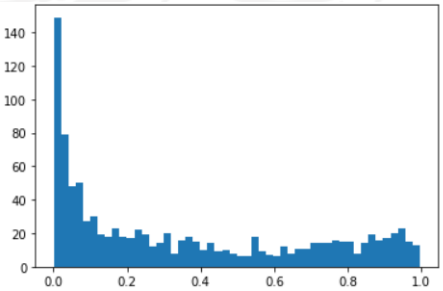
- Hasil Visualisasi Pengujian Oppo F7 dan Oppo Reno 6:

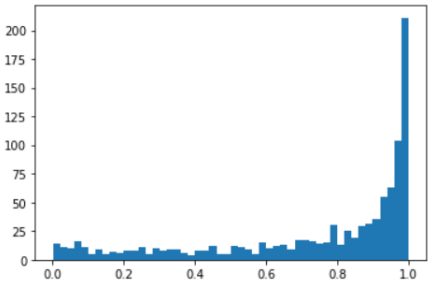




- Hasil Visualisasi Pengujian Oppo F7 dan Canon EOS 750D:

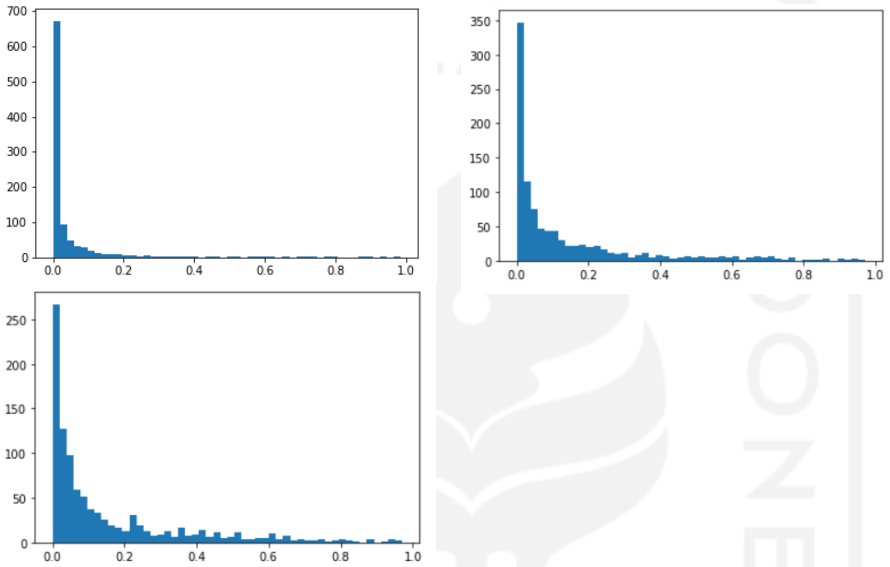
- Hasil Visualisasi Pengujian Oppo F7 dan Realme 9 Pro:

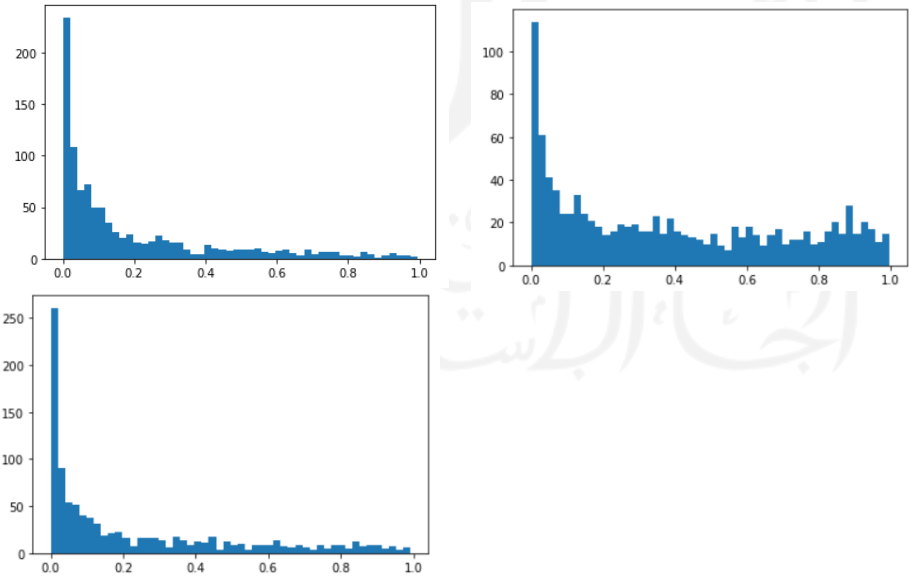


4. Gambar Acuan Oppo Reno 6:

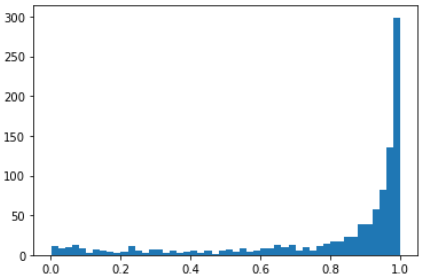
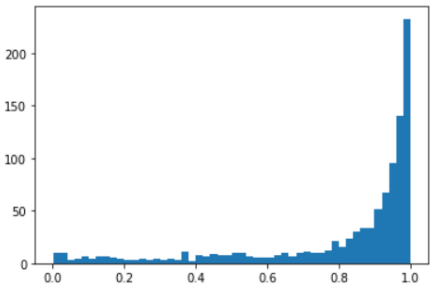
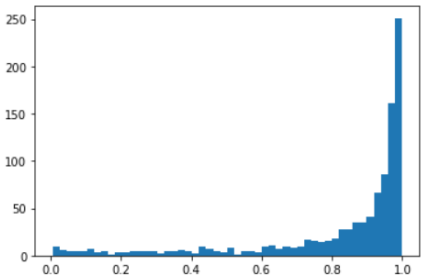
- Hasil Visualisasi Pengujian Oppo Reno 6 dan Xiaomi Mi 5:



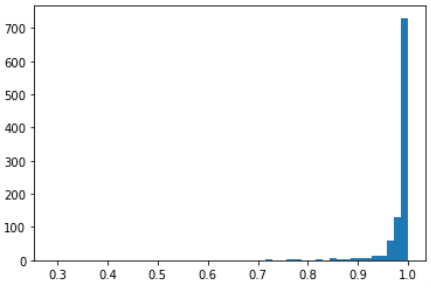
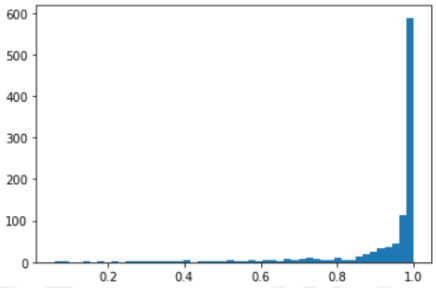
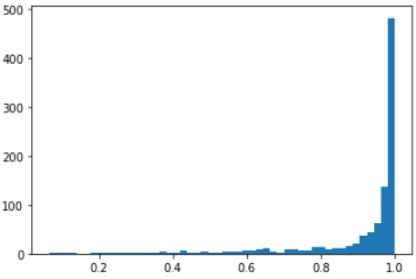
- Hasil Visualisasi Pengujian Oppo Reno 6 dan Xiaomi Mi A1:



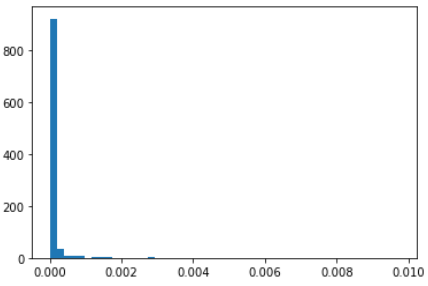
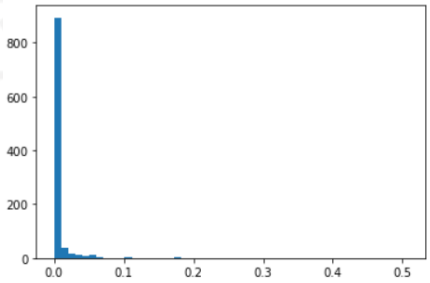
- Hasil Visualisasi Pengujian Oppo Reno 6 dan Oppo F7:

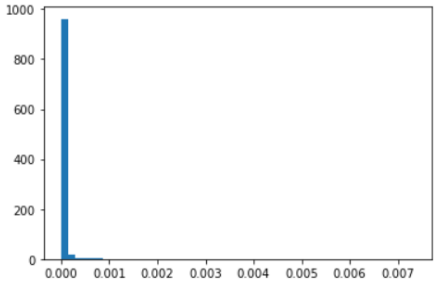




- Hasil Visualisasi Pengujian Oppo Reno 6 dan Oppo Reno 6:

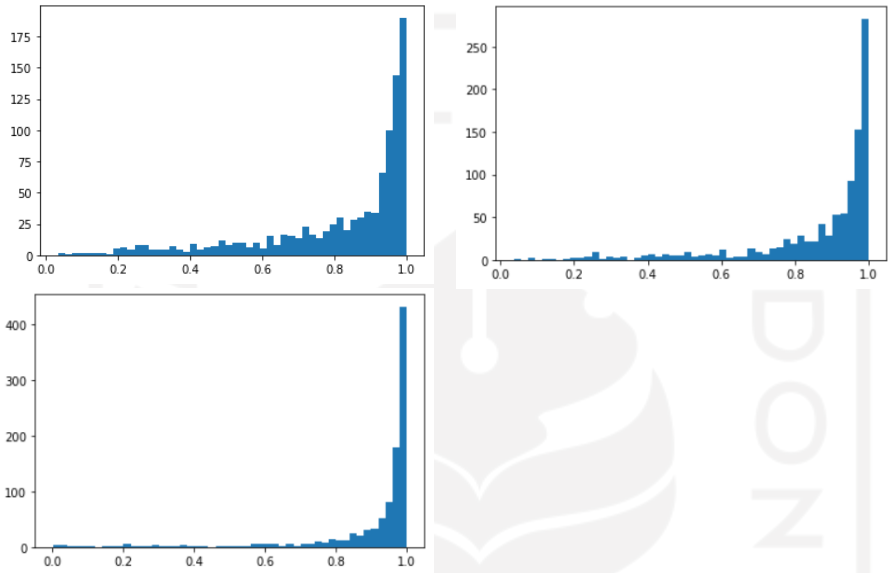




- Hasil Visualisasi Pengujian Oppo Reno 6 dan Canon EOS 750D:

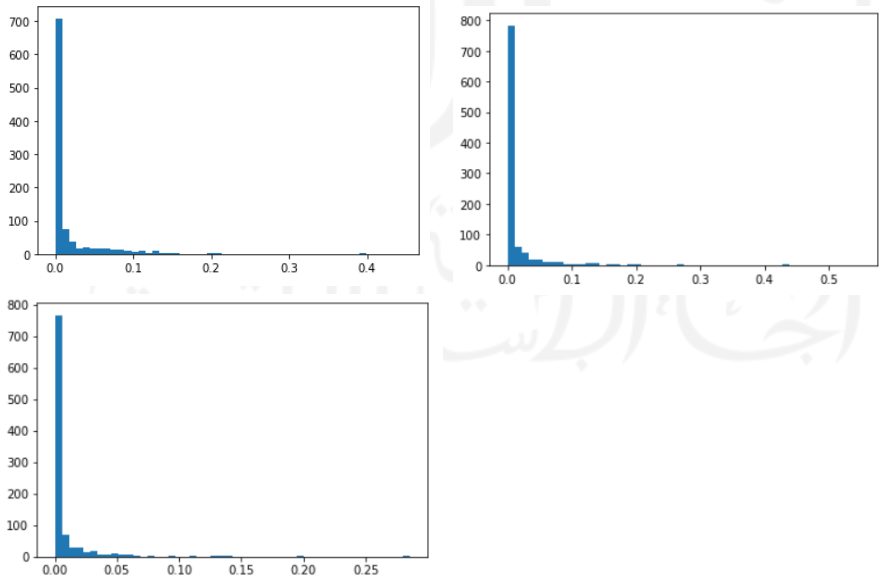





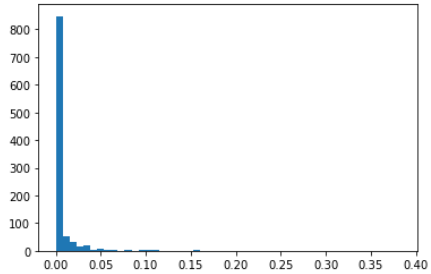
- Hasil Visualisasi Pengujian Oppo Reno 6 dan Realme 9 Pro:

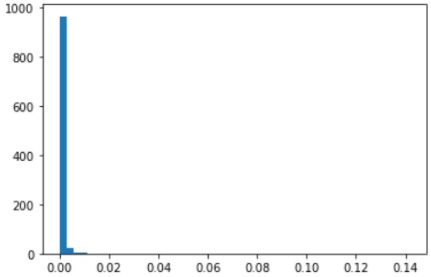


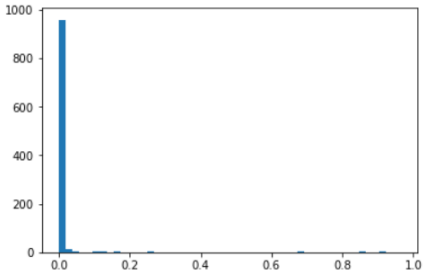
5. Gambar Acuan Canon EOS 750D:
   - Hasil Visualisasi Pengujian Canon EOS 750D dan Xiaomi Mi 5:



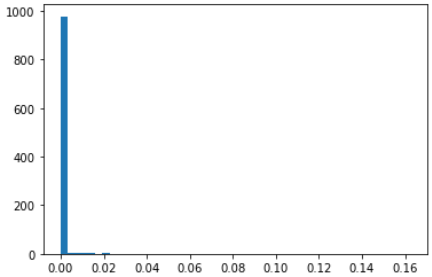
- Hasil Visualisasi Pengujian Canon EOS 750D dan Xiaomi Mi A1:

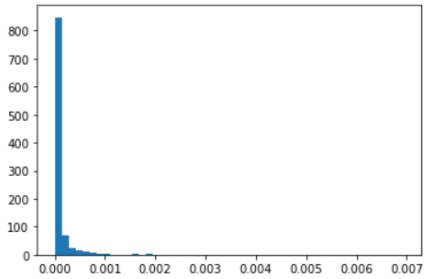


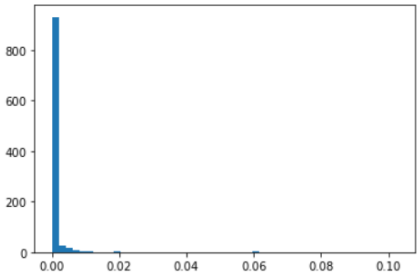




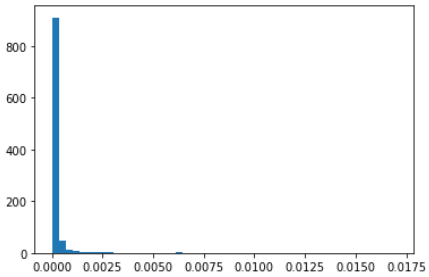
- Hasil Visualisasi Pengujian Canon EOS 750D dan Oppo F7:

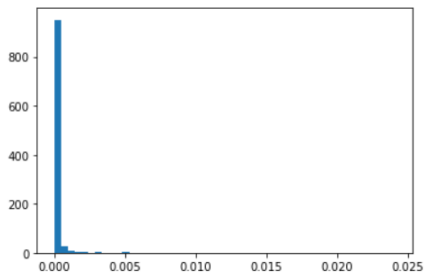


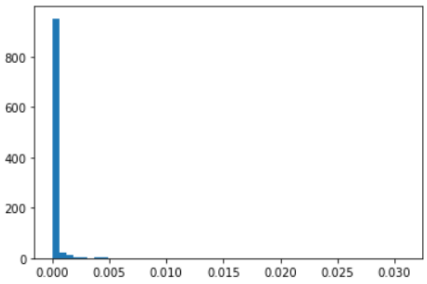




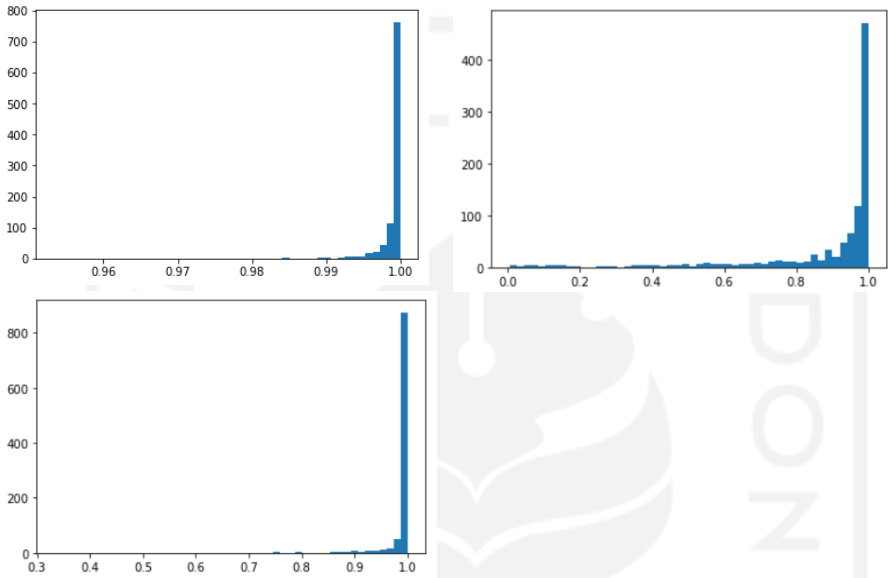
- Hasil Visualisasi Pengujian Canon EOS 750D dan Oppo Reno 6:



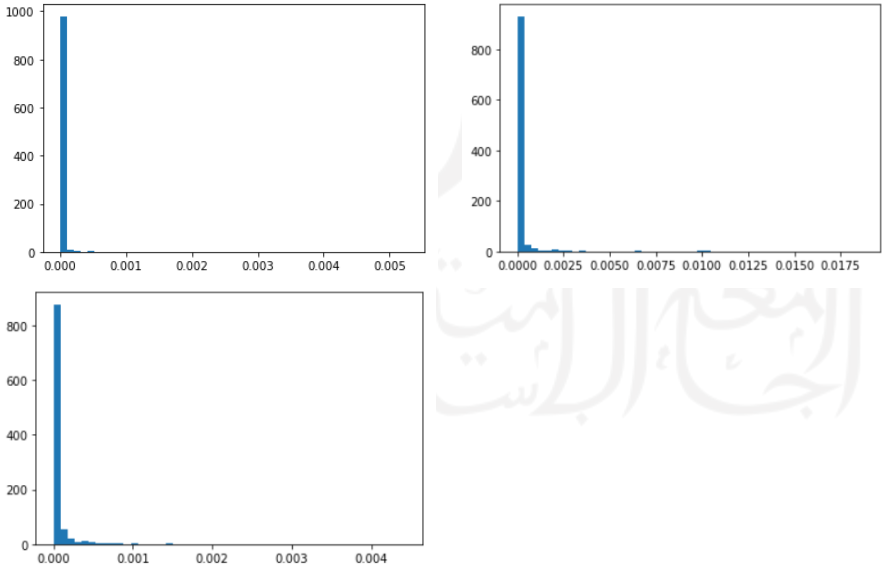




- Hasil Visualisasi Pengujian Canon EOS 750D dan Canon EOS 750D:

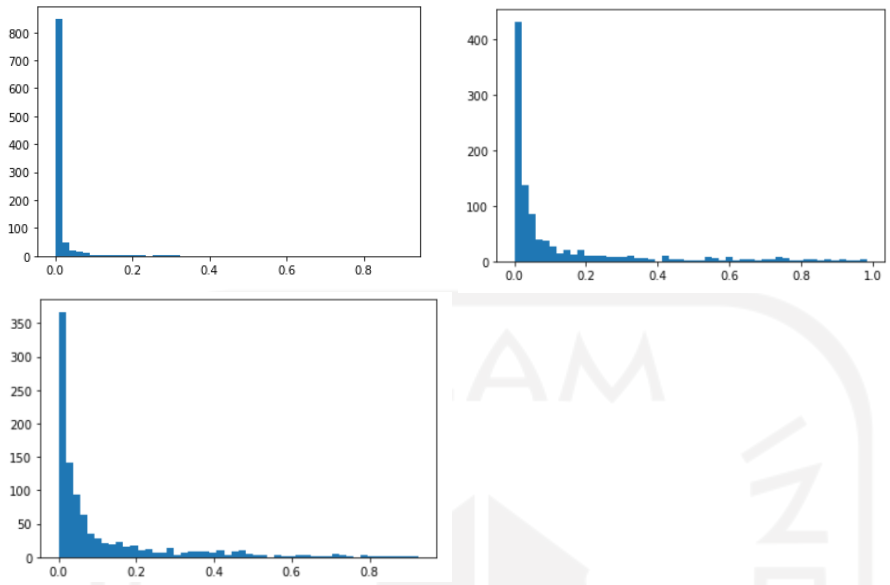


- Hasil Visualisasi Pengujian Canon EOS 750D dan Realme 9 Pro:

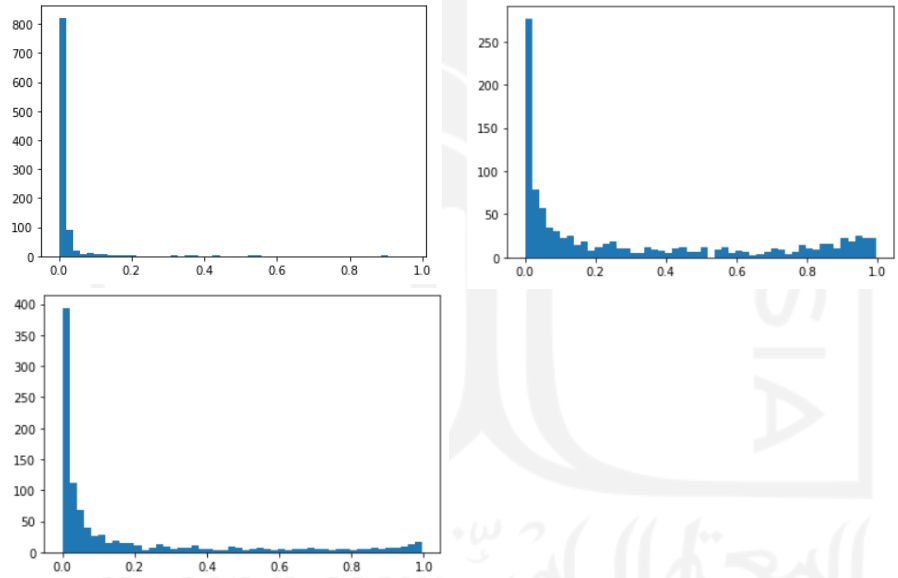


6. Gambar Acuan Realme 9 Pro:

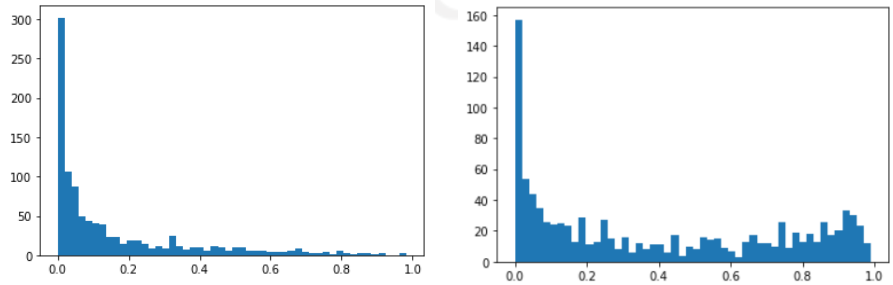
- Hasil Visualisasi Pengujian Realme 9 Pro dan Xiaomi Mi 5:

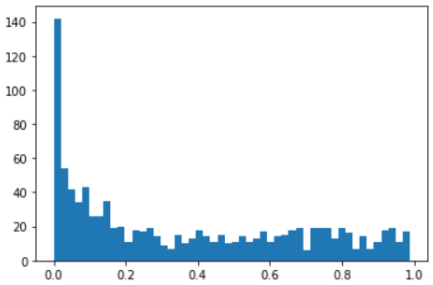


- Hasil Visualisasi Pengujian Realme 9 Pro dan Xiaomi Mi A1:

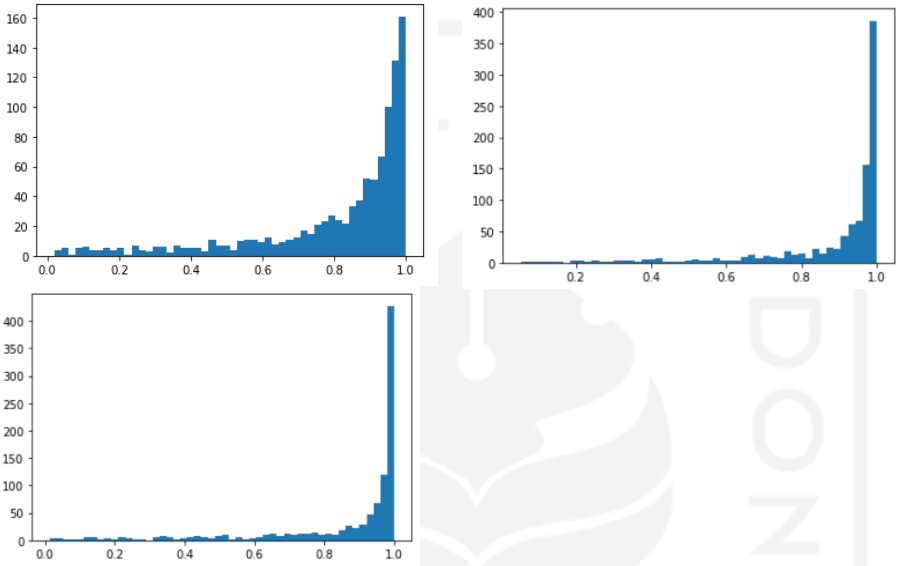


- Hasil Visualisasi Pengujian Realme 9 Pro dan Oppo F7:

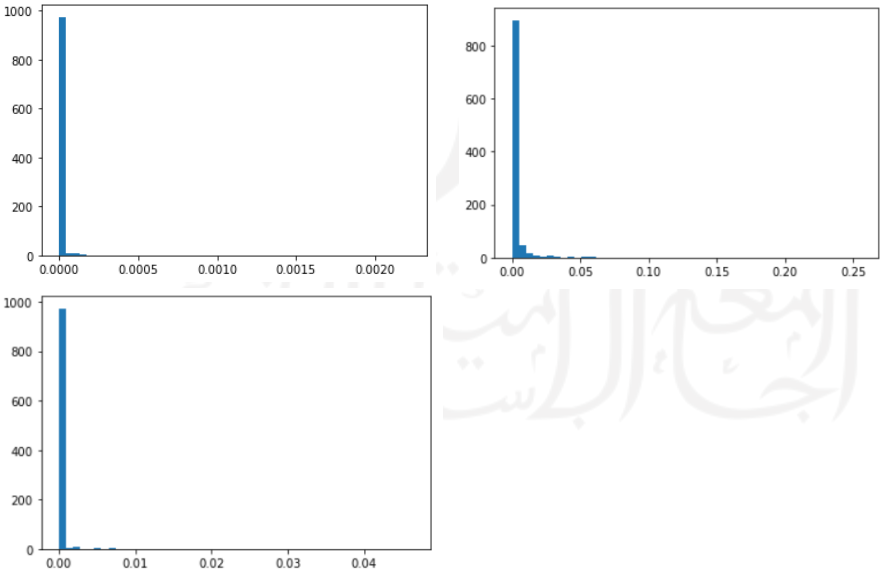




- Hasil Visualisasi Pengujian Realme 9 Pro dan Oppo Reno 6:



- Hasil Visualisasi Pengujian Realme 9 Pro dan Canon EOS 750D:



- Hasil Visualisasi Pengujian Realme 9 Pro dan Realme 9 Pro: