Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic*

Siti Kartika Munawarah

20917056

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

Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic*

Siti Kartika Munawarah
20917056

Yogyakarta, 08 Desember 2022

Pembimbing

Dr. Yudi Prayudi, S.Si., M.Kom	Erika Ramadhani, M.Eng.

Lembar Pengesahan Penguji

Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic*

Siti Kartika Munawarah

20917056

Yogyakarta, 24 Desember 2022

Tim Penguji,

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

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

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

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic*

Teknologi pencitraan yang semakin maju saat ini menimbulkan banyak permasalahan dan tantangan baru dalam menentukan realisme citra dalam citra digital. Dengan penggunaan teknologi pencitraan, dapat membuat beberapa citra digital bisa terlihat nyata (*real*) walaupun telah dilakukan pemalsuan diantara beberapa citra digital tersebut, sehingga diperlukan ilmu forensik citra. Forensik citra digital atau yang disebut sebagai *Image Forensic* merupakan salah satu bidang ilmu yang mendalami suatu penelitian yang bertujuan untuk mengumpulkan bukti-bukti yang menentukan keaslian suatu citra digital. Metode *feature detection* digunakan untuk mendeteksi titik-titik kunci (*keypoint*) yang terdapat pada suatu citra digital. Metode *feature matching* digunakan untuk menentukan *keypoint* terbaik (atau disebut sebagai *good matches*) sebagai parameter untuk mengidentifikasi persentase kemiripan suatu citra yang dibandingkan, dimana citra yang dibandingkan adalah *image* asli dan *image* rekayasa guna mendukung analisis *image forensic*. Hasil pengujian dengan menggunakan metode *feature detection* untuk kedua *image* telah diperoleh perbedaan antara jumlah *keypoint image* asli dengan jumlah *keypoint image* rekayasa. Hal ini disebabkan karena adanya gangguan citra yang terdapat pada *image* rekayasa, sehingga jumlah *keypoint* pada *image* rekayasa berbeda dengan jumlah *keypoint* pada *image* asli. Pada penerapan metode *feature matching* untuk kedua *image* telah diperoleh nilai persentase kemiripan dari kedua *image* yang diperoleh dari nilai *good matches* dibagi dengan jumlah *keypoint* dikali 100%. Dari perhitungan ini, terdapat nilai persentase kemiripan paling rendah pada *image* rekayasa – *flip*. Dari hasil fitur-fitur tersebut, terdapat perbedaan yang dapat mendukung Analisis *image forensic*. Perbedaan fitur pada sebuah *image* ini diperoleh dari perbedaan jumlah *keypoint,* selain itu perbedaan fitur ini dilakukan validasi melalui *difference* RGB dengan melihat perbedaan dari *pixel* atau elemen citra yang dimiliki oleh masing-masing citra.

Kata kunci

Citra Digital, Image Forensic, Feature Detection, Feature Matching, OpenCV

Abstract

Digital Image Similarity Detection Using Feature Detection and Feature Matching Methods To Support Image Forensic Analysis

Imaging technology that is increasingly advanced today creates many new problems and challenges in determining image realism in digital images. With the use of imaging technology, it can make some digital images look real (real) even though some of the digital images have been forged, so that image forensic science is needed. Digital image forensics or what is known as Image Forensics is a field of science that studies a research that aims to collect evidence that determines the authenticity of a digital image. Feature detection method is used to detect key points contained in a digital image. The feature matching method is used to determine the best keypoints (or known as good matches) as a parameter to identify the percentage of similarity of an image being compared, where the images being compared are original images and engineered images to support image forensic analysis. The test results using the feature detection method for both images have obtained the difference between the number of original keypoint images and the number of engineered keypoint images. This is due to the presence of image disturbance in the engineered image, so the number of keypoints in the engineered image is different from the number of keypoints in the original image. In the application of the feature matching method for the two images, the percentage similarity value of the two images has been obtained from the good matches divided by the number of keypoints multiplied by 100%. From this calculation, there is the lowest percentage similarity value in the engineered image – flip. From the results of these features, there are differences that can support image forensic analysis. The difference in features in an image is obtained from the difference in the number of keypoints. In addition, the difference in these features is validated through the difference RGB by looking at the differences in the pixels or image elements that each image has.

Keywords

Digital Image, Image Forensic, Feature Detection, Feature Matching, OpenCV

Pernyataan Keaslian Tulisan

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, 02 Februari 2023

Siti Kartika Munawarah, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Munawarah, S. K., Prayudi, Y, Ramadhani, E. 2023. Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic*. JUSTI (Jurnal Sains Terapan Teknologi Informasi), 15 (1).

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Siti Kartika Munawarah	Mendesain eksperimen (65%) Menulis *paper* (60%)
Dr. Yudi Prayudi, S.Si., M.Kom.	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (25%)
Erika Ramadhani, M.Eng.	Mendesain eksperimen (15%) Menulis dan mengedit *paper* (15%)

Halaman Kontribusi

Kontribusi dari beberapa pihak terkait dalam penyelesaian penelitian tesis ini, diantaranya:

1. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. selaku Dosen Pembimbing I yang telah memberikan bimbingan serta arahan-arahan kepada penulis, sehingga penulisan tesis ini dapat diselesaikan dengan baik.
2. Ibu Erika Ramadhani, M.Eng. selaku Dosen Pembimbing II yang telah memberikan bimbingan serta dukungan untuk menyelesaikan tahapan progress hingga peneyelsaian tesis ini.
3. Ayahanda, yang telah membiayai seluruh biaya perkuliahan dan selalu memberikan dukungan sehingga penulis dapat menyelesaikan masa studi hingga tahap penyelesaian tesis ini.
4. Serta seluruh teman-teman Angkatan FD-23 dan teman-teman di Magister Informatika UII lainnya yang telah meluangkan waktu untuk berbagi terkait tahapan penyelesaian tesis bersama penulis.

Halaman Persembahan

Bismillahirrahmanirrahim

Dengan menyebut nama Allah SWT yang Maha Pengasih dan Maha Penyayang, atas ridho Allah Subhanahu Wa Ta'ala, karya tesis ini saya persembahkan kepada:

1. Almarhumah Ibunda, semasa hidup almarhumah telah mengharapkan dan memberikan dukungan kepada penulis untuk melanjutkan pendidikan setinggi-tingginya.
2. Ayahanda, sebagai orang tua satu-satunya yang telah menemani dan mendukung proses pendidikan S2 penulis dari awal hingga akhir masa studi penulis.
3. Saudara serta keluarga besar, yang selalu memberikan dukungan kepada penulis baik dari jarak dekat ataupun jarak jauh.

Kata Pengantar

Assalamu'alaikum warahmatullahi wabarakatuh

Puji syukur kehadirat Allah Subhanahu Wa Ta'ala karena atas berkat rahmat, taufik serta hidayahnya sehingga penulis dapat menyelesaikan Laporan Tesis dengan judul "**Deteksi Kemiripan Citra Digital Menggunakan Metode *Feature Detection* dan *Feature Matching* Untuk Mendukung Analisis *Image Forensic***". Adapun maksud dari penulisan laporan tesis ini adalah sebagai persyaratan dalam mencapai jenjang pendidikan Magister Informatika dengan Konsentrasi Forensika Digital di Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta. Pada proses penyelesaian tesis ini, penulis tidak dapat menyelesaikannya bila tidak ada turut serta dari pihak lain yang juga ikut membantu baik secara langsung maupun tidak langsung dalam penyelesaian penelitian ini, oleh karena itu penulis ingin menyampaikan rasa terima kasih kepada beberapa pihak yang telah mendukung dalam menempuh dan menyelesaikan pendidikan di Universitas Islam Indonesia, antara lain:

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D, selaku Rektor Universitas Islam Indonesia yang memberikan kesempatan pada penulis untuk menempuh pendidikan serta memberikan motivasi di Universitas Islam Indonesia.
2. Bapak Prof. Dr. Ir. Heri Purnomo, MT., selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan motivasi dalam proses menempuh pendidikan di Universitas Islam Indonesia.
3. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D., selaku Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri Universitas Islam Indonesia yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku Dosen Pembimbing I yang telah banyak meluangkan waktunya dalam memberikan bimbingan serta arahan kepada penulis selama proses penyelesaian tesis ini.
5. Ibu Erika Ramadhani, M.Eng., selaku Dosen Pembimbing II yang telah memberikan masukan dan arahan untuk penulis selama proses penyelesaian tesis ini.
6. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom. dan Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., selaku Dosen Penguji yang telah memberikan komentar dan masukan terhadap tesis ini.

7. Ayahanda, Saudara, serta Keluarga Besar yang telah banyak memberikan bantuan secara moril ataupun materiil kepada penulis serta memberikan dukungan kepada penulis hingga akhirnya penulis dapat menyelesaikan masa studi.
8. Seluruh Dosen, Staff Administrasi, dan Civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama masa studi penulis.
9. Pihak SMKN 2 Tanjung Selor, yang telah memberikan izin untuk melaksanakan PJJ (Pembelajaran Jarak Jauh) selama menyelesaikan masa studi serta memberikan support kepada penulis.
10. Teman-teman Angkatan FD-23, teman-teman Magister Informatika UII, serta teman-teman lainnya yang selalu memberikan support dan meluangkan waktu untuk saling bertukar pikiran kepada penulis.
11. Serta tidak lupa untuk mengucapkan terima kasih kepada diri sendiri, karena telah mampu menyelesaikan masa studi dengan baik.

Yogyakarta, 02 Februari 2023

Hormat Saya,

Siti Kartika Munawarah, S.Kom.

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi pengolahan citra digital yang memudahkan pengguna dalam memodifikasi citra berdampak pada maraknya pemalsuan citra. Pengubahan gambar atau pemalsuan gambar dapat menimbulkan kesalahpahaman bagi orang yang melihat citra tersebut. Orang juga sulit membedakan mana gambar asli atau gambar yang sudah dimanipulasi dari gambar aslinya (Wijaya dkk, 2017). Citra adalah representasi (gambar), rupa atau tiruan dari suatu objek. Citra sebagai output suatu sistem perekaman data dapat bersifat gambar optik seperti foto, dimana foto memiliki sifat analog dengan sinyal video seperti gambar pada layar televisi, atau digital yang dapat disimpan langsung pada media penyimpanan. Suatu citra atau bayangan dapat didefinisikan sebagai fungsi dua dimensi yakni f(x, y), dimana x dan y adalah koordinat bidang, dan nilai fungsi f pada setiap pasangan koordinat (x, y) disebut intensitas atau tingkat keabuan (*grey level*) gambar dari gambar dititik itu (Harefa, 2016).

Penggunaan gambar (citra) hasil manipulasi dengan tujuan tidak baik dapat menimbulkan tindakan pemalsuan citra atau yang disebut sebagai *image forgery*. *Image forgery* atau disebut juga sebagai manipulasi citra merupakan istilah yang sering digunakan oleh beberapa orang dalam melakukan manipulasi sebuah produk digital dan menyebabkan makna yang terkandung pada sebuah citra menjadi berbeda (Endardhi dkk, 2021). Pemalsuan citra sering dilakukan dengan beberapa jenis gangguan citra atau yang disebut sebagai *image tampering*. Menurut Sharma & Abrol (2013) menjelaskan bahwa *image tampering* adalah seni digital yang membutuhkan pemahaman tentang properti gambar dan kreativitas visual yang baik. Seseorang merusak gambar karena berbagai alasan baik untuk menikmati kesenangan karya digital menciptakan foto yang luar biasa atau untuk menghasilkan bukti palsu. Apa pun penyebab tindakannya, pemalsu harus menggunakan serangkaian operasi pemrosesan gambar tunggal atau kombinasi. Berbagai teknik *image tampering* yang umum digunakan antara lain: *Copy-Move, Image-Splicing, Resize, Cropping,* dan *Noising or Blurring*.

Pemalsuan gambar terus mempengaruhi berbagai bidang seperti media sosial, fashion, obat-obatan, perawatan kesehatan, dan pengadilan pengadilan. Pemalsuan gambar digital juga dikenal sebagai manipulasi gambar (atau perusakan gambar atau manipulasi gambar) melibatkan upaya yang disengaja untuk menipu seseorang untuk mempercayai apa yang tidak benar. Ini dapat dilakukan dengan menyembunyikan objek tertentu dalam gambar yang ada atau dengan menambahkan beberapa objek yang tidak ada untuk menghadirkan gambar yang benar-benar baru. Sejumlah daerah tetap terkena masalah pemalsuan gambar, yaitu, jurnal ilmiah, ruang redaksi, mode, dan persidangan ruang sidang (Gokhale dkk, 2020). Menurut Endardhi, dkk (2021) menyebutkan bahwa salah satu kategori pemalsuan citra yang cukup popular dan sering untuk dilakukan yakni pemalsuan dengan teknik *copy-move* karena tergolong teknik pemalsuan yang cukup mudah untuk dilakukan oleh orang. *Copy-move* adalah jenis teknik perusakan gambar (*image tampering*) yang paling umum digunakan, di mana seseorang perlu menutupi sebagian gambar untuk menambah atau menghapus informasi. Daerah bertekstur digunakan sebagai bagian yang ideal untuk pemalsuan *copy-move*. Karena area bertekstur memiliki warna (*color*), rentang dinamis (*dynamic range*), sifat variasi noise (*noise variation properties*) yang serupa dengan gambar, hal itu tidak dapat dipahami oleh mata manusia yang menyelidiki ketidaksesuaian dalam sifat statistik gambar.

(a) (b) (c)

Gambar 1.1 Contoh gambar yang identik secara visual

Keterangan Gambar 1.1:

- Gambar (a) merupakan *image* asli yang telah terstandarisasi dari basis data Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California.
- Gambar (b) merupakan *image* duplikasi dari gambar (a) tanpa dilakukan manipulasi atau terdapat gangguan citra pada *image*.
- Gambar (c) merupakan *image* yang menyerupai gambar (a), namun gambar (c) telah dimanipulasi atau terdapat gangguan citra pada *image* tersebut.

Teknologi pencitraan yang semakin maju saat ini menimbulkan banyak permasalahan dan tantangan baru dalam menentukan realisme citra dalam citra digital. Dengan penggunaan teknologi pencitraan, dapat membuat beberapa citra digital bisa terlihat nyata (*real*) walaupun telah dilakukan pemalsuan diantara beberapa citra digital tersebut, sehingga diperlukan ilmu forensik citra. Forensik citra digital atau yang disebut sebagai *Image Forensic* merupakan salah satu bidang ilmu yang mendalami suatu penelitian yang bertujuan untuk mengumpulkan bukti-bukti yang menentukan keaslian suatu citra dalam citra digital.

Forensik citra digital atau disebut *Digital Image Forensic* (DIF) adalah bidang pengetahuan yang berfokus pada pemulihan dan analisis bukti digital dalam proses investigasi kriminal. DIF terutama digunakan untuk fokus pada dua masalah: identifikasi asal usul suatu gambar dan integritasnya. Mengidentifikasi asal usul gambar digital terdiri dari pengenalan aspek, misalnya model kamera yang bertanggung jawab untuk menghasilkan gambar. Untuk memverifikasi integritas gambar digital melibatkan evaluasi isi file untuk menentukan apakah telah mengalami satu atau lebih proses pemalsuan untuk menghasilkan gambar palsu (Ferreira dkk, 2020).

Metode *Feature Detection* atau disebut juga metode deteksi fitur adalah metode untuk mendeteksi sudut (*corners*) yang ada pada suatu citra. Pada tahap ini, sistem akan dapat dengan cepat dan akurat menemukan berbagai sudut dalam kondisi pencitraan yang berbeda. Tahap deteksi fitur atau *feature detection* ini akan menghasilkan detector. Selanjutnya sudut (*corners*) yang terdeteksi akan diekstraksi kuantitas sudut (*corners*) yang terdapat pada citra sehingga dapat dibandingkan dan dianalisis. Pada tahap ekstraksi ini, maka akan terbentuk vektor deskriptor (*Descriptor Vector*). Metode *Feature Matching* adalah langkah mencocokkan atau membandingkan sudut (*corners*) yang telah diekstraksi dengan lapisan data citra yang disimpan dalam database untuk menemukan kecocokan dan relasi terbaik pada citra. Jika langkah pencocokan fitur berhasil, citra dapat dikenali oleh sistem (Prathivi, 2014). OpenCV (*Open Source Computer Vision*) adalah *library* (pustaka) yang utamanya digunakan untuk pemrosesan citra komputer. OpenCV adalah library gratis yang dapat digunakan di berbagai platform, seperti GNU/Linux maupun Windows. OpenCV mulanya ditulis dalam bahasa pemrograman C++, namun saat ini OpenCV dapat digunakan pada berbagai bahasa seperti Python, Java atau MATLAB.

Berdasarkan dari penelitian sebelumnya, belum ada penelitian yang menentukan tingkat kemiripan yang terdapat pada *image* (citra) yang secara visual terlihat sama. Dan juga belum adanya analisis terhadap jejak (*trace*) yang terdapat pada fitur (*feature*) yang dimiliki masing-masing *image*, dimana fitur atau titik kunci (*keypoint*) pada sebuah *image*

dapat digunakan guna mendukung analisis *image forensic*, sehingga perlu adanya penelitian yang melakukan deteksi kemiripan citra melalui jejak (*trace*) yang ditentukan melalui fitur (*feature*) masing-masing *image* serta menentukan persentase kemiripan kedua *image*. Penentuan titik kunci (*keypoint*) pada *image* dapat mendeteksi pemalsuan antara *image* asli dan *image* rekayasa dengan melakukan validasi melalui *difference* RGB, dimana *difference* RGB digunakan untuk membandingkan nilai RGB kedua *image* (yakni *image* asli dan *image* rekayasa) dengan inisiasi nilai R=0; G=0; dan B = 0. *Difference* RGB juga digunakan untuk mendukung analisis *image forensic*, dimana *difference* RGB akan menampilkan perbedaan RGB kedua *image* jika nilai RGB yang dimiliki kedua *image* berbeda. Dengan nilai RGB yang berbeda, dapat menyimpulkan bahwa *image* yang terlihat mirip secara visual belum tentu memiliki elemen citra yang sama atau dapat disimpulkan bahwa ada proses pemalsuan citra pada salah satu image tersebut (yakni pada *image* rekayasa).

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang di atas, maka dalam penelitian ini merumuskan sebuah permasalahan tentang bagaimana menentukan fitur (*feature*) dalam mendeteksi kemiripan pada citra melalui tingkat persentase kemiripan guna untuk mendukung analisis *image forensic*?

1.3 Batasan Penelitian

Berdasarkan penjelasan latar belakang di atas, maka diperlukan batasan masalah untuk membatasi pembahasan dalam penelitian ini. Batasan masalah dalam penelitian antara lain:

1. Penelitian ini menggunakan citra digital yang telah terstandarisasi dari basis data Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California.
2. Penelitian ini melakukan penerapan metode *feature detection* dan *feature matching* untuk mendeteksi kemiripan dari kedua *image*.
3. Penerapan metode *feature detection* digunakan untuk mendeteksi titik-titik kunci atau *keypoint* dari masing-masing citra.
4. Penerapan metode *feature matching* digunakan menentukan *keypoint* terbaik (*good matches*) untuk menghasilkan persentase kemiripan citra guna mendukung analisis *image forensic*.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah dapat menentukan fitur (*feature*) dalam mendeteksi kemiripan pada citra melalui tingkat persentase kemiripan guna untuk mendukung analisis *image forensic* dengan menggunakan metode *feature detection* dan *feature matching*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah dapat membantu penyidik untuk melakukan penyidikan terkait informasi pendeteksian kemiripan citra digital melalui tingkat persentase kemiripan pada citra digital dari hasil yang diperoleh setelah dilakukan penelitian.

1.6 Sistematika Penulisan

Penelitian ini disusun dengan menggunakan sistematika penulisan yang terbagi dalam beberapa bab, yakni:

BAB I Pendahuluan

Bagian ini merupakan pendahuluan dari permasalahan penelitian yang akan dibahas, meliputi latar belakang penelitian ini, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian serta sistematika penulisan laporan penelitian.

BAB II Tinjauan Pustaka

Bagian ini membahas terkait teori-teori yang berkaitan dengan penelitian ini untuk mendukung pemecahan masalah pada penelitian ini.

BAB III Metodologi Penelitian

Bagian ini meliputi deskripsi prosedur penelitian perangkat keras (*hardware*), perangkat lunak (*software*) yang diperlukan untuk melakukan penelitian yang digunakan dalam perancangan aplikasi pendeteksi kemiripan citra digital.

BAB IV Hasil dan Pembahasan

Bagian ini berisi tentang pembahasan skenario pengujian, implementasi sistem, pengujian, serta mengAnalisis hasil pengujian sistem.

BAB V Kesimpulan dan Saran

Bagian ini memberikan kesimpulan tentang hasil penelitian yang diperoleh dan saran untuk pengembangan penelitian ini.

BAB 2
Tinjauan Pustaka

2.1 Tinjauan Pustaka

Perkembangan teknologi yang semakin pesat mendukung perkembangan dalam dunia citra digital terutama dalam perkembangan perangkat citra yang memungkinkan banyaknya perangkat citra yang memiliki resolusi tinggi dengan biaya yang rendah. Perkembangan citra digital juga dapat memudahkan masyarakat dalam mendapatkan informasi, namun kemudahan ini tidak didukung oleh keaslian sebuah informasi yang diperoleh dari citra digital tersebut. Hal ini disebabkan banyak pihak yang menyalahgunakan kondisi tersebut untuk melakukan manipulasi terhadap sebuah citra digital, sehingga masyarakat mengalami kesulitan untuk percaya terkait keaslian dari sebuah citra digital.

Pada penelitian Wijaya, dkk (2017) telah melakukan pengembanhan metode *block mathing* untuk mendeteksi *copy-move* pada pemalsuan citra, dimana pada pengembangan metode *block matching* di penelitian ini menggunakan dua pendekatan diantaranya *exact match* dan *robust match*. Untuk pendekatan *exact match* meliputi: input citra RGB, pengambilan blok, perhitungan nilai hash tiap blok, pencarian blok yang mirip dan diakhiri dengan operasi morfologi untuk penghalusan hasil deteksi. Kemudian pendekatan *robust match* hampir mirip dengan exact match namun nilai hash diubah dengan *Discrete Cosine Transform* (DCT). Dari hasil penelitian yang dilakukan dengan menggunakan 2 pendekatan tersebut diperoleh bahwa hasil pendekatan *robust match* mendapatkan hasil sedikit lebih baik dibandingkan dengan *exact match* dimana nilai rata-rata kualitas deteksi 75% dengan kualitas deteksi terbaik sebesar 97%. Namun pendekatan *robust match* membutuhkan waktu yang lebih lama, hal ini disebabkan dikarenakan kompleksitas yang cukup tinggi saat perhitungan DCT.

Kemudian Tresnaningsih, dkk (2017) melakukan deteksi pemalsuan citra copy-move menggunakan metode *Dyadic Wavelet* dan *Scale Invariant Feature Transform* (SIFT), dimana penelitian ini menggunakan citra digital yang didekomposisi menggunakan metode *Dyadic Wavelet Transform* (DyWT) dan diambil sub-citra LL, kemudian diekstraksi fitur lokal dengan metode *Scale Invariant Feature Transform* (SIFT) Hasil yang diperoleh dari penelitian ini adalah mendeteksi pemalsuan *copy-move* pada area citra berbeda yang telah mengalami beberapa perubahan pemrosesan citra diantaranya rotasi, dan skala (seperti skala diperbesar atau diperkecil). Namun terdapat kekurangan pada hasil deteksi dengan

penggunaan kedua metode tersebut, yakni false matches, dimana titik yang terdeteksi tidak tepat dengan titik *copy-move* sebenarnya.

Selain penelitian Tresnaningsih, dkk (2017), penelitian Endardhi, dkk (2021) melakukan *forensic image forgery* dengan menggunakan teknik *wavelet denoising* pada citra 2D, dimana metode algoritma yang digunakan untuk melakukan deteksi pada citra *copy-move* adalah *Discrite Wavelet Transform* (DWT). Metode algoritma *Discrite Wavelet Transform* (DWT) akan mendeteksi *noise* pada citra *copy-move* dengan menggunakan teknik *Wavelet Denoising* untuk menghasilkan blocking pada daerah citra yang telah dilakukan proses image forgery. Penelitian ini berhasil mengidentifikasi citra yang memiliki *blocking* pada daerah citra, dimana area *blocking* ini menandakan citra telah dilakukan proses *image forgery*. Namun, penelitian ini memiliki persentase pada false match yang diterapkan pada citra dengan format JPG cukup tinggi, yakni 56,25%. penelitian ini hampir mirip seperti penelitian Tresnaningsih, dkk (2017) dimana terdapat *false match* yang dapat menyebabkan terjadi kesalahan dalam mengidentifikasi citra yang termanipulasi *copy-move*.

Pada penelitian Nuari, dkk (2019) dilakukan perbandingan 2 metode untuk melakukan deteksi *image forgery* (Pemalsuan Gambar) pada citra yang termanipulasi *copy-move.* 2 Metode yang dibandingkan adalah *Speeded Up Robust Features* (SURF) dan *Scale Invariant Feature Transform* (SIFT). Metode SIFT dan SURF menggunakan beberapa jenis pengujian sebagai perbandingan kedua metode. Jenis pengujian diantaranya: tanpa transformasi, transformasi rotasi, transformasi pencahayaan, dan transformasi blur. Dari hasil pengujian pada penelitian ini disimpulkan bahwa algoritma SIFT memiliki akurasi lebih tinggi dibandingkan dengan algoritma SURF, sedangkan waktu eksekusi untuk algoritma SURF lebih cepat dibandingkan dengan algoritma SIFT, dimana diperoleh hasil selisih pada pengujian 1,2, dan 3 sebesar 1,97 detik, selisih pada pengujian 4 sebesar 0,7 detik dan selisih pada pengujian 5 sebesar 0,62 detik.

Penelitian yang dilakukan adalah bagaimana mendeteksi kemiripan suatu citra digital dengan menggunakan metode *feature detection* dan metode *feature matching* untuk mendukung analisis *image forensic*. Algoritma *Scale Invariant Feature Transform* (SIFT) merupakah salah satu algoritma yang diterapkan pada metode *feature detection* untuk mendeteksi titik-titik kunci (*keypoint*) yang terdapat pada suatu citra digital. Algoritma *Fast Library Approximated Nearest Neighbor* (FLANN) merupakah salah satu algoritma yang diterapkan pada metode *feature matching* untuk menentukan *keypoint* terbaik (atau disebut sebagai *good matches*) sebagai parameter untuk mengidentifikasi persentase kemiripan suatu citra yang dibandingkan, dimana citra yang dibandingkan adalah *image* asli dengan

image rekayasa guna mendukung analisis *image forensic*. Pengujian akan dilakukan dengan menggunakan bahasa pemrograman Python. Python memiliki *library* khusus *image processing* salah satunya adalah OpenCV (*Open Source Computer Vision*). Penelitian ini akan membangun program deteksi kemiripan citra dengan menggunakan metode *feature detection* dan metode *feature matching* untuk mendukung analisis *image forensic*.

Untuk mendukung penelitian ini, diperoleh beberapa literature review terkait penelitian ini yang diringkas pada Tabel 2.1 di bawah ini:

Tabel 2.1: *Literature Review*

Literatur	Metode Deteksi	Konsep Penerapan Metode Deteksi	Hasil Penerapan Metode
Wijaya, dkk (2017)	*Block Matching*	• Menggunakan dua pendekatan yaitu *exact match* dan *robust match*. • Pendekatan *exact match* ini meliputi: input citra RGB, pengambilan blok, perhitungan nilai *hash* tiap blok, pencarian blok yang mirip dan diakhiri dengan operasi morfologi untuk penghalusan hasil deteksi. • Pendekatan *robust match* hampir mirip dengan *exact match*, namun nilai *hash* diubah dengan *Discrete Cosine Transform* (DCT).	• Hasil pendekatan *robust match* mendapatkan hasil sedikit lebih baik dibandingkan dengan *exact match*. • Nilai rata-rata kualitas deteksi 75% dengan kualitas deteksi terbaik sebesar 97%. • Namun pendekatan *robust match* membutuhkan waktu yang lebih lama, hal ini disebabkan dikarenakan kompleksitas yang cukup tinggi saat perhitungan DCT.
Tresnaningsih, dkk (2017)	*Dyadic Wavelet* & *Scale Invariant Feature Transform* (SIFT)	• Penelitian ini menggunakan citra digital yang didekomposisi. • Menggunakan metode *Dyadic Wavelet Transform* (DyWT) dan diambil sub-citra LL. Diekstraksi fitur lokal dengan metode *Scale Invariant Feature Transform* (SIFT)	• Terdeteksi pemalsuan *copy-move* pada area citra berbeda yang telah mengalami beberapa perubahan pemrosesan citra. • Perubahan pemrosesan citra yang terjadi diantaranya rotasi, dan penyekalaan. • Terdapat *false matches*, dimana titik yang terdeteksi tidak tepat dengan titik *copy-move* sebenarnya.

Tabel 2.1: *Literature Review* (Lanjutan)

Literatur	Metode Deteksi	Konsep Penerapan Metode Deteksi	Hasil Penerapan Metode
Endardhi, dkk (2021)	*Discrite Wavelet Transform* (DWT)	• Metode algoritma *Discrite Wavelet Transform* (DWT) akan mendeteksi *noise* pada citra *copy-move*. • Menggunakan teknik *Wavelet Denoising* untuk menghasilkan *blocking* pada daerah citra yang telah dilakukan proses *image forgery*.	• Mengidentifikasi *blocking* pada daerah citra dengan menandakan citra telah dilakukan proses *image forgery*. • Namun persentase pada *false match* yang diterapkan pada citra dengan format JPG cukup tinggi, yakni 56,25%. • Hal ini dapat menyebabkan terjadi kesalahan dalam mengidentifikasi citra *copy-move*.
Sulistyo, dkk (2020)	*Speeded Up Robust Features* (SURF)	• Metode *Speeded Up Robust Features* (SURF) menerapkan beberapa parameter untuk perbandingan nilai kualitas citra untuk proses deteksi. • Parameter yang digunakan antara lain: perhitungan MSE, RMSE, dan PSNR.	• Nilai PSNR lebih tinggi, sehingga memiliki kualitas yang bagus, • Namun hal tersebut dinyatakan termasuk manipulasi citra.
Purwandari, dkk (2019)	*Discrete Cosine Transform* (DCT) dan *Scale Invariant Feature Transform* (SIFT)	-	• Membuat aplikasi pendeteksi pemalsuan citra dengan menggunakan metode DCT dan SIFT. • Aplikasi pendeteksi kerusakan pemasangan gambar ini berhasil memeriksa gambar dengan 100% data internet, memeriksa gambar dengan 100% data yang dikumpulkan secara pribadi. • Aplikasi ini lebih cepat untuk gambar dengan ukuran piksel lebih besar dibandingkan dengan gambar dengan ukuran piksel kecil.

Tabel 2.1: *Literature Review* (Lanjutan)

Literatur	Metode Deteksi	Konsep Penerapan Metode Deteksi	Hasil Penerapan Metode
Lionnie, dkk (2018)	*Speeded Up Robust Features (SURF) & Scale Invariant Feature Transform (SIFT)*	• Menggunakan metode SIFT dan SURF untuk mendapatkan kecocokan deteksi dengan hasil pemrosesan yang cepat.	• Metode SIFT menghasilkan kecocokan dua kali lebih cocok untuk mendeteksi gambar termanipulasi jenis penyerangan copy-move forgery. • Metode SURF diperoleh dua kali lebih cepat dibandingkan SIFT yakni 0.33 kali.
Rosidin, dkk (2018)	*Speeded Up Robust Features (SURF) & Histogram Color RGB*	• Memperoleh banyaknya jumlah keypoint pada citra digital, • Menggunakan parameter tambahan lainnya. • Parameter tambahan lainnya adalah: perbandingan jumlah piksel pada citra yang dianalisis, serta perubahan histrogram warna RGB pada setiap citra dianalisis.	• Hasil pengujian pada penelitian ini menggunakan algoritma SIFT (Scale Invariant Feature Transform) telah menghasilkan analisis citra yang lebih baik.
Nuari, dkk (2019)	*Speeded Up Robust Features (SURF) & Scale Invariant Feature Transform (SIFT)*	• Metode SIFT dan SURF menerapkan beberapa pengujian untuk perbandingan kedua metode. • Jenis pengujian diantaranya: tanpa transformasi, transformasi rotasi, transformasi pencahayaan, dan transformasi blur.	• Disimpulkan algoritma SIFT memiliki akurasi lebih tinggi dibandingkan dengan algoritma SURF. • Waktu eksekusi untuk algoritma SURF lebih cepat dibandingkan dengan algoritma SIFT.
Siahaan (2017)	*Frei-Chan dan Laplacian*	• Citra tidak ada gangguan citra seperti copy-move • Hanya mendeteksi tepi menggunakan algoritma frei-chan dan Laplacian.	• Deteksi tepi memisahkan antara objek dengan latar belakang sehingga menghasilkan objek yang sesuai dengan citra asli. • Namun penelitian ini hanya memberikan tampilan hasil deteksi tepi, tanpa ada deskripsi keterangan tentang titik tepi yang dihasilkan.

Tabel 2.1: *Literature Review* (Lanjutan)

Literatur	Metode Deteksi	Konsep Penerapan Metode Deteksi	Hasil Penerapan Metode
Penelitian yang diusulkan	*Feature Detection, Feature Matching*	• Metode *Feature Detection* akan menggunakan algoritma *Scale Invariant Feature* (SIFT) untuk penentuan titik-titik kunci (*Keypoint*) masing-masing citra. • Metode *Feature Matching* akan menggunakan *Fast Library Approximated Nearest Neighbor* untuk menentukan *keypoint* terbaik (*good matches*) guna sebagai parameter untuk menentukan persentase kemiripan kedua citra.	• Menghasilkan titik-titik kunci (*keypoint*) pada masing-masing citra (yakni *image* asli dan *image* rekayasa) • Menghasilkan *keypoint* terbaik (*good matches*) • Mengidentifikasi persentase kemiripan citra digital untuk mendukung analisis *image forensic.*

2.2 Citra Digital

Citra adalah representasi (gambar), rupa atau tiruan dari suatu objek. Citra sebagai output suatu sistem perekaman data dapat bersifat gambar optik seperti foto, dimana foto memiliki sifat analog dengan sinyal video seperti gambar pada layar televisi, atau digital yang dapat disimpan langsung pada media penyimpanan. Suatu citra atau bayangan dapat didefinisikan sebagai fungsi dua dimensi yakni f(x, y), dimana x dan y adalah koordinat bidang, dan nilai fungsi f pada setiap pasangan koordinat (x, y) disebut intensitas atau tingkat keabuan (*grey level*) gambar dari gambar dititik itu (Harefa, 2016).

Menurut Sinaga (2017) menjelaskan bahwa citra yang diambil oleh kamera dan telah dikuantisasi sebagai nilai diskrit disebut citra digital. Foto yang dicetak dari printer tidak bisa disebut foto digital, tetapi foto yang disimpan dalam format JPG, PNG, dan file gambar format lain di komputer bisa disebut foto digital. Menurut Sunardi, dkk (2017) juga menyebutkan bahwa citra yang diambil dengan kamera akan menghasilkan gambar persis sesuai dengan keadaan objek.

Salomon & Motta (2010) menjelaskan bahwa citra digital atau disebut gambar digital adalah matriks persegi panjangan yang terdiri dari titik-titik yang disebut elemen gambar (piksel) yang disusun dalm M baris dan N kolom. Resolusi gambar digital adalah M kali N.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix} \quad \ldots (2.1)$$

Menurut Van (2009) menyebutkan bahwa sebuah citra digital *grayscale* yang disebut juga *monochrome* terdiri dari nilai antara 0 hingga 255 dan setiap piksel diwakili oleh 1 *byte*, sedangkan pada citra digital *full color*, setiap piksel diwakili oleh 3 warna yang berbeda, yaitu merah (*red*), hijau (*green*), dan biru (*blue*). Setiap warna memiliki nilai antara 0 sampai dengan 255 dan setiap piksel direpresentasikan dalam 3 byte untuk 3 warna tersebut.

2.3 Resolusi Gambar

Resolusi citra merupakan tingkatan detail pada suatu citra, dimana semakin tinggi resolusi yang dimiliki suatu citra maka akan semakin tinggi tingkat detail dari citra tersebut. Menurut Sutoyo (2009) menjelaskan bahwa terdapat dua jenis resolusi yang perlu diketahui, yakni:

1) Resolusi Spasial merupakan ukuran halus atau kasarnya pembagian kisi-kisi baris dan kolom pada saat pengambilan contoh (*sampling*). Resolusi ini digunakan untuk menentukan jumlah pixel per satuan panjang. Satuan yang umum digunakan pada resolusi spasial adalah dpi (*dots per inch*). Resolusi memiliki pengaruh pada detail serta perhitungan gambar.
2) Resolusi kecemerlangan (intensitas / *brightness*) atau kedalaman bit atau juga bida disebut juga sebagai kedalaman warna (*Bit Depth*) merupakan suatu ukuran halus kasarnya pembagian tingkat gradasi pada warna saat dilakukan kuantisasi. *Bit Depth* ini menentukan jumlah banyak informasi warna yang tersedia untuk ditampilkan dalam setiap piksel. Nilai Bit Depth ini memiliki pengaruh terhadap kualitas gambar, dimana semakin besar nilai bit depth, maka akan semakin bagus kualitas gambar yang dihasilkan serta ukurannya juga semakin besar. Setiap piksel yang dimiliki oleh citra warna ini mewakili warna yang merupakan kombinasi dari tiga warna dasar (RGB = *Red Green Blue*).

2.4 Elemen Citra (*Pixel*)

Pixel merupakan singkatan dari *picture element* atau elemen citra (Salomon & Motta, 2010). Umumnya, orang mengetahui *pixel* sebagai persegi yang sangat kecil. Hal tersebut memang benar untuk layar monitor pada komputer. Tetapi *pixel* perangkat *output* digital lain, seperti printer, dapat berupa persegi ataupun lingkaran. Pada akhirnya, dapat dikatakan bahwa *pixel* adalah sebuah titik matematis yang tak berdimensi (Salomon & Motta, 2010).

Dalam proses gambar digital, unit gambar terkecil yang biasanya direpresentasikan dalam bentuk titik atau kotak kecil adalah piksel, dimana tiap-tiap piksel memiliki alamat masing-masing yang berbeda antara piksel yang satu dengan yang lain. Alamat piksel tersebut berkaitan erat dengan titik koordinasinya yang biasanya disusun berdasarkan pada *grid* (tabulasi) 2 dimensi. Masing-masing piksel memiliki intensitas warna sesuai dengan gambar yang diwakilinya. Intensitas warna piksel ini biasanya diwakili dalam sistem 3 komponen warna, yaitu merah (*red*), hijau (*green*), dan biru (*blue*) (Al-Azhar, 2012).

Semakin tinggi kualitas piksel yang digunakan, maka akan semakin banyak *space* dari media penyimpanan dari suatu kamera digital yang digunakan. Hal ini akan berdampak pada semakin sedikit jumlah gambar digital yang dapat disimpan di media tersebut. Untuk itu, pemilihan kualitas piksel haruslah disesuaikan dengan kebutuhan dan kapasitas dari media penyimpan itu sendiri.

Di samping itu, juga diketahui bahwa semakin banyak jumlah total piksel yang menyusun suatu gambar digital akan semakin tinggi kualitasnya, sebaliknya semakin rendah jumlah total piksel, maka semakin rendah kualitas dari gambar digital tersebut. Efek dari jumlah total piksel yang tinggi adalah ketika dilakukan proses pembesaran (*zoom in*) terhadap suatu gambar digital, maka hasil pembesaran tersebut pada beberapa tahapan masih tampak jelas dan tidak kabur (*blurred*). Hal ini tidak dapat dilakukan terhadap gambar digital dengan jumlah total piksel yang rendah.

Banyaknya piksel yang menyusun suatu gambar digital dapat juga diketahui melalui satuan dpi, yaitu *dots per inch*, artinya dalam satu inchi ada berapa banyak piksel yang ada. Jika diketahui suatu gambar digital tersusun atas 300 dpi, maka itu artinya dalam setiap inchi terdapat 300 titik piksel yang menyusun gambar tersebut. Semakin tinggi nilai dpi, maka kualitas gambar digital tersebut akan semakin baik dan jelas (Al-Azhar, 2012).

2.5 Format Gambar

Format gambar atau grafik memiliki banyak tipe format file yang umum digunakan, namun karena perkembangan teknologi yang cukup pesat sehingga tidak semua digunakan. Berikut adalah beberapa tipe format gambar yang umum digunakan, antara lain:

2.5.1 JPG / JPEG (*Joint Photographic Expert Group*)

Format file JPEG merupakan format file grafis yang sangat terkenal di dunia grafis. Umumnya format ini digunakan pada teknologi kamera digital mengingat kamera digital dapat menciptakan foto dengan kombinasi warna serta kontras. Namun, format ini tidak sesuai untuk rasio aspek, dikarenakan kontras yang tajam antara piksel yang bersebelahan

bisa dengan jelas menampilkan artefak piksel. Cukup banyak ruang warna yang dapat digunakan dalam format ini, ialah RGB (*Red Green Blue*), CMYK (*Cyan Magenta Yellow Key*) serta *Grayscale*. Selain itu, format ini juga dapat memakai *alpha channel*. Format JPEG terbuat dengan dimensi file yang tidak sangat besar, sebab format ini umumnya digunakan untuk mempublikasikan foto pada fitur elektronik dan juga digunakan untuk menaruh foto yang dapat dilihat di halaman website.

2.5.2 GIF (*Graphic Interchange Format*)

Format GIF merupakan salah satu format grafik yang memiliki ukuran yang cukup kecil dan sederhana. Format file ini juga memiliki kombinasi warna yang terbatas dibandingkan dengan format grafik lainnya. Hal ini dikarenakan format GIF hanya mendukung 256 warna sehingga tidak cocok untuk gambar atau objek foto dengan lapisan warna yang kompleks serta format GIF ini juga memiliki kedalaman bit sebesar 8 bit saja. Format GIF juga hanya mendukung mode warna *Grayscale*, *Bitmap* dan *Indexed Color*. Namun format ini memiliki kelebihan yaitu format GIF dapat digunakan untuk animasi grafis dua dimensi sederhana serta dapat menggunakan *transparency masking*. Desainer grafis biasanya menggunakan format file ini untuk animasi spanduk sederhana di web karena sangat kecil dan tidak membebani situs.

2.5.3 PNG (*Portable Network Graphic*)

Format file PNG merupakan format pengembangan dari format file GIF. Format PNG ini mempunyai keuntungan lain dibandingkan dengan format GIF yakni memiliki kemampuan untuk menyimpan file dengan *bit depth* hingga 48 bit *truecolor*. Format ini dapat menciptakan latar belakang yang transparan dengan meminimalkan efek bergerigi di sudut gambar/*image*, sehingga menghasilkan gambar/*image* dengan sudut yang lebih halus. Selain itu, format PNG juga mendukung penggunaan *alpha channel*, *gamma*, metadata, dan tampilan gambar yang lebih progresif. Format ini digunakan untuk menampilkan objek pada website. Selain itu, format PNG juga dapat digunakan untuk aplikasi lain misalkan pemanfaatan latar belakang atau *background* transparan pada objek gambar yang dapat digunakan dalam image di dalam aplikasi office.

2.5.4 TIFF (*Tagged Image Format File*)

Salah satu tipe format file gambar atau grafik lainnya adalah TIFF (*Tagged Image Format File*), dimana format file ini kemungkinan sangat jarang di dengar oleh pengguna awam. Namun, format file ini sudah cukup terkenal dan sering dipakai oleh para profesional di dunia industri cetak. Format TIFF memiliki kualitas yang cukup sangat tinggi. Selain itu

juga format file ini sering digunakan oleh para fotografer profesional karena kelebihan yang dimiliki oleh format TIFF. Kelebihan yang dimiliki oleh format TIFF adalah dapat menggunakan *clipping path* dan vektor serta file format TIFF ini juga dapat diedit dan disimpan menghilangkan kualitas gambar. File ini memiliki kedalaman warna atau disebut sebagai *depth color* sampai 32 bit dengan mode CMYK dan 24 bit RGB. Namun, format ini memiliki kekurangan yakni ukuran file yang cukup besar sehingga pengolahan gambar di website dengan format ini tidak disarankan.

2.5.5 BMP (*Bitmap Image*)

Format BMP (*Bitmap Image*) adalah format gambar/image yang umum digunakan dalam aplikasi pencitraan 2D atau *image* 2 dimensi. Beberapa sistem operasi menggunakan format ini untuk menggunakan gambar. Format BMP merupakan format yang sangat umum digunakan untuk melakukan pengeditan gambar dasar. Pada perkembangannya format BMP ini memiliki ukuran file yang cukup besar, karena tidak ada kompresi dalam pengolahannya. Format BMP sangat fleksibel dan dapat dibaca oleh pengolah gambar manapun dan dapat menyimpan kedalaman warna mulai dari 1 bit hingga 24 bit. Format file ini dapat menangani gambar/image dalam mode warna RGB, *Grayscale*, *Indexed Color*, dan Bitmap. Namun, sayangnya format BMP memiliki kekurangan yakni tidak dapat mengaplikasikan *alpha channel* dalam pemrosesannya. Biasanya format ini digunakan dalam pembuatan wallpaper dalam sistem informasi dengan tingkat kompleksitas yang sederhana.

2.5.6 RAW

RAW adalah format gambar yang sangat terkenal di kalangan para fotografer profesional dan seniman digital. RAW merupakan format gambar mentah yang dihasilkan dari sebuah penerima gambar elektronik seperti kamera digital. File gambar RAW adalah file murni dengan kualitas yang sangat tinggi dibandingkan dengan format file lainnya. Format file RAW memiliki tingkatan pencocokan warna yang sangat tinggi dan memiliki kehalusan gambar yang cukup tinggi. RAW dapat melakukan ekstraksi kualitas gambar yang maksimal. RAW dapat menggunakan pengaturan kontras image, *brightness*, *democaising*, serta koreksi gamma yang digunakan untuk menghasilkan nilai piksel. Namun, format RAW memiliki beberapa kekurangan yakni ukuran file yang cukup besar dibandingkan dengan format gambar lainnya. Selain itu tidak semua perangkat lunak atau *software* dapat menerima format ini sehingga jika pengguna ingin melakukan pemrosesan gambar akan membutuhkan tahapan yang lebih lama dibandingkan mengolah gambar dengan format yang lainnya.

2.6 *Digital Image Forensics*

Image Forensic atau dikenal sebagai forensic citra merupakan cabang dari forensic digital yang bertujuan untuk memperoleh fakta-fakta yang sulit untuk ditentukan keaslian atau perubahan suatu citra. Bidang forensic citra mendukung lembaga penegak hukum untuk menangani kasus-kasus yang berkaitan dengan gambar atau foto (Riadi, Yudhana & Sulistyo, 2019). Verifikasi keaslian file gambar atau foto dapat menggunakan sejumlah teknik forensik untuk pembuktian dan pemeriksaan terhadap foto tersebut dengan menggunakan alat dan teknik fotografi (Irwansyah & Yudiastuti, 2019).

Menurut Ferreira, dkk (2020) menjelaskan bahwa forensik citra digital atau disebut juga dengan *Digital Image Forensics* (DIF) adalah bidang ilmu yang berfokus pada penggunaan dan analisis bukti digital dalam investigasi kriminal. DIF sebagian besar digunakan untuk fokus pada dua hal, yakni identifikasi asal gambar beserta intergritasnya. Identifikasi asal gambar digital terdiri dari mengidentifikasi aspek-aspek seperti model kamera yang digunakan untuk menghasilkan gambar. Kemudian verifikasi intergritas gambar digital melibatkan evaluasi isi file untuk menentukan apakah telah dirusak oleh satu atau lebih proses palsu untuk menghasilkan gambar palsu.

Deteksi pemalsuan pada gambar bekerja dalam dua cara utama yakni mencari pola yang seharusnya tidak ada atau mencari kesalahan di tempat yang seharusnya seperti contoh jika menyambungkan objek dari satu gambar ke gambar lain dan mengubah ukurannya sehingga diskalakan ke ukuran yang sama dengan gambar target, maka akan ada perubahan dari penyambungan objek pada kedua gambar tersebut. Perubahan tersebut merupakan perubahan ukuran yang menciptakan pola korelasi antara piksel yang seharusnya tidak ada. Gambar target memiliki beberapa pola seperti CFA (*Color Filter Array*), warna pencahayaan (iluminasi) dan lain-lain.

Kecanggihan saat ini pada forensik citra digital menyediakan alat dan teknik untuk analisis forensik. Schetinger, dkk (2016) mengembangkan penyelidikan dengan pendekatan yang paling relevan dan kemampuan dalam hal penerapan (yaitu kapan bisa menggunakannya) dan penilaian (yaitu tingkat yang bisa dicapai dalam skala FD (*Forgery Detection*)). Secara umum, dapat dikatakan bahwa terdapat *trade-off* antara generalitas dan tingkat FD yang dapat dicapai oleh dengan teknologi tersebut dan bersifat intuitif karena semakin tinggi level pada skala, maka akan semakin spesifik penilaiannya. FD1 dapat disederhanakan sebagai pernyataan boolean (gambar asli atau palsu), sedangkan dari FD2 dan seterusnya, ada besar kemungkinan merupakan kombinasi piksel yang berbeda dalam

foto. Pada FD3, untuk mengidentifikasi sifat pemalsuan pada gambar perlu teknik yang dapat mencari fitur yang lebih spesifik.

Menurut Schetinger, dkk (2016) bahwa alat forensik gambar (*image forensic*) umumnya dirancang dengan mempertimbangkan tiga hal berikut, antara lain:

1) Beberapa jejak (*trace*) pada gambar kemungkinan diperkenalkan oleh proses pemalsuan, kemudian diidentifikasi terkait jejak tersebut. Jejak tersebut dapat berupa informasi tingkat pemandangan seperti pencahayaan gambar (iluminasi), atau tingkat sinyal, seperti pola larik filter warna (CFA).
2) Jejak ini diukur dan dikuantifikasi dengan cara tertentu dengan menghasilkan fitur yang biasanya bersifat numerik.
3) Melakukan analisis melalui eksperimen bagaimana himpunan fitur berperilaku pada gambar asli dan palsu, kemudian sebuah keputusan diambil tentang gambar. Hal ini dapat dilakukan dengan menggunakan sederhana ambang batas atau teknik pembelajaran mesin yang canggih.

Jejak yang digunakan adalah iluminan atau sumber cahaya. Pengamatan utama adalah bahwa jika suatu objek disambung dan gambar asli memiliki kondisi cahaya yang berbeda, seperti di dalam ruangan atau pencahayaan luar ruangan, atau bahkan lampu pijar ataupun lampu neon, jejak ini dapat digunakan untuk identifikasi. Fitur yang digunakan adalah perkiraan warna iluminan dan intensitas cahaya di bagian tepi, untuk wilayah gambar yang dianalisis berbeda. Keputusan proses menggunakan *Support Vector Machine* (SVM) untuk mengklasifikasikan gambar sebagai disambung (FD3) atau tidak meyakinkan (FD0) berdasarkan fitur-fitur. Klasifikasi alat forensik didasarkan pada jejak mereka menganalisis. Piva (2013) membedakan antara jejak yang ditinggalkan oleh tiga langkah yang berbeda dari proses pembentukan gambar: akuisisi, pengkodean dan pengeditan. Klasifikasi intuitif lainnya yang dikemukakan oleh Farid (2009) dimana teknik forensik berada dikelompokkan ke dalam lima kategori utama: berbasis piksel, berbasis format, berbasis kamera, berbasis fisik dan berbasis geometris. Menurut Farid (2009) melakukan klasifikasi lebih umum dalam literatur dan membedakan antara jejak dengan lebih baik, tetapi Piva (2013) dapat terkait erat ke skala FD. Menurut Farid (2009) memberikan usulan terkait klasifikasi berdasarkan Piva (2013) pendekatan, tetapi dengan spesifisitas yang lebih besar, mirip dengan milik Farid (2009). Jejak dan alat koresponden yang paling relevan dikembangkan oleh komunitas forensik akan dibahas berikut ini ayat. Skala FD akan digunakan untuk menggambarkan level mana penilaian dapat diharapkan ketika memeriksa gambar menggunakan alat tertentu.

Schetinger dkk (2016) mengusulkan skala klasifikasi umum baru yang disebut FD (kependekan dari *Forgery Detection Scale*). Skala ini didasarkan dalam konsep gambar asli atau tidak. Gambar asli adalah gambar yang ditangkap oleh perangkat dan kemudian dikeluarkan ke pengguna "apa adanya". Secara konseptual, ini mudah dilakukan mendefinisikan, tapi secara teknis mungkin ada beberapa komplikasi: perangkat yang berbeda memproses gambar secara berbeda.

Skala FD mengurutkan teknik forensik berdasarkan jenisnya bukti yang dapat diberikan tentang keaslian sebuah gambar. Berikut ini adalah berbagai tingkat skala Deteksi Forensik yang dikembangkan oleh Schetinger dkk (2016) :

FD0 Tidak ada bukti yang dapat ditemukan bahwa gambar tersebut bukan asli.

FD1 Gambar telah mengalami beberapa bentuk perubahan dari sumber asalnya, tetapi sifat dan lokasinya tidak diketahui.

FD2 Citra telah mengalami beberapa bentuk perubahan dari keadaan asalnya dan lokasi perubahannya ditentukan, tetapi sifatnya tidak diketahui.

FD3 Gambar telah mengalami beberapa perubahan dari keadaan aslinya, lokasi perubahannya kemungkinan telah ditentukan dan diketahui sifatnya.

FD4 Semua kesimpulan dari item sebelumnya, dan khususnya alat atau teknik dapat dikaitkan dengan pemalsuan.

2.6.1 FD1 – *Nativity* (Kelahiran)

Tingkat FD1 berbeda dari kasus negatif FD0 dikarenakan ada kemungkinan bahwa gambar tersebut bukan asli. Hal ini disebabkan bukan karena penilaian yang sedernahan, namun karena kebanyakan kamera modern memiliki pemrosesan yang terdiri dari beberapa operasi (*demosicing*, keseimbangan warna, dan lain-lain) serta pengubahan gambar yang sebelumnya telah dilakukan. Selain itu, *demosaicing* adalah operasi yang sangat mendasar di kamera modern yang tidak dapat dimengerti dan dipahami. Menurut Schetinger dkk (2016) mengusulkan segala bentuk pra-pemrosesan pada gambar hingga satu kompresi dapat diterima tanpa melanggar keaslian gambar. Sebuah teknik forensik mencapai FD1 ketika dapat menemukan bukti perubahan pada gambar. Teknik yang menganalisis informasi EXIF gambar adalah dapat mendeteksi inkonsistensi dalam metadata yang membuktikan bahwa suatu gambar bukan asli, tetapi tidak ada yang bisa dikatakan tentang lokasi atau sifat perubahan.

2.6.2 FD2 – *Location* (Lokasi)

Tingkat FD2 diperoleh ketika lokasi umum perubahan pada gambar diketahui. Ada kemungkinan bahwa wilayah gambar telah dihapus oleh serangkaian operasi seperti *copy-paste* dan kemudian diperbaiki dengan sikat penghalus (*brush*). Pada bagian ini batas-batas pemalsuan mungkin tidak sama jernih. Jika suatu teknik dapat memperoleh segala bentuk spesifisitas pada wilayah yang diubah, FD2 tercapai. Hal ini adalah kasus ketika menganalisis jejak seperti PRNU (*Photo-Response Non-Uniformity*), CFA (*Color Filter Array*) atau ELA (*Error Level Analysis*), yang disusun secara lokal di gambar. Jika bukti adanya perubahan global pada gambar tersebut ditemukan, seperti median atau bilateral filtering, lalu lokasinya pemalsuan adalah keseluruhan gambar. Demikian pula operasi yang menghapus bagian dari gambar seperti ukiran jahitan dan pemotongan dapat dideteksi tetapi area yang diubah sebenarnya tidak ada di menganalisis gambar lagi. Dikatakan bahwa pemalsuan lokasi dapat dianggap semua gambar, mencapai FD2.

2.6.3 FD3 – *Nature* (Alam)

Sifat pemalsuan dapat bersifat subjektif karena tidak dapat melakukan prediksi pada semua cara dimana sebuah gambar dapat dibuat serta diubah. Bentuk pemalsuan yang paling sering dipelajari adalah sebagai penyambungan, penyalinan, dan penghapusan, hanyalah sebagian dari kemungkinan. Gambar teknik komposisi mampu mengubah bentuk, tekstur dan orientasi objek, dan bahkan menggabungkannya menjadi satu. Untuk kesederhanaan, informasi yang berarti selain lokasi pemrosesan yang dapat digunakan untuk membantu analis forensik dapat dianggap FD3. Jika suatu benda telah diputar dan diskalakan, maka mengidentifikasi salah satu dari operasi ini memberikan tingkat FD3 pada skala mengidentifikasi objek yang disambung bernilai FD3 skala karena gambar tidak asli (FD1), lokasinya pada gambar target jelas (FD2), dan sifat dari perubahan diketahui (FD3).

2.6.4 FD4 – *Technique* (Teknik)

Level tertinggi pada skala FD yang dikembangkan oleh Schetinger dkk (2016), FD4 dicapai saat analis menemukan bukti yang dapat menghubungkan pemalsuan itu dengan yang tertentu teknik atau alat. Penyambungan dapat dilakukan hanya dengan memotong suatu wilayah dari gambar yang menempel di atas yang lain, tetapi ada juga cara canggih untuk memadukannya, seperti *Alpha Matting* atau Kloning Tanpa Batas. Sebuah teknik forensik yang mampu setelah mendapatkan FD3, memberikan wawasan lebih lanjut tentang teknik tersebut atau alat yang digunakan untuk melakukan pemalsuan mencapai FD4.

2.7 *Image Tampering*

Menurut Sharma & Abrol (2013) menjelaskan bahwa *image tampering* adalah seni digital yang membutuhkan pemahaman tentang properti gambar dan kreativitas visual yang baik. Seseorang merusak gambar karena berbagai alasan baik untuk menikmati kesenangan karya digital menciptakan foto yang luar biasa atau untuk menghasilkan bukti palsu. Apa pun penyebab tindakannya, pemalsu harus menggunakan serangkaian operasi pemrosesan gambar tunggal atau kombinasi. Berbagai teknik *image tampering* yang umum digunakan antara lain:

1) *Copy-Move*; adalah jenis teknik perusakan gambar yang paling umum digunakan, di mana seseorang perlu menutupi sebagian gambar untuk menambah atau menghapus informasi. Daerah bertekstur digunakan sebagai bagian yang ideal untuk pemalsuan *copy-move*. Karena area bertekstur memiliki warna (*color*), rentang dinamis (*dynamic range*), sifat variasi noise (*noise variation properties*) yang serupa dengan gambar, hal itu tidak dapat dipahami oleh mata manusia yang menyelidiki ketidaksesuaian dalam sifat statistik gambar.

Gambar 2.1: Contoh *Copy-Move Forgery*

2) *Image-Splicing*; disebut sebagai *paste-up* yang dihasilkan dengan menempelkan gambar-gambar fotografi. Sementara istilah *photomontage* pertama kali digunakan untuk merujuk pada suatu bentuk seni atau tindakan menciptakan foto komposit dapat ditelusuri kembali ke masa penemuan kamera.
3) *Resize*; Operasi ini melakukan transformasi geometris yang dapat digunakan untuk mengecilkan atau memperbesar ukuran suatu gambar atau bagian dari suatu gambar. Reduksi citra dilakukan dengan melakukan interpolasi antar nilai piksel pada lingkungan lokal.
4) *Cropping*; Ini adalah teknik untuk memotong batas gambar atau mengurangi kanvas tempat gambar ditampilkan. Umumnya operasi semacam ini digunakan untuk menghilangkan informasi perbatasan yang tidak terlalu penting untuk ditampilkan.

5) *Noising or Blurring*; Merusak gambar dengan operasi yang dijelaskan di atas seperti penyambungan gambar, penskalaan, rotasi dapat menjadi jelas bagi pemirsa dalam bentuk artefak seperti tepi yang tidak tepat, cacat aliasing, dan variasi nada. Jejak gangguan yang jelas ini dapat dibuat tidak terlihat dengan menerapkan sedikit noise atau operasi blur di bagian di mana cacat gangguan terlihat.

2.8 Operasi Pengolahan Citra

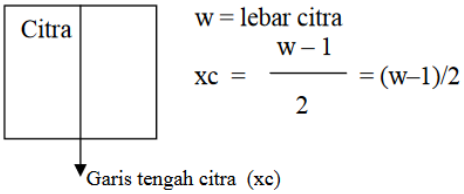
Citra digital direpresentasikan dengan matriks sehingga operasi pada citra digital pada dasarnya memanipulasi elemen-elemen matriks. Operasi dasar pengolahan citra salah satunya adalah operasi geometri. Operasi geometri pada pengolahan citra ditujukan untuk memodifikasi koordinat piksel dalam suatu citra dengan pendekatan tertentu, tetapi dalam perkembangannya dimungkinkan juga memodifikasi nilai skala. Operasi geometri berhubungan dengan perubahan bentuk geometri citra, antara lain:

2.8.1 Pencerminan (*Flipping*)

Operasi pencerminan (*flipping*) merupakan opeerasi transformasi geometri yang memindahkan titik koordinat. Efek pencerminan yang umum digunakan adalah pencerminan pada sumbu Y (*Flipping Horizontal*) dan pencerminan pada sumbu X (*Flipping Vertical*). Rumus yang digunakan pada *flipping horizontal* adalah sebagai berikut:

$$x' = -x$$

Karena koordinat asal (x) bernilai nol atau positif, maka koordinat hasil (x') yang diperoleh dari rumus akan selalu bernilai nol atau negatif, sedangkan koordinat piksel citra tidak ada (tidak boleh) negatif. Rumus dimodifikasi menjadi:



x' – xc = –(x – xc) , dengan xc nilai koordinat garis tengah citra.

$$x' - xc = -x + xc$$

$$x' = 2xc - x \quad \ldots(2.2)$$

Karena xc = (w–1)/2

Maka :

$$x' = 2((w-1)/2) - x$$

$$x' = w - 1 - x \quad \ldots(2.3)$$

2.8.2 Rotasi/Pemutaran (*Rotating*)

Operasi rotasi / pemutaran (*rotating*) merupakan operasi dengan memutar koordinat pada citra. Operasi rotasi yang umum digunakan adalah rotasi ¼ putaran (90^0) dan rotasi ½ putaran (180^0).

a. Rotasi ¼ putaran (90^0) searah jarum jam (CW/clock wise)

$$w' = h \text{ dan } h' = w \rightarrow \text{pertukaran ukuran lebar \& tinggi citra}$$
$$x' = w' - 1 - y \quad \ldots(2.4)$$
$$y' = x$$

b. Rotasi ½ putaran (180^0) searah jarum jam (CW/clock wise)

$$x' = w' - 1 - x \quad \ldots(2.5)$$
$$y' = h' - 1 - y$$

2.8.3 Pemotongan (*Cropping*)

Operasi pemotongan atau disebut dengan *cropping* merupakan pengolahan citra dengan kegiatan memotong satu bagian dari citra. Rumus dari operasi pemotongan sebagai berikut:

$$x' = x - xL \quad \text{untuk } x = xL \text{ sampai } xR \quad \ldots(2.6)$$
$$y' = y - yT \quad \text{untuk } y = yT \text{ sampai } yB$$

Keterangan:

(xL, yT) dan (xR, yBb) adalah koordinat titik pojok kiri atas dan pojok kanan bawah citra yang akan di-crop.

Ukuran citra menjadi:

$$w' = xR - xL \quad \ldots(2.7)$$
$$h' = yB - yT$$

2.8.4 Penskalaan (*Scaling/Zooming*)

Operasi penskalaan (*scaling*) merupakan operasi untuk memperbesar (*zoom-in*) atau memperkecil (*zoom-out*) citra. Rumus dari operasi penskalaan sebagai berikut:

$$x' = Sh\ x \quad \ldots(2.8)$$
$$y' = Sh\ v$$

Keterangan:

Sh : faktor skala horizontal

Sv : faktor skala vertikal

Ukuran citra berubah menjadi:

$$w' = Sh\ w \qquad \ldots(2.9)$$
$$h' = Sh\ h$$

2.9 *Feature Detection* dan *Feature Matching*

Metode *Feature Detection* atau disebut juga metode deteksi fitur adalah metode untuk mendeteksi sudut (*corners*) yang ada pada suatu citra. Pada tahap ini, sistem akan dapat dengan cepat dan akurat menemukan berbagai sudut dalam kondisi pencitraan yang berbeda. Tahap deteksi fitur atau *feature detection* ini akan menghasilkan detector. Selanjutnya sudut (*corners*) yang terdeteksi akan diekstraksi kuantitas sudut (*corners*) yang terdapat pada citra sehingga dapat dibandingkan dan dianalisis. Pada tahap ekstraksi ini, maka akan terbentuk vektor deskriptor (*Descriptor Vector*).

Metode *Feature Matching* adalah langkah mencocokkan atau membandingkan sudut (*corners*) yang telah diekstraksi dengan lapisan data citra yang disimpan dalam database untuk menemukan kecocokan dan relasi terbaik pada citra. Jika langkah pencocokan fitur berhasil, citra dapat dikenali oleh sistem (Prathivi, 2014).

2.10 SIFT (*Scale Invariant Feature Transform*)

Pencocokan gambar (*Image Matching*) adalah aspek mendasar dari banyak masalah dalam visi (penglihatan) komputer, termasuk pengenalan objek atau pemandangan, pemecahan struktur 3D dari banyak gambar, pencocokan stereo, dan pelacakan gerak. *Scale Invariant Feature Transform* (SIFT) menjelaskan fitur gambar yang memiliki banyak property yang membuatnya cocok untuk pencocokan gambar dari objek atau pemandangan berbeda. Hal ini ditandai dengan adanya fitur (*feature*) diantaranya adalah invariant terhadap penskalaan dan rotasi gambar, dan sebagian invariant terhadap perubahan pencahayaan (iluminasi) dan sudut pandang kamera 3D. Fitur (*feature*) akan terlokalisasi dengan baik dalam domain spasial dan frekuensi, yang mengurangi potensi gangguan oleh oklusi, kekacauan, atau interferensi. Sejumlah besar fitur dapat diekstrasi dari gambar biasa dengan algoritma yang efisien. Selain itu, fitur-fiturnya adalah sangat berbeda (khas), yang memungkinkan satu fitur untuk dicocokkan dengan benar melalui probabilitas tinggi secara akurat terhadap database fitur yang besar, membentuk dasar untuk pengenalan objek dan pemandangan (Lowe, 2004).

Biaya pemanfaatan atau ekstrasi fitur ini diminimalkan dengan menerapkan pendekatan penyaringan berjenjang, di mana operasi yang lebih mahal hanya diterapkan di

lokasi yang lulus tes awal. Berikut ini adalah tahapan utama komputasi yang digunakan untuk menghasilkan kumpulan fitur gambar:

1. ***Scale-space Extrema Detection***

   Tahapan pertama, komputasi mencari semua skala dan lokasi gambar. Tahapan ini diimplementasikan secara efisien dengan menggunakan fungsi *difference-of-Gaussian* untuk mengidentifikasi titik unik (menarik) berpotensi yang invarian terhadap skala dan orientasi.

2. ***Keypoint Localization***

   Setiap kandidat lokasi, model detail cocok untuk menentukan lokasi dan skala. Titik kunci (*keypoint*) dipilih berdasarkan ukuran stabilitasnya.

3. ***Orientation Assignment***

   Suatu arah (orientasi) yang berjumlah satu atau lebih orientasi ditentukan untuk setiap lokasi titik kunci (*keypoint*) berdasarkan arah gradien gambar lokal. Semua operasi di masa mendatang dilakukan pada data gambar yang diubah sesuai dengan arah, skala, dan lokasi yang ditentukan untuk setiap fitur, sehingga membuat transformasi tidak dapat diubah.

4. ***Keypoint Descriptor***

   Gradien gambar lokal diukur pada skala yang dipilih di wilayah sekitar setiap titik kunci (*keypoint*). Ini ditransformasikan menjadi representasi yang memungkinkan tingkat distorsi bentuk lokal yang signifikan dan perubahan iluminasi.

2.11 FLANN (*Fast Library Approximated Nearest Neighbor*)

Metode *Fast Library Approximated Nearest Neighbor* (FLANN) adalah library untuk melakukan pencarian cepat, mengestimasi piksel tetangga yang ditemukan pada ruang berdimensi tinggi. Library ini merupakan sekumpulan algoritma yang bekerja dengan baik untuk mencari nilai tetangga terdekat sekaligus mengoptimalkan hasil parameter, namun tergantung dari kumpulan data yang digunakan.

Metode FLANN merupakan himpunan algoritma yang termasuk dalam metode pencocokan objek karena metode FLANN digunakan untuk mencocokkan objek pada algoritma *Scale Invariant Feature Transform* (SIFT). Fungsi SIFT terdiri dari titik-titik kunci (*keypoint*) dan deskriptor dalam bentuk vektor. Untuk gambar dalam database, ada beberapa *cluster* untuk setiap fitur SIFT. *Cluster* ini secara otomatis dibangkitkan dengan KNN (*K-Nearest Neighbor*) menggunakan tipe indeks pohon kd, dimana KNN akan mencari jarak terkecil antara vektor objek dengan vektor dalam *cluster*. Proses pencocokan fitur pada

citra *query* dan fitur citra pada database, vektor *keypoint* dan *decoder* pada citra *query* akan dicocokkan nilainya pada bantuan pencarian KNN.

Pencarian KNN (KNN *search*) akan mencari *cluster* pada database yang nilai vektor deskriptornya paling dekat dengan vektor deskriptor pada citra *query*. Setelah didapatkan *cluster*, maka nilai vektor deskriptor pada *cluster* tersebut sama atau paling dekat dengan vektor deskriptor pada citra *query*. Jika ada kesamaan, maka ada titik kunci yang cocok antara kedua gambar. Kemudian, untuk setiap frame, sebuah garis akan ditarik dari satu titik ke titik lainnya dengan nilai keypoint yang sesuai (Tania, 2010).

2.12 OpenCV (*Open Source Computer Vision*)

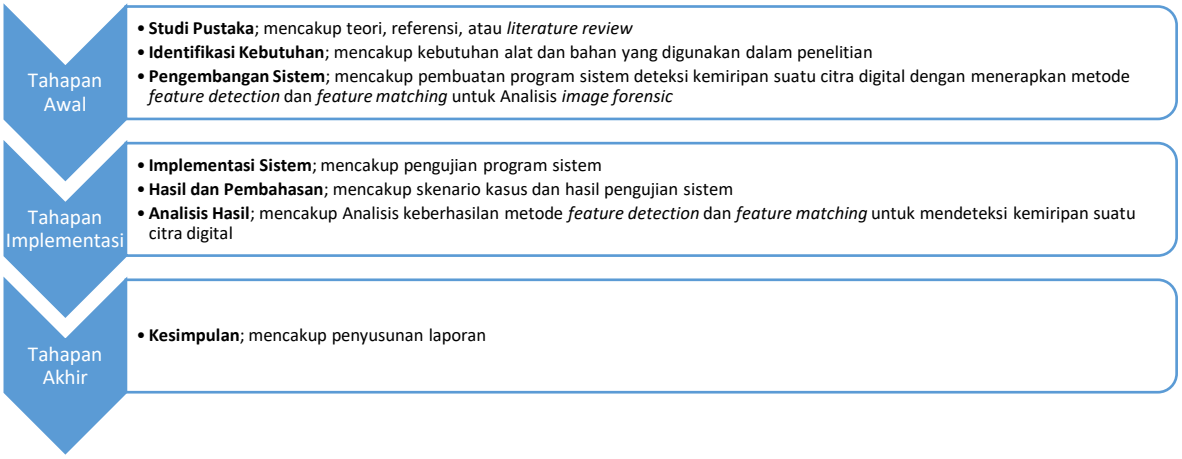
Open Source Computer Vision atau disebut OpenCV merupakan sebuah *library* (Pustaka) perangkat lunak *Computer Vision* (Visi Komputer) dan *Machine Learning* yang bersifat *Open Source*. Open CV dirancang untuk menyediakan infrastruktur umum untuk aplikasi visi komputer dan untuk mempercepat penggunaan persepsi mesin dalam produk komersial. OpenCV dilisensikan di bawah lisensi BSD (*Berkeley Software Distribution*), sehingga memudahkan bisnis untuk menggunakan dan memodifikasi kode (Gautama dkk, 2016) .

OpenCV (*Open Source Computer VIsion*) adalah *library* (pustaka) yang utamanya digunakan untuk pemrosesan citra komputer. OpenCV adalah library gratis yang dapat digunakan di berbagai platform, seperti GNU/Linux maupun Windows. OpenCV mulanya ditulis dalam bahasa pemrograman C++, namun saat ini OpenCV dapat digunakan pada berbagai bahasa seperti Python, Java atau MATLAB.

Gambar 2.2 Logo OpenCV

BAB 3
Metodologi Penelitian

Pada penelitian perlu adanya urutan langkah-langkah yang dibuat secara sistematis agar bisa dijadikan sebagai pedoman yang jelas dalam menyelesaikan penelitian ini. Adapun langkah-langkah penelitian yang akan dilaksanakan pada penelitian ini dapat dilihat pada Gambar 3.1 berikut:



Gambar 3.1 Tahapan Penelitian

3.1 Studi Pustaka

Studi Pustaka merupakan metode pengumpulan data dengan cara membaca, merangkum, serta membandingkan literatur yang sebagian besar berasal dari jurnal, artikel, buku/*e-book*. Semua litetatur tersebut berhubungan dengan tema penelitian ini seperti pengolahan citra, kompresi dan multimedia. Metode ini sangat berguna untuk mendukung penelitian yang akan dilakukan dengan mengacu pada penelitian ynag dilakukan sebelumnya.

3.2 Identifikasi Kebutuhan

Untuk melakukan membangun program deteksi kemiripan citra dengan menggunakan metode *feature detection* dan metode *feature matching* untuk mendukung Analisis *image forensic,* maka diperlukan alat dan bahan untuk melaksanakan penelitian ini. Alat dan bahan yang digunakan pada penelitian ini adalah sebagai berikut:

Tabel 3.1: Alat dan Bahan Penelitian

No.	Alat dan Bahan	Keterangan
1.	**Laptop**	**Sistem Operasi :** Windows 10 Home Single Language 64-bit **RAM :** 8 GB **HDD**: 1TB **Processor :** Intel(R) Core(TM) i3-1005G1 CPU @ 1.20GHz 1.19 GHz
2.	**Bahasa Pemrograman**	**Python Versi 3.9**
3.	***Library Open Source***	***Open Source Computer Vision* (OpenCV) Versi 3.4.17.63**

3.3 Skenario Kasus

Skenario pada penelitian ini menerapkan deteksi kemiripan pada citra digital yang memiliki visual yang identik secara kasat mata. Skenario ini dibuat dikarenakan banyaknya kasus penyebaran informasi palsu yang disebar luaskan melalui citra digital yang mirip secara visual, namun memiliki informasi yang berbeda. Hal ini menyebabkan perlu adanya penelitian untuk mengetahui kemiripan yang dimiliki oleh citra digital tersebut. Pada penelitian ini menggunakan *image* asli dan *image* rekayasa, dimana untuk data *image* asli menggunakan *file image* yang telah terstandarisasi dan dikhususkan untuk sebuah *research* (penelitian). *File image* bersumber dari basis data Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California, dimana file image yang terdapat pada basis data tersebut adalah *file image* yang telah terstandarisasi melalui penerbitan pada publikasi atau penelitian seperti buku, artikel jurnal, prosiding konferensi, tesis, disertasi, dan lain sebagainya. File image pada basis data tersebut menggunakan ekstensi file image TIFF (*Tag Image File Format*). Kemudian image asli ini dilakukan manipulasi untuk dijadikan sebagai image rekayasa dalam penelitian ini. Image rekayasa ini diberikan gangguan citra seperti Rotasi, *Flip*, *Cropping* dan *Copy-move*. Penelitian ini akan menggunakan 3 image asli serta 18 image rekayasa. Dari 3 image asli, masing-masing gambar akan diberikan 6 gangguan citra diantaranya: Rotasi 90°, Rotasi 180°, *Flip Vertical*, *Flip Horizontal*, *Cropping*, serta *Copy-move*.

Tabel 3.2: Image asli yang telah terstandarisasi

Image Asli		
… **Image A**	… **Image B**	… **Image C**

Tabel 3.2 di atas merupakan objek data dari image asli yang telah terstandarisasi yang termasuk dalam database Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California yang dikhususkan untuk research (penelitian).

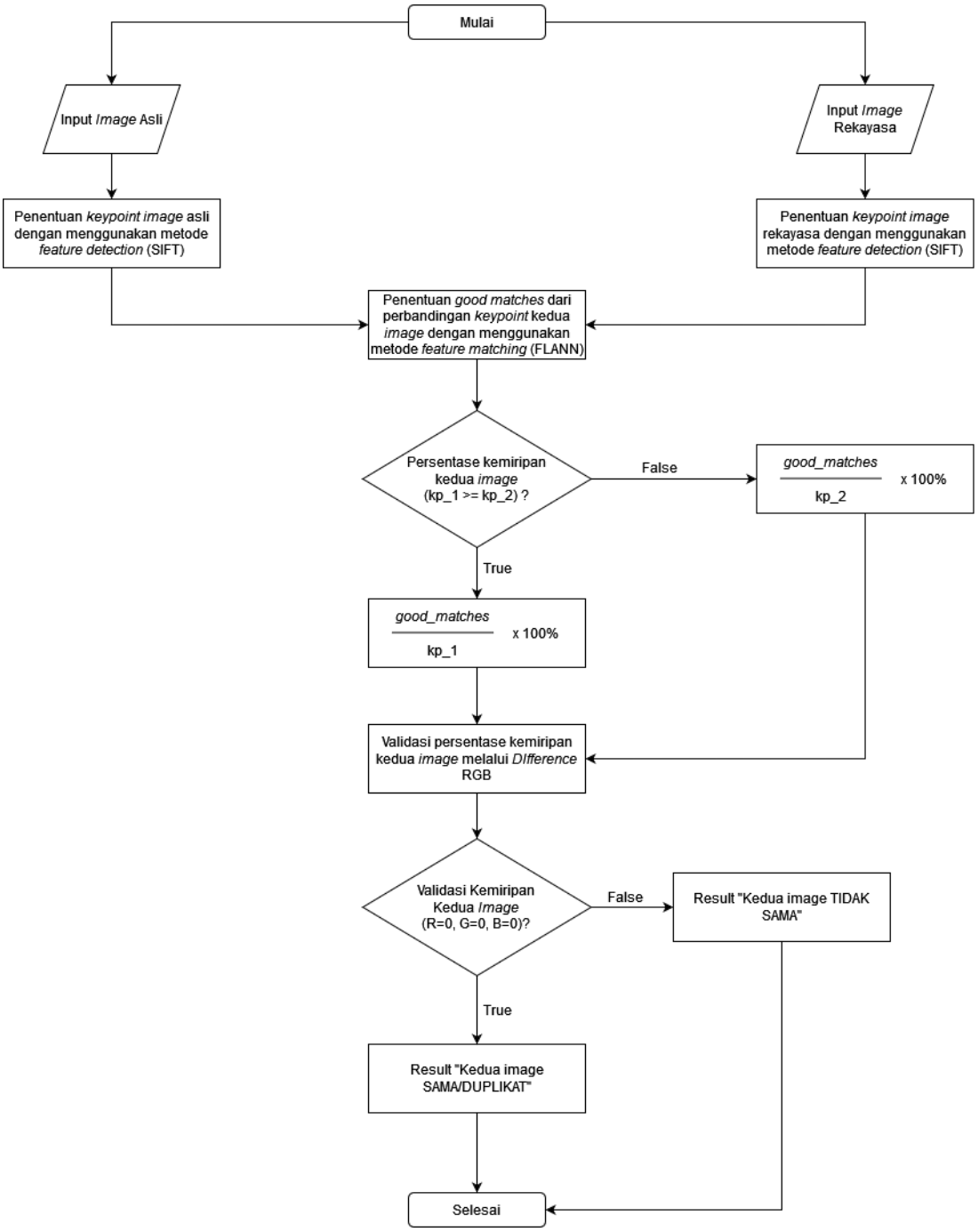
Tabel 3.3: Image rekayasa yang telah dilakukan manipulasi

Image Asli		
… **Image A**		
Image Rekayasa (Image 1 – Image 6)		
Image 1 - Rotasi 90°	**Image 2 - Rotasi 180°**	**Image 3 - *Flip Horizontal***
…	…	…
Image 4 - *Flip Vertical*	**Image 5 - *Crop***	**Image 6 - *Copy-move***
…	…	…

Tabel 3.3 di atas berisikan objek data dari image palsu yang merupakan duplikasi dari file image asli yang diberikan gangguan citra seperti rotasi, flip, cropping dan copy-move.

3.4 Pengembangan Sistem

Penelitian ini akan membangun sebuah sistem untuk mendeteksi kemiripan citra digital dengan menggunakan metode *feature detection* dan metode *feature matching* untuk mendukung Analisis *image forensic*. Sistem akan dibangun menggunakan bahasa pemrograman Python dengan memanfaatkan salah satu *library package* yang diperuntukkan image processing yakni OpenCV (*Open Source Computer Vision*). OpenCV memiliki beberapa fitur yang terkandung di dalamnya, salah satu diantaranya adalah *feature detection* dan *feature matching*. Pada Gambar 3.2 di bawah ini adalah diagram alir atau flowchart dalam mendeteksi kemiripan suatu citra digital menggunakan metode feature detection melalui algoritma *Scale Invariant Feature Transform* (SIFT) dan metode feature matching melalui algoritma *Fast Library Approximated Nearest Neighbor* (FLANN) pada OpenCV.



Gambar 3.2 *Flowchart* deteksi kemiripan pada citra digital

Keterangan Gambar:

kp_1 : Menunjukkan jumlah keypoint yang dimiliki oleh *image* asli.

kp_2 : Menunjukkan jumlah keypoint yang dimiliki oleh *image* rekayasa.

Gambar 3.2 menunjukkan *flowchart* (alur) deteksi kemiripan pada citra digital dengan penggunaan metode *feature detection* dan *feature matching* guna mendukung Analisis *image forensic* dan dapat dijelaskan sebagai berikut:

1. Kedua *image* (yakni *image* asli dan *image* rekayasa) diinputkan pada OpenCV.
2. Setelah itu kedua *image* akan ditentukan jumlah *keypoint* yang dimiliki oleh masing-masing *image* melalui metode *feature detection* dengan *package* algoritma SIFT yang telah di-*import* terlebih dahulu pada OpenCV.
3. Kemudian jumlah *keypoint* dari masing-masing *image* akan dibandingkan untuk mendapatkan nilai *good matches*. Nilai *good matches* akan diperoleh melalui pencocokan *keypoint* melalui metode *feature matching* dengan algoritma FLANN.
4. Setelah nilai *good matches* sudah diperoleh, maka dapat ditentukan nilai persentase kemiripan dengan membandingkan nilai jumlah *keypoint* kedua *image*. Nilai *good matches* akan dibagi dengan jumlah *keypoint* dikali 100%.
5. Untuk mendukung Analisis *image forensic*, maka dilakukan validasi terkait hasil persentase kemiripan kedua *image* melalui *Difference* RGB, dimana *difference* RGB ini menentukan perbedaan nilai *pixel* yang terdapat pada kedua *image*. Jika nilai R=0, G=0, B=0, maka akan diperoleh hasil bahwa kedua *image* SAMA/DUPLIKAT atau dapat disimpulkan bahwa kedua *image* merupakan *image* duplikasi. Namun jika ada perbedaan nilai RGB, maka akan diperoleh hasil bahwa kedua *image* TIDAK SAMA atau dapat disimpulkan bahwa kedua *image* merupakan *image* yang berbeda.

3.5 Implementasi Sistem

Implementasi sistem merupakan tahapan penggunaan metode *feature detection* dan metode *feature matching* yang bertujuan untuk mendeteksi kemiripan suatu citra digital dengan menggunakan beberapa algoritma. Pada metode feature detection digunakan algoritma *Scale Invariant Feature Transform* (SIFT) untuk menentukan titik-titik kunci (*keypoint*) sebagai fitur deteksi, sedangkan pada metode feature matching akan digunakan algoritma *Fast Library Approximated Nearest Neighbor* (FLANN) untuk menentukan titik kunci (*keypoint*) terbaik atau disebut sebagai *good matches* sebagai parameter untuk menentukan persentase kemiripan suatu citra digital. Implementasi sistem akan menggunakan salah satu library package dari Python yang dikhususkan untuk *image processing*.

3.6 Pengujian

Pengujian akan dilakukan dengan menggunakan 2 metode yakni metode feature detection dan feature matching, dimana kedua metode ini akan mendeteksi persentase kemiripan antara *image* asli dan *image* rekayasa (sebagai citra yang terduga dimanipulasi) dengan menggunakan algoritma *Scale Invariant Feature Transform* (SIFT) untuk menentukan titik-titik kunci (*keypoint*) masing-masing citra, serta menggunakan algoritma *Fast Library Approximated Nearest Neighbor* untuk menentukan *keypoint* terbaik (*good matches*).

3.7 Analisis Hasil Pengujian

Setelah dilakukan pengujian dengan menggunakan metode *feature detection* dan *feature matching* melalui algoritma *Scale Invariant Feature Transform* (SIFT) dan *Fast Library Approximated Nearest Neighbor* (FLANN), tahapan akhir adalah mengambil kesimpulan dari hasil pengujian yang telah dilakukan. Kesimpulan analisis hasil bertujuan guna untuk mendukung Analisis *image forensic* yang dapat membantu kebutuhan investigator dalam menyelidiki kasus kejahatan pada sebuah citra digital. Kesimpulan diperoleh dari hasil Analisis hasil pengujian yang akan disajikan dalam tabel rekapitulasi hasil pengujian seperti berikut:

Tabel 3.4: Rekapitulasi Hasil Pengujian Deteksi Kemiripan Image Asli Dan Image Rekayasa

***IMAGE* ASLI**	***IMAGE* REKAYASA**	**PERBANDINGAN**						
		UKURAN PIKSEL		**JUMLAH *KEYPOINT***		***GOOD MATCHES* KEDUA *IMAGE***	**PERSENTASE KEMIRIPAN**	***DIFFERENCE* RGB (TAMPIL / TIDAK)**
		***IMAGE* ASLI**	***IMAGE* REKAYASA**	***IMAGE* ASLI**	***IMAGE* REKAYASA**			
Image A	Image 1 - Rotasi 90°	…	…	…	…	…	…	…
	Image 2 - Rotasi 180°	…	…	…	…	…	…	…
	Image 3 - *Flip Horizontal*	…	…	…	…	…	…	…
	Image 4 - *Flip Vertical*	…	…	…	…	…	…	…
	Image 5 - *Cropping*	…	…	…	…	…	…	…
	Image 6 - *Copy Move*	…	…	…	…	…	…	…

BAB 4
Hasil dan Pembahasan

4.1 Skenario Penelitian

Skenario pada penelitian ini menerapkan deteksi kemiripan pada citra digital yang memiliki visual yang identik secara kasat mata. Skenario ini dibuat dikarenakan banyaknya kasus penyebaran informasi palsu yang disebarluaskan melalui citra digital yang mirip secara visual, namun memiliki informasi yang berbeda. Hal ini menyebabkan perlu adanya penelitian untuk mengetahui kemiripan yang dimiliki oleh citra digital tersebut. Pada penelitian ini menggunakan image asli dan image rekayasa, dimana untuk data image asli menggunakan file image yang telah terstandarisasi dan dikhususkan untuk sebuah research (penelitian). File image bersumber dari basis data Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California, dimana file image yang terdapat pada basis data tersebut adalah file image yang telah terstandarisasi melalui penerbitan pada publikasi atau penelitian seperti buku, artikel jurnal, prosiding konferensi, tesis, disertasi, dan lain sebagainya. File image pada basis data tersebut menggunakan ekstensi file image TIFF (*Tag Image File Format*). Kemudian image asli ini dilakukan manipulasi untuk dijadikan sebagai image rekayasa dalam penelitian ini. Image rekayasa ini diberikan gangguan citra seperti Rotasi, *Flip*, *Cropping* dan *Copy-move*. Penelitian ini akan menggunakan 3 image asli serta 18 image rekayasa dimana *image* rekayasa ini berasal 3 image asli, kemudian masing-masing gambar akan diberikan 6 gangguan citra diantaranya: Rotasi 90°, Rotasi 180°, *Flip Vertical*, *Flip Horizontal*, *Cropping*, serta Copy-move. Gambar 4.1 merupakan contoh penyajian gambar yang akan digunakan dalam penelitian ini:

<table>
<tr><th colspan="3">Image Asli</th></tr>
<tr><th colspan="3">Image A</th></tr>
<tr><td colspan="3">  </td></tr>
<tr><th colspan="3">Image Rekayasa (Image 1 – Image 6)</th></tr>
<tr><th>Image 1 - Rotasi 90°</th><th>Image 2 - Rotasi 180°</th><th>Image 3 - Flip Horizontal</th></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
<tr><th>Image 4 - Flip Vertical</th><th>Image 5 - Crop</th><th>Image 6 - Copy-move</th></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
</table>

Gambar 4.1 *Image* Asli dan *Image* Rekayasa

4.2 Analisis Fungsi OpenCV

Pada *source code* yang terdapat pada OpenCV (*Open Source Computer Vision*) memiliki *library* terkait *image processing*, dimana terdapat beberapa fungsi yang berpengaruh terhadap analisis *image* dalam penelitian ini dengan penerapan metode *feature detection* dan *feature matching*, antara lain:

1. **Pengecekan kemiripan antara 2 citra digital.**

```
#Cek Kemiripan Antara 2 Citra Digital
01    sift = cv2.xfeatures2d.SIFT_create()
02    kp_1, desc_1 = sift.detectAndCompute(image_asli, None)
03    kp_2, desc_2 = sift.detectAndCompute(image_rekayasa, None)
04    print("Jumlah Keypoints Pada Image Asli: " + str(len(kp_1)))
05    print("Jumlah Keypoints Pada Image Rekayasa: " + str(len(kp_2)))
06    result = cv2.drawMatches(image_asli, kp_1, image_rekayasa, kp_2,
      good_points, None)
07    cv2.imshow("Result Kemiripan Antara Image Asli dan Image Rekayasa",
      result)
```

Untuk menghasilkan kemiripan antara *image* asli dan *image* rekayasa, maka dilakukan pengecekkan kemiripan melalui metode *feature detection* dengan penggunaan *library* dari algoritma SIFT yang terdapat pada OpenCV, dimana kode program yang digunakan untuk menjalankan algoritma SIFT ini adalah kode program pada baris 01. Program ini bertujuan untuk menentukan titik-titik kunci (*keypoint*) dari masing-masing *image*, dimana penentuan *keypoint* kedua *image* dijalankan pada kode program pada baris 02 dan baris 03. Kemudian hasil deteksi penentuan *keypoint* kedua *image* dijalankan pada kode program pada baris 07.

2. **Pengecekan tingkat persentase kemiripan *image* asli dan *image* rekayasa.**

```
# Persentase Kemiripan Citra Digital
09    index_params = dict(algorithm=0, trees=5)
10    search_params = dict()
11    flann = cv2.FlannBasedMatcher(index_params, search_params)
12    matches = flann.knnMatch(desc_1, desc_2, k=2)
13    good_points = []
14    for m, n in matches:
15            if m.distance < 0.6*n.distance:
16                    good_points.append(m)
17    jumlah_keypoints = 0
```

```
18  if len(kp_1) <= len(kp_2):
19          jumlah_keypoints = len(kp_1)
20  else:
21  jumlah_keypoints = len(kp_2)
#Output Persentase Kemiripan Citra Digital
22  print("Good Matches Dari Perbandingan Kedua Keypoints: ",
    len(good_points))
23  print("Persentase Kemiripan Kedua Image: ",
    '{:0.2f}'.format(len(good_points) / jumlah_keypoints * 100))
```

Setelah dilakukan pengecekkan kemiripan kedua *image* melalui metode *feature detection* untuk menentukan kesamaan titik-titik kunci (*keypoint*), kemudian dilakukan pengecekkan terhadap tingkat persentase kemiripan kedua *image*. Pengecekkan tingkat persentase kemiripan kedua *image* ini dilakukan melalui metode *feature matching* dengan penggunaan *library* algoritma FLANN yang terdapat pada OpenCV, dimana kode program yang digunakan untuk menjalankan algoritma FLANN ini adalah kode program pada baris 09 hingga baris 12. Selanjutnya algoritma FLANN dapat menghasilkan titik-titik kunci (*keypoint*) terbaik atau yang disebut sebagai *good matches*, dimana *good matches* merupakan salah satu parameter yang digunakan untuk menghasilkan tingkat persentase kemiripan citra digital seperti yang dijalankan di bagian kode program pada baris 22 dan baris 23.

3. Validasi Persentase Kemiripan Citra Digital

```
#Validasi Persentase Kemiripan Citra Digital
24  image1 = image_asli.shape
25  image2 = image_rekayasa.shape
26  print("Ukuran dan Komponen RGB Image Asli:", image1)
27  print("Ukuran dan Komponen RGB Image Rekayasa:", image2)
28  if image_asli.shape == image_rekayasa.shape:
29  print("Kedua image memiliki ukuran dan komponen RGB yang sama")
30  difference = cv2.subtract(image_asli, image_rekayasa)
31  r, g, b = cv2.split(difference)
32  cv2.imshow("Difference RGB Antara Image Asli dan Image Rekayasa",
    difference)
```

```
33    if cv2.countNonZero(r) == 0 and cv2.countNonZero(g) == 0 and
      cv2.countNonZero(b) == 0:
34    print("Kedua image SAMA/DUPLIKAT")
35    else:
36    print("Kedua image TIDAK SAMA")
```

Untuk mendukung hasil deteksi kemiripan citra digital, maka dilakukan validasi persentase kemiripan melalui *difference* RGB, dimana validasi ini dilakukan untuk menampilkan hasil perbedaan nilai RGB antara *image* asli dan *image* rekayasa. Dari validasi ini dapat diperhatikan bagian kode program pada baris 34 dan baris 36, dimana hasil validasi ini akan menghasilkan output status kemiripan dari kedua *image* tersebut sama/duplikat atau kedua *image* tidak sama.

4.3 Implementasi Sistem

Pada penelitian ini mengimplementasikan *library open source* yakni OpenCV dengan menggunakan bahasa pemrograman Python yang menerapkan algoritma SIFT serta algoritma FLANN untuk menentukan keypoint dari masing-masing gambar serta menghitung tingkat persentase kemiripan gambar. OpenCV dijalankan dengan menggunakan aplikasi code editor yakni PyCharm Community Edition 2021.

4.4 Hasil Pengujian

Hasil pengujian dilakukan dengan menerapkan metode *feature detection* dan *feature matching* pada OpenCV untuk mendeteksi kemiripan dari *image* asli dan *image* rekayasa. Penerapan metode *feature detection* dilakukan dengan menggunakan algoritma SIFT sebagai pendeteksi *keypoint* pada masing-masing *image*, sedangkan penerapan metode *feature matching* dilakukan dengan menggunakan algoritma FLANN untuk menentukan *good matches* dari *keypoint* kedua *image* tersebut.

4.4.1 Hasil Pengujian Melalui *Feature Detection*

Pengujian yang dilakukan dengan menggunakan metode *feature detection* menghasilkan hasil dengan menentukan titik-titik kunci atau disebut dengan *keypoint* untuk masing-masing *image*, yakni *image* asli dan *image* rekayasa. Penentuan *keypoint* pada *image* diproses dengan menggunakan algoritma SIFT (*Scale Invariant Feature Transform*). *Keypoint* pada masing-masing *image* akan tampak seperti pada Gambar 4.2 di bawah ini:

Gambar 4.2 Hasil Pengujian Algoritma SIFT

Jumlah *keypoint* yang diperoleh untuk seluruh *image* (baik *image* asli maupun *image* rekayasa) disajikan dalam Tabel 4.1 di bawah ini:

Tabel 4.1: Data Jumlah *Keypoint Image* Asli dan *Image* Rekayasa

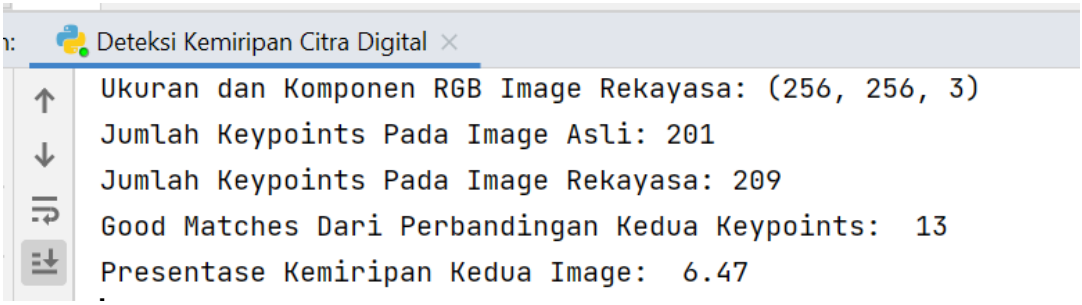
Image Asli	Jumlah Keypoint	Image Rekayasa					
		Rotasi 90°	Rotasi 180°	*Flip Horizontal*	*Flip Vertical*	*Cropping*	*Copy Move*
		Jumlah Keypoint					
Image A	289	297	291	297	301	205	357
Image B	201	209	202	209	207	168	305
Image C	299	303	303	303	309	245	342

Dari Tabel 4.1 dapat diperhatikan bahwa ada perbedaan pada jumlah *keypoint* pada *image* asli dengan jumlah *keypoint* pada *image* rekayasa. Hal ini disebabkan karena titik kunci (*keypoint*) atau disebut sebagai fitur (*feature*) yang dideteksi melalui *feature detection* tidak memiliki posisi yang sama sehingga menghasilkan nilai jumlah *keypoint* yang berbeda. Pada Tabel 4.1 juga dapat diperhatikan bahwa ada nilai konsisten yang terdapat pada jumlah *keypoint* pada *image* rekayasa – *cropping* dimana ada perolehan nilai konsisten yakni nilai yang lebih rendah dari jumlah *keypoint* yang terdapat pada *image* asli, seperti pada jumlah *keypoint* pada Image A berjumlah 289 titik, sedangkan untuk Image 5 – Cropping memiliki jumlah *keypoint* lebih kecil dibandingkan dengan jumlah *keypoint* pada Image A yakni sebesar 205 titik. Hal ini disebabkan karena adanya proses pemotongan (*cropping*) ukuran piksel *image*, sehingga jumlah *keypoint* yang terdapat pada *image* rekayasa – *cropping* akan lebih kecil daripada jumlah *keypoint* yang terdapat pada *image* asli.

4.4.2 Hasil Pengujian Melalui *Feature Matching*

Pengujian yang dilakukan dengan menggunakan metode *feature matching* untuk menghasilkan *keypoint* terbaik dari perbandingan kedua *image* atau yang disebut sebagai

good matches terhadap *keypoint* kedua *image* (yakni *image* asli dan *image* rekayasa) serta menentukan persentase kemiripan dari kedua *image* tersebut. Nilai *good matches* dan persentase kemiripan pada perbandingan kedua *image* akan tampak seperti pada Gambar 4.3 di bawah ini:



Gambar 4.3 Hasil Pengujian Algoritma FLANN

Penentuan nilai *good matches* diperoleh dengan menggunakan algoritma FLANN (*Fast Library Approximated Nearest Neighbor*), sedangkan untuk nilai persentase kemiripan pada perbandingan kedua *image* diperoleh dari hasil pembagian antara nilai *good matches* dibagi dengan jumlah *keypoint* salah satu *image* dikalikan 100%. Tabel 4.2 merupakan hasil data dari *good matches* dan persentase kemiripan antara *image* asli dan *image* rekayasa.

Tabel 4.2: Data *Good Matches* dan Persentase Kemiripan Antara *Image* Asli dan *Image* Rekayasa

Image Asli	**Image Rekayasa**											
	Rotasi 90°		**Rotasi 180°**		***Flip Horizontal***		***Flip Vertical***		***Cropping***		***Copy Move***	
	Good Matches	**Persentase Kemiripan**	**Good Matches**	**Persentase Kemiripan**	**Good Matches**	**Persentase Kemiripan**	**Good Matches**	**Persentase Kemiripan**	**Good Matches**	**Persentase Kemiripan**	**Good Matches**	**Persentase Kemiripan**
Image A	275	95,16%	268	92,73%	3	1,04%	3	1,04%	201	98,05%	259	89,62%
Image B	186	92,54%	179	89,05%	13	6,47%	13	6,47%	166	98,91%	189	94,03%
Image C	276	92,31%	271	90,64%	6	2,01%	5	1,67%	243	99,18%	248	82,94%

Dari Tabel 4.2 di atas dapat diperhatikan bahwa terdapat nilai konsisten yang diperoleh pada *image* rekayasa – *flip*. Nilai konsisten ini terdapat pada nilai *good matches* dan persentase kemiripan. Untuk nilai *good matches* dapat diperhatikan pada Tabel 4.2 bahwa nilai *good matches* yang diperoleh lebih kecil yakni berjumlah 3 hingga 13 titik kunci terbaik (*good matches*) dibandingkan dengan nilai *good matches* dari *image* lainnya. Hal ini dikarenakan pada proses *flip* (pencerminan) pada *image* terdapat perubahan pada koordinat *pixel* citra, dimana koordinat pixel pada proses pencerminan menjadi negatif, sedangkan koordinat *pixel* tidak ada (tidak boleh) negatif, c hal ini yang menyebabkan nilai *good matches* yang diperoleh melalui *feature matching* dengan algoritma FLANN menjadi lebih kecil dibandingkan dengan nilai *good matches* pada *image* rekayasa lainnya dan hal ini juga

berdampak pada persentase kemiripan yang menjadi lebih rendah yakni sebesar 1,04% dibandingkan dengan lainnya.

4.5 Analisis Hasil Pengujian

Pada hasil pengujian dengan menggunakan metode *feature detection* dan *feature matching* dilakukan pada 3 *image* asli yang bersumber dari basis data Signal and Image Processing Institute yang dimiliki oleh Ming Hsich Department of Electrical and Computer Engineering University of Southern California, dimana file image tersebut adalah file *image* yang telah terstandarisasi melalui penerbitan pada publikasi atau penelitian seperti buku, artikel jurnal, prosiding konferensi, tesis, disertasi, dan lain sebagainya serta 18 *image* rekayasa yang berasal dari *image* asli yang telah dilakukan manipulasi atau terdapat gangguan citra (*image tampering*) yang terdiri dari Rotasi 90°, Rotasi 180°, *Flip Vertical*, *Flip Horizontal*, *Cropping*, serta Copy-move. Pengujian dilakukan melalui 2 metode diantaranya:

1) Metode *feature detection*, dimana dalam proses penerapan metode ini dilakukan untuk menentukan *keypoint* dari masing-masing *image* (yakni *image* asli dan *image* rekayasa). Penentuan *keypoint* diperoleh dengan menggunakan algoritma SIFT (*Scale Invariant Feature Transform*).
2) Metode *feature matching*, dimana dalam proses penerapan metode ini dilakukan untuk menentukan *keypoint* terbaik atau disebut sebagai *good matches* dari perbandingan jumlah *keypoint* kedua *image* (yakni *image* asli dan *image* rekayasa). Penentuan *good matches* diperoleh dengan menggunakan algoritma FLANN (*Fast Approximated Nearest Neighbor*). Kemudian perolehan nilai *good matches* ini digunakan untuk meenentukan nilai persentase kemiripan kedua *image* dengan melalui proses pembagian, dimana nilai *good matches* dibagi dengan jumlah *keypoint* salah satu *image* dikalikan 100%.

Dari hasil penerapan metode *feature detection* dan *feature matching* melalui OpenCV, maka diperoleh hasil rekapitulasi data deteksi kemiripan antara *image* asli dan *image* rekayasa sesuai pada Tabel 4.3 di bawah ini:

Tabel 4.3: Hasil Rekapitulasi Pengujian Deteksi Kemiripan *Image* Asli dan *Image* Rekayasa

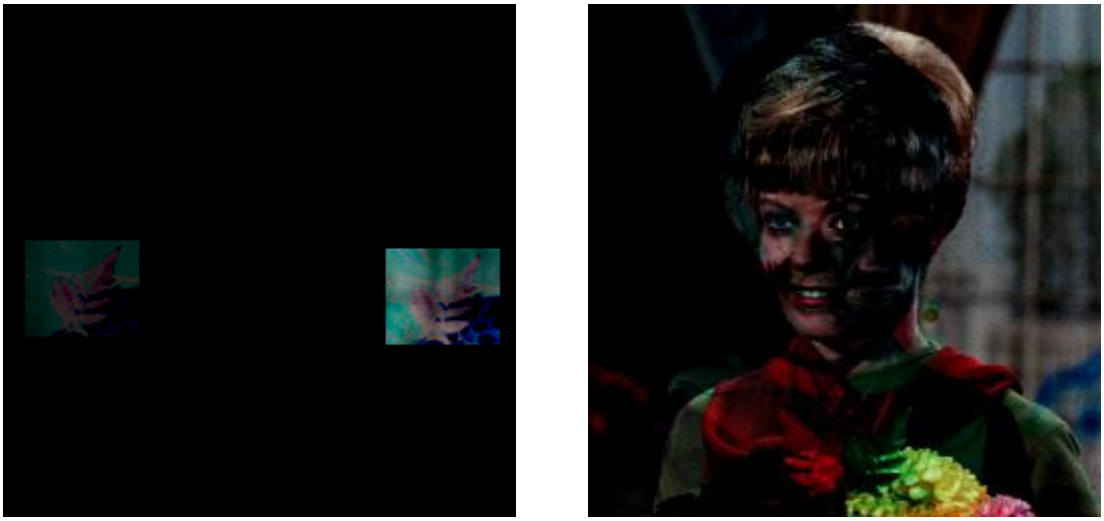
***IMAGE* ASLI**	***IMAGE* REKAYASA**	**PERBANDINGAN**						
		UKURAN PIKSEL		**JUMLAH *KEYPOINT***		***GOOD MATCHES* KEDUA *IMAGE***	**PERSENTASE KEMIRIPAN**	***DIFFERENCE* RGB (TAMPIL / TIDAK)**
		***IMAGE* ASLI**	***IMAGE* REKAYASA**	***IMAGE* ASLI**	***IMAGE* REKAYASA**			
Image A	Image 1 - Rotasi 90°	256 x 256	256 x 256	289	297	275	95,16%	Tampil
	Image 2 - Rotasi 180°	256 x 256	256 x 256	289	291	268	92,73%	Tampil
	Image 3 - *Flip Horizontal*	256 x 256	256 x 256	289	297	3	1,04%	Tampil
	Image 4 - *Flip Vertical*	256 x 256	256 x 256	289	301	3	1,04%	Tampil
	Image 5 - *Cropping*	256 x 256	202 x 248	289	205	201	98,05%	Tidak
	Image 6 - *Copy Move*	256 x 256	256 x 256	289	357	259	89,62%	Tampil
Image B	Image 7 - Rotasi 90°	256 x 256	256 x 256	201	209	186	92,54%	Tampil
	Image 8 - Rotasi 180°	256 x 256	256 x 256	201	202	179	89,05%	Tampil
	Image 9 - *Flip Horizontal*	256 x 256	256 x 256	201	209	13	6,47%	Tampil
	Image 10 - *Flip Vertical*	256 x 256	256 x 256	201	207	13	6,47%	Tampil
	Image 11 - *Cropping*	256 x 256	213 x 255	201	168	166	98,91%	Tidak
	Image 12 - *Copy Move*	256 x 256	256 x 256	201	305	189	94,03%	Tampil
Image C	Image 13 - Rotasi 90°	256 x 256	256 x 256	299	303	276	92,31%	Tampil
	Image 14 - Rotasi 180°	256 x 256	256 x 256	299	303	271	90,64%	Tampil
	Image 15 - *Flip Horizontal*	256 x 256	256 x 256	299	303	6	2,01%	Tampil
	Image 16 - *Flip Vertical*	256 x 256	256 x 256	299	309	5	1,67%	Tampil
	Image 17 - *Cropping*	256 x 256	187 x 253	299	245	243	99,18%	Tidak
	Image 18 - *Copy Move*	256 x 256	256 x 256	299	342	248	82,94%	Tampil

Berdasarkan penjelasan pada Tabel 4.1 dan Tabel 4.2 telah ditemukan bahwa ada perbedaan nilai yang terdapat pada jumlah *keypoint*, *good matches*, serta persentase kemiripan. Nilai tersebut dapat disimpulkan memiliki nilai yang konsisten yakni memiliki nilai rendah atau nilai kecil untuk setiap *image* rekayasa yang sama. Dengan adanya perbedaan nilai yang terdapat pada jumlah *keypoint*, *good matches*, serta persentase kemiripan kedua *image* tersebut dapat digunakan untuk mendukung analisis *image forensic*.

- ***Difference* RGB**

Untuk mendukung Analisis *image forensic*, maka dilakukan validasi untuk kedua *image* untuk membandingkan nilai persentase kemiripan kedua *image* tersebut. Proses validasi dilakukan dengan cara melakukan proses pengecekkan perbedaan RGB atau disebut sebagai *difference* RGB. Menurut teori yang dikembangkan oleh Schetinger, dkk (2016) bahwa alat *image forensic* (forensik citra) yang dikembangkan harus memperhatikan hal yang dapat menganalisis terkait jejak (*trace*) terhadap fitur (*feature*) pada gambar guna untuk

mengetahui sifat pemalsuan pada suatu gambar. Jejak dari fitur (*feature*) pada gambar yang digunakan yakni terkait iluminan atau sumber cahaya, dimana jika *image* rekayasa disambung dengan *image* asli akan terlihat kondisi cahaya yang berbeda. Pada penelitian ini, jejak dari *feature* gambar menggunakan pengecekkan melalui *difference* RGB. *Difference* RGB akan membandingkan nilai RGB dari kedua *image* dengan inisiasi nilai R=0, nilai G=0, dan nilai B=0.



(a) (b)

Gambar 4.4: Hasil *Difference* RGB Dari Perbandingan *Image* Asli dan *Image* Rekayasa

Keterangan Gambar 4.4:

- Gambar (a) merupakan hasil tampilan dari *difference* RGB untuk perbandingan Image A dengan Image Rekayasa 6 – *Copy Move.*
- Gambar (b) merupakan hasil tampilan dari *difference* RGB untuk perbandingan Image A dengan Image Rekayasa 3 – *Flip Horizontal*.

Dari Gambar 4.4 dapat dilihat bahwa ada perbedaan kondisi cahaya *image* rekayasa disambung dengan *image* asli. Perbedaan tersebut diperoleh dengan membandingkan nilai RGB yang telah diinisiasi nilai R=0, nilai G=0, dan nilai B=0. Dari kedua tampilan *difference* RGB yang terdapat pada Gambar 4.4, perbedaan yang tampak jelas terdapat *image* rekayasa *flip*, hal ini berdasarkan pada proses *flip* (pencerminan) pada *image* terdapat perubahan pada koordinat *pixel* citra, dimana koordinat pixel pada proses pencerminan menjadi negatif, sedangkan koordinat *pixel* tidak ada (tidak boleh) negatif, sehingga menghasilkan nilai *good matches* & nilai persentase kemiripan yang rendah, dan menampilkan *difference* RGB yang cukup signifikan.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Pada penelitian ini menghasilkan kesimpulan bahwa menentukan fitur (*feature*) dalam mendeteksi kemiripan pada citra melalui tingkat persentase kemiripan guna untuk mendukung analisis *image forensic* dilakukan dengan menerapkan metode *feature detection* dan *feature matching*, dimana melalui metode tersebut telah menghasilkan jumlah titik-titik kunci (*keypoint*) untuk masing-masing image (yakni *image* asli dan *image* rekayasa). Pada penerapan metode *feature detection* untuk kedua image telah diperoleh perbedaan antara jumlah keypoint image asli dengan jumlah keypoint image rekayasa. Hal ini disebabkan karena adanya gangguan citra yang terdapat pada image rekayasa, sehingga jumlah keypoint pada image rekayasa berbeda dengan jumlah keypoint pada image asli, sedangkan pada penerapan metode *feature matching* untuk kedua image telah diperoleh nilai persentase kemiripan dari kedua image yang diperoleh dari nilai good matches dibagi dengan jumlah keypoint dikali 100%. Pada perhitungan ini, terdapat nilai persentase kemiripan paling rendah pada image rekayasa – *flip* yakni sebesar 1,04%. Hal ini disebabkan dikarenakan pada proses pencerminan terdapat perubahan pada koordinat pixel citra, dimana koordinat pixel pada proses pencerminan menjadi negatif, sedangkan koordinat pixel tidak ada (tidak boleh) negatif, sehingga hal ini yang menyebabkan nilai kemiripan menjadi rendah atau kecil. Penerapan metode *feature detection* dan *feature matching* difokuskan untuk menghasilkan fitur-fitur dari sebuah image (citra). Hasil fitur tersebut terdapat perbedaan yang dapat mendukung analisis *image forensic*. Perbedaan fitur pada sebuah image ini diperoleh dari perbedaan jumlah keypoint, selain itu perbedaan fitur ini dilakukan validasi melalui *difference* RGB dengan melihat perbedaan dari pixel atau elemen citra yang dimiliki oleh masing-masing citra.

5.2 Saran

Saran untuk penelitian selanjutnya adalah untuk mengembangkan penelitian deteksi kemiripan terhadap citra digital dengan membuat *image* rekayasa yang memiliki tingkat kompleksitas yang cukup kompleks agar dapat menyesuaikan dengan perkembangan teknologi yang saat ini semakin modern.

Daftar Pustaka

Al-Azhar, M. N. (2012). Digital Forensic Panduan Praktis Investigasi Komputer. Jakarta: Salemba Infotek.

Endardhi, A. R., Ulfah, A. N., Lizarti, N., Susandri., & Harianto, K. (2021). Forensic Image Forgery Menggunakan Teknik Wavelet Denoising Pada Citra 2D. *Jurnal Edik Informatika*. 7(2), 21- 34.

Ferreira, W. D., Ferreira, C. B., da Cruz Júnior, G., & Soares, F. (2020). A review of digital image forensics. *Elsevier: Computers & Electrical Engineering*, 85, 106685.

Gautama, T. K., Hendrik, A., & Hendaya, R. (2016). Pengenalan Objek pada Computer Vision dengan Pencocokan Fitur Menggunakan Algoritma SIFT Studi Kasus: Deteksi Penyakit Kulit Sederhana. *Jurnal Teknik Informatika Dan Sistem Informasi*, 2(3), 437–450. https://doi.org/10.28932/jutisi.v2i3.554

Gokhale, A., Mulay, P., Pramod, D., & Kulkarni, R. (2020). A bibliometric analysis of digital image forensics. *Science & technology libraries*, 39(1), 96-113.

H, Farid. 2009. A survey of image forgery detection. IEEE Signal Processing Magazine. 26(2). 16-25.

Harefa, L. H. (2016). Analisis Edge Detection Citra Digital Dengan Menggunakan Metode Robert dan Canny. *Jurnal Riset Komputer (JURIKOM)*. 3(1). 29-34.

Irwansyah, I., & Yudiastuti, H. (2019). Analisis Digital Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta. *Jurnal Ilmiah Matrik*. *21*(1), 54-63. https://doi.org/10.33557/jurnalmatrik.v21i1.518

Lionnie, R., Kadarina, T. M., & Alaydrus, M. (2018). Analisis Metode SIFT dan SURF Untuk Sistem Pendeteksi Gambar Termanipulasi Penyerangan Copy-Move Forgery. *Jurnal Telekomunikasi Dan Komputer*, *8*(3), 183. https://doi.org/10.22441/incomtech.v8i3.3074

Lowe, D. G. (2004). Distinctive Image Features From Scale-Invariant Keypoint. *International Journal of Computer Vision*, *60*(2), 91-110.

Nuari, R., Utami, E., & Raharjo, S. (2019). Comparison of Scale Invariant Feature Transform and Speed Up Robust Feature For Image Forgery Detection Copy Move. *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2019*, 107–112. https://doi.org/10.1109/ICITISEE48480.2019.9003761

Piva, A. 2013. An overview on image forensics. *ISRN Signal Processing*. 1-22.

Prathivi, R. (2014). Feature Recognition Berbasis Corner Detection Dengan Metode FAST, SURF, dan FLANN Tree Untuk Identifikasi Logo Pada Augmented Reality Mobile System. *Jurnal Transformatika*, *11*(2), 51-59.

Purwandari, E. P., Vatresia, A., & Siburian, S. (2019). Deteksi Image Splicing Pada Citra Dengan Metode Discrete Cosine Transform (DCT) dan Scale Invariant Feature Transform (SIFT). *Pseudocode*, *6*(2), 138–148. https://doi.org/10.33369/pseudocode.6.2.138-148

Riadi, I., Yudhana, A., Sulistyo, W. Y. (2019). Analisis Image Forensics Untuk Mendeteksi Pemalsuan Foto Digital *Mobile and Forensics*, *1*(1), 13-21.

Rosidin, Sugiantoro, B., & Prayudi, Y. (2018). Analisis Pendeteksi Kecocokan Objek Pada Citra Digital Dengan Metode Algoritma SIFT dan Histogram Color RGB. *1*(1), 20–27.

Salomon, D., & Motta, G. 2010. Handbook of Data Compression (5th ed.). London: Springer

Schetinger, V., Iuliani, M., Piva, A., & Oliveira, M. M. (2016). Digital image forensics vs. image composition: An indirect arms race. arXiv preprint arXiv:1601.03239.

Sharma, D., & Abrol, P. (2013). Digital Image Tampering-A Threat to Security Management. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(10), 4120–4123. www.ijarcce.com

Siahaan, A. J. N. (2017). Penerapan Metode Frei-Chan dan Metode Laplacian Untuk Mendeteksi Tepi Citra Digital. *Informasi Dan Teknologi Ilmiah (INTI)*, *12*, 146–149.

Sinaga, A. S. R. (2017). Implementasi Teknik Threshoding pada Segmentasi Citra Digital. Jurnal Mantik Penusa, 1(2), 48–51.

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2020). Penerapan Teknik SURF Pada Forensik Citra Untuk Analisis Rekayasa Foto Digital. *JUITA: Jurnal Informatika*, *8*(2), 179. https://doi.org/10.30595/juita.v8i2.6602

Sunardi, Yudhana, A., & Saifullah, S. (2017). Identity Analysis of Egg Based on Digital and Thermal Imaging: Image Processing and Counting Object Concept. *International Journal of Electrical and Computer Engineering*, 7(1), 200–208. https://doi.org/10.11591/ijece.v7i1.pp200-208

Sutoyo, T. (2009). Teori Pengolahan Citra Digital. Yogyakarta: Andi Publisher.

Tania, K. D. (2010). Pengenalan Gambar Menggunakan Sebagian Data Gambar. *Generic*. *5*(2), 12-14.

Tresnaningsih, W. R., Purwandari, E. P., & Andreswari, D. (2017). Deteksi Pemalsuan Citra Copy Move Menggunakan Dyadic Wavelet Dan Scale Invariant Feature Transform. *Jurnal Pseudocode*, *IV*(1).

Van, V. S. 2009. Image Compression Using Burrows-Wheeler Transform. Master Thesis, Helsinki University of Technology, Department of Signal Processing and Accoustics, Espoo.

Wijaya, A. Y., Musayyab, S. Al, & Studiawan, H. (2017). Pengembangan Metode Block Matching Untuk Deteksi Copy-Move Pada Pemalsuan Citra. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *15*(1), 84. https://doi.org/10.12962/j24068535.v15i1.a638

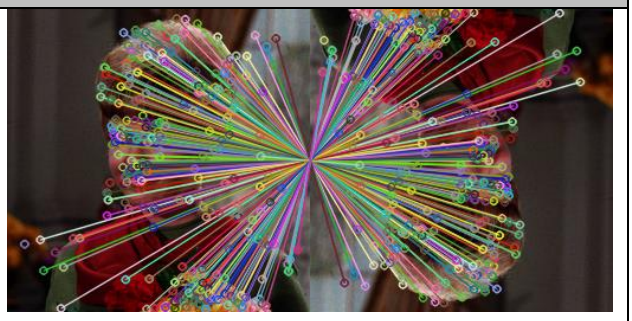
LAMPIRAN

<table>
<tr><th colspan="3">Image Asli</th></tr>
<tr><th colspan="3">Image A</th></tr>
<tr><td colspan="3">  </td></tr>
<tr><th colspan="3">Image Rekayasa (Image 1 – Image 6)</th></tr>
<tr><th>Image 1 - Rotasi 90°</th><th>Image 2 - Rotasi 180°</th><th>Image 3 - Flip Horizontal</th></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
<tr><th>Image 4 - Flip Vertical</th><th>Image 5 - Crop</th><th>Image 6 - Copy-move</th></tr>
<tr><td>  </td><td>  </td><td>  </td></tr>
</table>

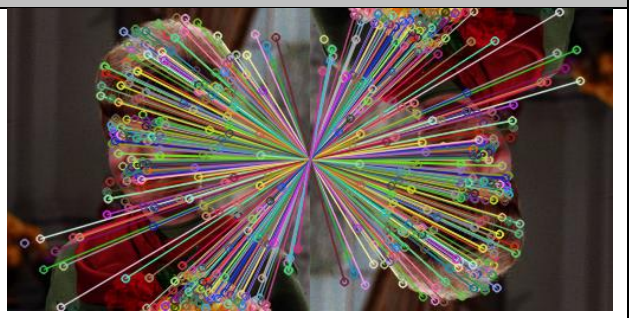
Image Asli		
Image B		
		
Image Rekayasa (Image 7 – Image 12)		
Image 7 - Rotasi 90°	**Image 8 - Rotasi 180°**	**Image 9 - *Flip Horizontal***
		
Image 10 - *Flip Vertical*	**Image 11 - *Crop***	**Image 12 - *Copy-move***
		

Image Asli		
Image C		
		
Image Rekayasa (Image 13 – Image 18)		
Image 13 - Rotasi 90°	**Image 14 - Rotasi 180°**	***Image 15 - Flip Horizontal***
		
Image 16 - *Flip Vertical*	**Image 17 - *Crop***	**Image 18 - *Copy-move***
		

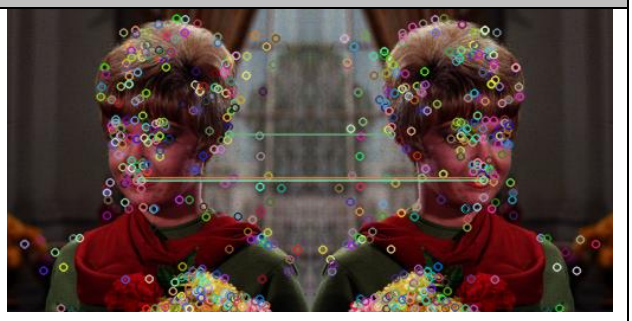
1. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 1 – Rotasi 90°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 297 *Good Matches* Kedua *Image*: 275 Persentase Kemiripan Kedua *Image*: 95,16%

2. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 2 – Rotasi 180°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 **Keterangan:** *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 291 *Good Matches* Kedua *Image*: 268 Persentase Kemiripan Kedua *Image:* 92,73%

3. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 3 – *Flip Horizontal*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 297 *Good Matches* Kedua *Image*: 3 Persentase Kemiripan Kedua *Image:* 1,04%

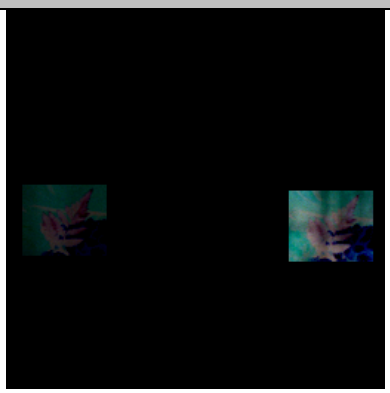
4. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 4 – *Flip Vertical*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 301 *Good Matches* Kedua *Image*: 3 Persentase Kemiripan Kedua *Image:* 1,04%

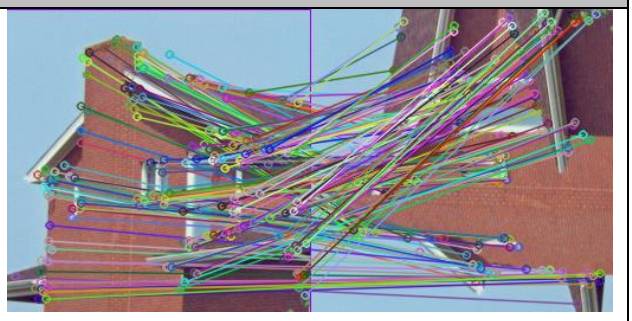
5. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 5 – *Crop*

***Difference* RGB**	***Good Matches***
TIDAK TAMPIL KARENA UKURAN PIKSEL BERBEDA	 *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 205 *Good Matches* Kedua *Image*: 201 Persentase Kemiripan Kedua *Image:* 98,05%

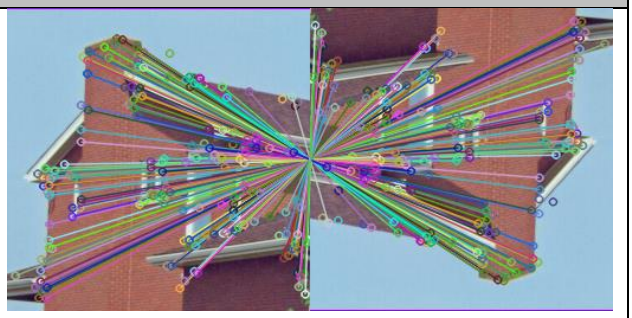
6. Hasil *Difference* RGB & *Good Matches* Image A dibandingkan dengan Image 6 – *Copy-move*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 289 *Keypoint Image* Rekayasa: 357 *Good Matches* Kedua *Image*: 259 Persentase Kemiripan Kedua *Image:* 89,62%

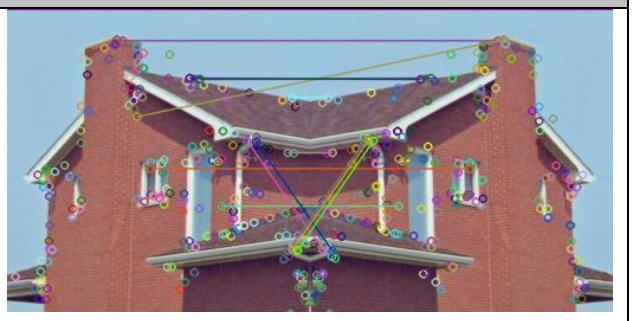
7. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 7 – Rotasi 90°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 209 *Good Matches* Kedua *Image*: 186 Persentase Kemiripan Kedua *Image:* 92,54%

8. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 8 – Rotasi 180°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 202 *Good Matches* Kedua *Image*: 179 Persentase Kemiripan Kedua *Image:* 89,05%

9. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 9 – *Flip Horizontal*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 209 *Good Matches* Kedua *Image*: 13 Persentase Kemiripan Kedua *Image:* 6,47%

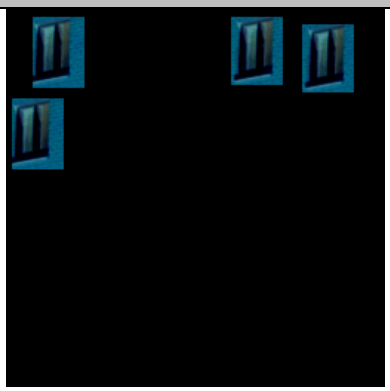
10. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 10 – *Flip Vertical*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 207 *Good Matches* Kedua *Image*: 13 Persentase Kemiripan Kedua *Image:* 6,47%

11. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 11 – *Crop*

***Difference* RGB**	***Good Matches***
TIDAK TAMPIL KARENA UKURAN PIKSEL BERBEDA	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 168 *Good Matches* Kedua *Image*: 166 Persentase Kemiripan Kedua *Image:* 98,91%

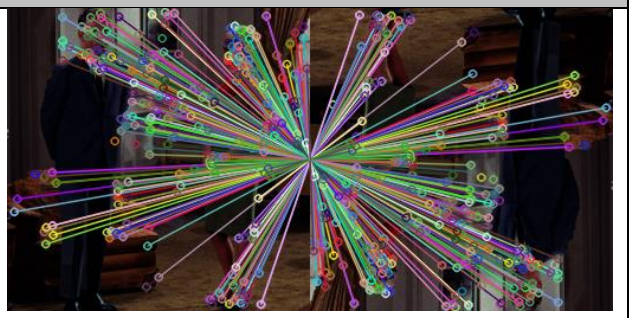
12. Hasil *Difference* RGB & *Good Matches* Image B dibandingkan dengan Image 12 – *Copy-move*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 201 *Keypoint Image* Rekayasa: 305 *Good Matches* Kedua *Image*: 189 Persentase Kemiripan Kedua *Image:* 94,03%

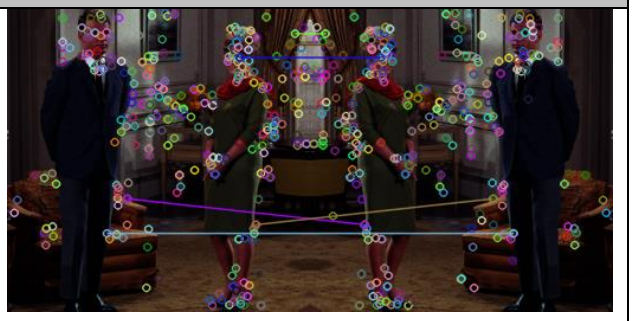
13. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 13 – Rotasi 90°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 303 *Good Matches* Kedua *Image*: 276 Persentase Kemiripan Kedua *Image:* 92,31%

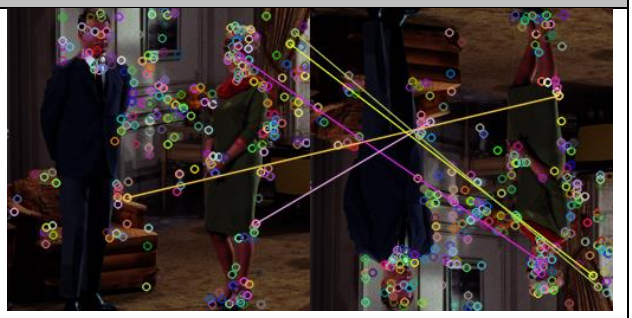
14. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 14 – Rotasi 180°

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 303 *Good Matches* Kedua *Image*: 271 Persentase Kemiripan Kedua *Image:* 90,64%

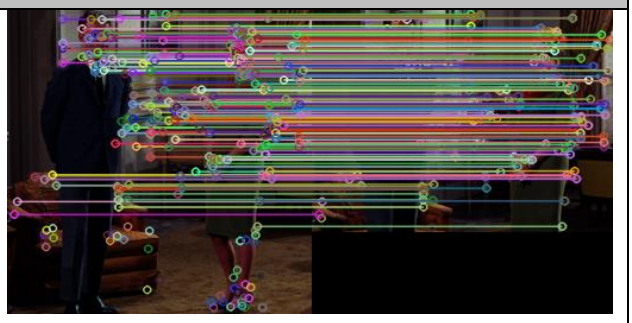
15. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 15 – *Flip Horizontal*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 303 *Good Matches* Kedua *Image*: 6 Persentase Kemiripan Kedua *Image:* 2,01%

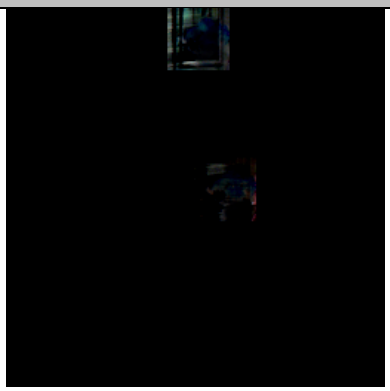
16. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 16 – *Flip Vertical*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 303 *Good Matches* Kedua *Image*: 5 Persentase Kemiripan Kedua *Image:* 1,67%

17. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 17 – *Crop*

***Difference* RGB**	***Good Matches***
TIDAK TAMPIL KARENA UKURAN PIKSEL BERBEDA	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 245 *Good Matches* Kedua *Image*: 243 Persentase Kemiripan Kedua *Image:* 99,18%

18. Hasil *Difference* RGB & *Good Matches* Image C dibandingkan dengan Image 18 – *Copy-move*

***Difference* RGB**	***Good Matches***
 **Keterangan:** Hasil *difference* RGB, tampaknya jelas bahwa nilai R tidak sama dengan 0; nilai G tidak sama dengan 0 dan nilai B tidak sama dengan 0	 *Keypoint Image* Asli: 299 *Keypoint Image* Rekayasa: 342 *Good Matches* Kedua *Image*: 248 Persentase Kemiripan Kedua *Image:* 82,94%