

# Sistem Pendeteksi Gambar Termanipulasi Menggunakan Metode SIFT

Regina Lionnie<sup>1</sup>, Mudrik Alaydrus<sup>2</sup>

Program Studi Magister Teknik Elektro,  
Universitas Mercu Buana, Jakarta

<sup>1</sup>regina.lionnie.id@ieee.org, <sup>2</sup>mudrikalaydrus@mercubuana.ac.id

## Ringkasan

Pada penelitian di publikasi ini, penulis membangun sistem pendeteksi gambar termanipulasi dengan metode pemalsuan penyerangan *copy-move*. Metode SIFT oleh David Lowe digunakan untuk menentukan SIFT fitur vektor yang berisi deskriptor titik kunci dengan membandingkan 4 nilai ( $dr$ ) perbandingan jarak antara hasil terdekat pertama dan kedua. Gambar sebagai masukan dari sistem dimanipulasi penulis dengan mengubah ukuran dan arah dari gambar asli. Hasil dari percobaan memperlihatkan bahwa metode SIFT memberikan kecocokan salah terkecil ketika bagian gambar yang disalin tidak diubah ukuran dan arahnya. Sedangkan, ketika ukuran diubah menjadi besar dan arah diubah sebesar 180 derajat memperlihatkan hasil kecocokan salah yang lebih banyak.

**Kata kunci:** *copy-move forgery*, deteksi pemalsuan, *multimedia forensic*, SIFT

## 1. Pendahuluan

Teknologi di dunia semakin berkembang pesat. Salah satu perkembangan teknologi adalah mudahnya memanipulasi gambar-gambar digital dengan perangkat lunak pengolah gambar yang juga didapatkan dengan mudah. Fitur-fitur dari perangkat lunak ini menjadikan gambar asli diubah menjadi gambar yang sudah dimanipulasi. Hal ini dapat menjadi keuntungan jika memang gambar asli mempunyai kualitas yang buruk sehingga perlu sebuah editan dari perangkat lunak agar kualitasnya menjadi lebih baik dan dapat dinikmati. Akan tetapi, banyak sekali pelaku kriminal memanfaatkan hal ini dan memanipulasi gambar digital untuk tujuan kejahatan seperti untuk memalsukan kendaraan rusak untuk klaim asuransi (padahal kenyataannya tidak ada kendaraan yang rusak) atau membuat berita palsu melalui gambar yang dimanipulasi di dunia maya (hoax).

Pada umumnya sebuah pemalsuan gambar digital dapat dikelompokkan menjadi dua jenis yaitu *copy-move forgery* dan *splicing* [1]. Kedua jenis pemalsuan dan penyerangan ini termasuk dalam bidang ilmu *multimedia forensic* dimana analisis akan menggunakan metode yang mengambil informasi dari konten multimedia dan mengambil keputusan apakah konten tersebut sudah dimanipulasi apa tidak [2]. Pada penyerangan *copy-move forgery*, sebuah gambar digital dimanipulasi dengan melakukan penyalinan sebagian gambar dan menempelkannya kembali pada gambar yang sama. Sedangkan pada penyerangan *splicing*, beberapa gambar digital diambil sebagian gambar pada masing-masing sumber dan disatukan dari beberapa gambar tersebut menjadi suatu gambar manipulasi. Pada publikasi ini, penulis menyelidiki efek dari perubahan nilai

perbandingan jarak di antara tetangga terdekat pertama dan kedua pada hasil kecocokan SIFT (*scale-invariant feature transform*) [3] fitur vektor untuk penyerangan jenis *copy-move*. Jika terdeteksi tetangga terdekat diantara dua buah SIFT fitur vektor, sistem menganggap bahwa gambar merupakan gambar yang sudah termanipulasi. Hasil dari kecocokan SIFT fitur vektor akan berupa kecocokan dimana performa terbaik dari desain sistem yang digunakan haruslah mempunyai kecocokan salah (*false match*) yang kecil.

## 2. Scale-Invariant Feature Transform (SIFT)

SIFT dikembangkan oleh David Lowe [3] di tahun 2004. Sejak saat itu, banyak sekali area riset menggunakan metode ini untuk mencari solusi dari permasalahan masing-masing. SIFT memiliki keunggulan karena metode ini dapat mendeteksi fitur-fitur signifikan yang stabil dalam ruang skala Gauss dan tahan terhadap transformasi geometri rotasi dan penyekalaan. Dalam menganalisis gambar digital yang telah dimanipulasi, pada tahun 2008, Huang dkk [4] menggunakan metode SIFT [3] untuk diterapkan pada deteksi penyerangan copy move untuk gambar digital. Publikasi Huang [4] adalah publikasi yang pertama kali menerapkan metode SIFT [3] pada area riset deteksi penyerangan copy move ini. Terdapat empat bagian metode SIFT yaitu, deteksi nilai lokal ekstrema dalam skala ruang hierarki Gauss, pencarian lokasi titik kunci dan penapisan, penentuan orientasi dan pembentukan deskriptor SIFT [3].

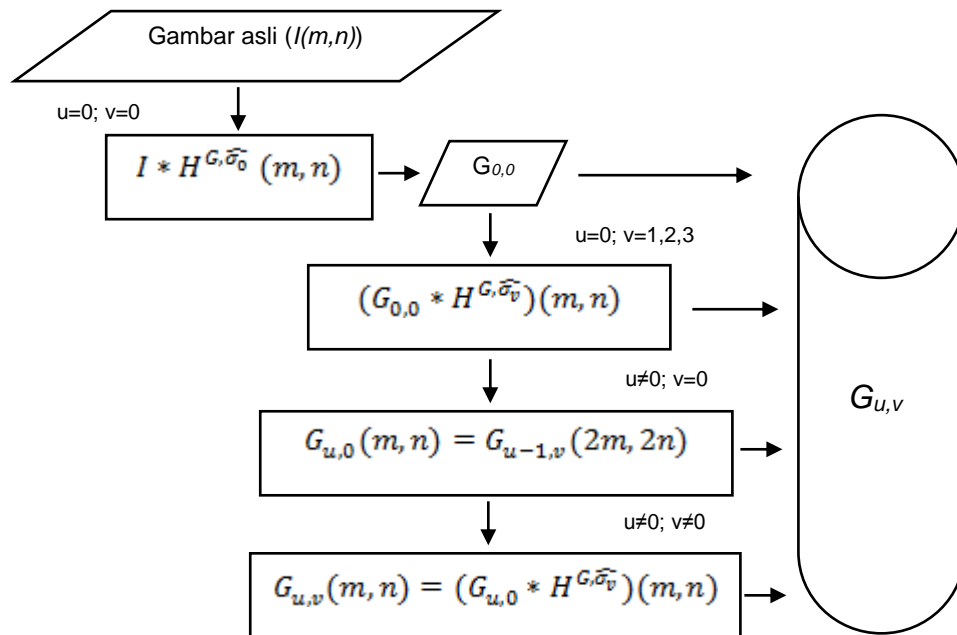
### 2.1. Deteksi Nilai Lokal Ekstrema dalam Skala Ruang Hierarki Gauss

Hal pertama yang dilakukan pada metode ini adalah membangun skala ruang hierarki Gauss dengan proses konvolusi gambar asli  $I(m,n)$  dengan kernel Gaussian  $H^{G,\hat{\sigma}_v}$  untuk beberapa level nilai sigma dan proses desimasi untuk beberapa oktaf yang akan dibangun. Proses ini terlihat pada Gambar 1 berikut. Nilai sigma dari kernel Gaussian yang digunakan dapat dilihat pada persamaan (1) dan (2) [5] dimana  $\sigma_0 = 1.6$  dan  $\sigma_s = 0.5$  [3].

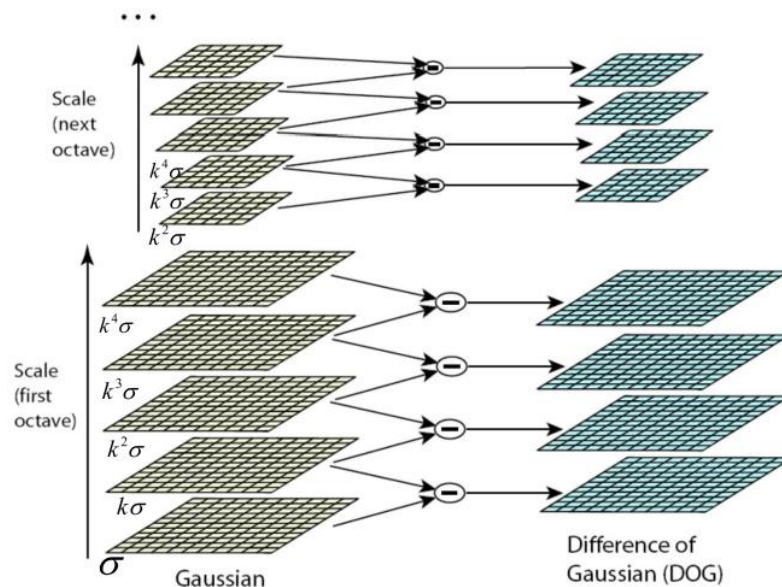
$$\hat{\sigma}_0 = \sqrt{\sigma_0^2 - \sigma_s^2} \quad (1)$$

$$\hat{\sigma}_v = \sigma_0 \cdot \sqrt{2^{2v/V} - 1} \quad (2)$$

Selanjutnya dibentuk *difference of Gaussian* (DoG) menggantikan *laplacian of Gaussian* (LoG) karena LoG membutuhkan usaha komputasi yang rumit dan tidak efisien. mendapatkan DoG cukup mengurangi skala ruang pada level di atas dan skala ruang level sebelumnya yang dapat dilihat pada Gambar 2 berikut.

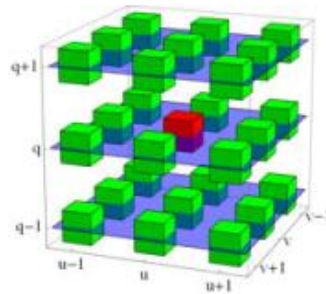


Gambar 1. Diagram Alir Skala Ruang Hierarki Gauss untuk  $U$  oktaf dan  $V$  level [3,5,6]



Gambar 2. Proses DoG [3]

Setelah mendapatkan DoG, proses berikutnya adalah mencari nilai ekstrema lokal dari DoG pada level di atas dan di bawah sebuah DoG. Untuk jelasnya dapat dilihat pada Gambar 3 berikut. Titik tujuan yang berwarna merah pada suatu level  $q$  akan dibandingkan dengan 26 titik hijau dari level  $q+1$ ,  $q$  dan  $q-1$ . Jika titik merah bernilai lebih besar atau lebih kecil dari semua titik hijau, akan dianggap sebuah nilai ekstrema lokal. Nilai ekstrema ini selanjutnya disebut kandidat titik kunci.



Gambar 3. Perbandingan Pencarian Nilai Lokal Ekstrema [5]

## 2.2. Pencarian Lokasi Titik Kunci dan Penapisan

Kandidat titik kunci yang sudah didapatkan akan direduksi karena tidak semua kandidat titik kunci mempunyai karakteristik yang stabil. Terlebih, terdapat banyak kandidat kunci dengan respon kuat seperti struktur tepian yang ingin dihilangkan. Cara mereduksi kandidat titik kunci pertama-tama dengan estimasi lokasi titik kunci yang kontinu pada sebuah posisi kuadratik dan diperhalus hasilnya dengan menggunakan order kedua ekspansi Taylor. Untuk mereduksi kandidat titik kunci sepanjang struktur tepian, Lowe [3] menggunakan *principal curvature* dengan menghitung nilai eigen dengan bantuan *trace* dan determinan dari sebuah matriks Hessian. Setelah melalui beberapa metode penapisan ini kandidat titik kunci akan difinalisasi menjadi titik kunci.

## 2.3. Penentuan Orientasi

Untuk mendapatkan orientasi, yaitu arah  $\theta(x, y)$  dan besar  $m(x, y)$  disekitar titik kunci, digunakan persamaan (3) dan (4) [3] dengan  $L(x, y)$  adalah hasil konvolusi gambar asli dengan kernel Gaussian yang dijelaskan pada sub bab 2.1. Tujuan pencarian orientasi agar dapat mencari orientasi yang dominan (nilai  $m$  terbesar) dan meluruskan arah agar searah dengan arah dimana nilai  $m$  terbesar.

$$m(x, y) = \sqrt{(L(x + 1, y) - L(x - 1, y))^2 + (L(x, y + 1) - L(x, y - 1))^2} \quad (3)$$

$$\theta(x, y) = \tan^{-1} \left( \frac{L(x, y + 1) - L(x, y - 1)}{L(x + 1, y) - L(x - 1, y)} \right) \quad (4)$$

Selanjutnya akan dihitung histogram orientasi dengan cara mengutus setiap  $10^0$  orientasi ke dalam 1 bin, sehingga total histogram orientasi yang terbentuk adalah 36 bin.

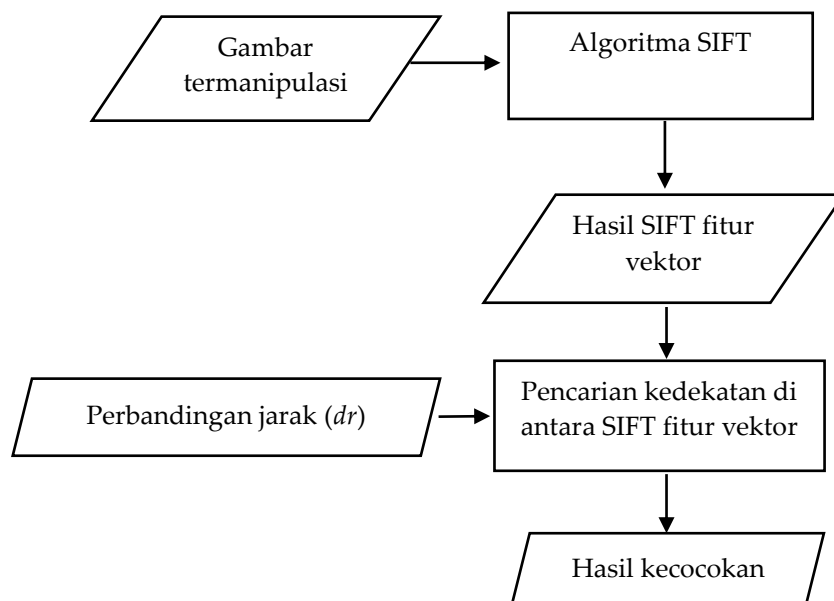
## 2.4. Pembentukan Deskriptor SIFT

Langkah terakhir adalah membentuk deskriptor di sekitar titik kunci. Diambil tetangga  $4 \times 4$  di sekitar titik kunci dan setiap tetangga akan dibentuk histogram orientasi 8 bin dimana 1 bin mencakup  $45^0$  arah. Total informasi yang diperoleh adalah  $4 \times 4 \times 8 = 128$  informasi yang selanjutnya diletakkan di dalam sebuah vektor kolom yang kita sebut SIFT fitur vektor.

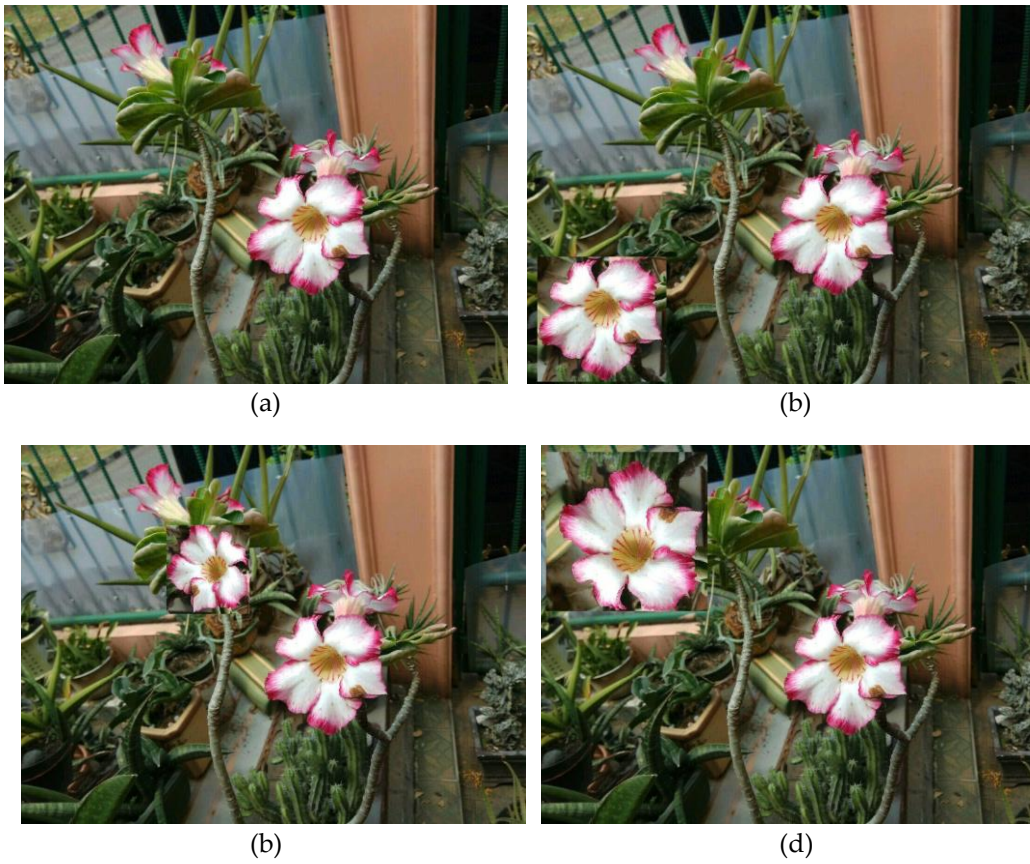
## 3. Perancangan Sistem Pendeteksi

Sistem pendeteksi gambar termanipulasi penyerangan *copy-move* dapat dilihat pada Gambar 4 berikut. Input dari sistem berupa gambar yang sudah termanipulasi dan sudah diubah formatnya ke dalam gambar skala keabuan. Pada penelitian di publikasi ini terdapat 3 jenis gambar yang sudah penulis manipulasi seperti ditampilkan pada

Gambar 5, gambar pertama merupakan gambar asli (5.a), kemudian gambar kedua merupakan manipulasi tanpa perubahan ukuran dan arah (5.b), gambar ketiga merupakan manipulasi dengan memperkecil dan perubahan arah 90 derajat (5.c) dan gambar keempat merupakan manipulasi dengan memperbesar dan perubahan arah 180 derajat (5.d). Sistem pendeteksi menggunakan algoritma SIFT [3] dan hasilnya akan merupakan fitur vektor kolom yang nanti akan dicari kedekatannya dan dibandingkan jarak kedekatan antara hasil terdekat pertama dan kedua. Jika terdeteksi tetangga terdekat diantara dua buah SIFT fitur vektor, sistem menganggap bahwa gambar merupakan gambar yang sudah termanipulasi. Aturan pada penulisan ini membandingkan nilai perbandingan jarak ( $dr$ ) berupa  $dr < 0.1$ ,  $dr < 0.3$ ,  $dr < 0.55$  dan  $dr < 0.8$ . Pada penelitian Huang dkk, penulis di publikasi tersebut menyarankan menggunakan perbandingan jarak  $dr < 0.3$  [4] dan pada David Lowe SIFT menggunakan  $dr < 0.8$  [3].



Gambar 4. Diagram Alir Desain Sistem Pendeteksi



Gambar 5. Gambar asli (a) dan ketiga gambar manipulasi (b,c,d).

#### 4. Hasil dan Diskusi

Hasil dari penelitian ini ditampilkan pada Tabel 1 serta Gambar 6, 7 dan 8. Dari Tabel 1 dapat dilihat jika bagian yang dimanipulasi (*copy-move*) diperkecil maka total titik kunci juga berkurang, sedangkan jika gambar diperbesar maka total titik kunci akan bertambah. Pada gambar 6, 7 dan 8 dapat terlihat hasil dari penelitian ini. Gambar 6,7,8 (a) akan memperlihatkan gambar manipulasi asli, sedangkan (b) adalah hasil kecocokan dengan perbandingan jarak  $dr < 0.1$ , (c) adalah hasil kecocokan dengan perbandingan jarak  $dr < 0.3$ , (d) adalah hasil kecocokan dengan perbandingan jarak  $dr < 0.55$  dan (e) adalah hasil kecocokan dengan perbandingan jarak  $dr < 0.8$ . Hasil kecocokan ini memperlihatkan hasil pendeteksian sistem dalam menganalisis gambar manipulasi penyerangan *copy-move*. Terlihat bahwa rata-rata hasil terbaik didapatkan pada penggunaan  $dr < 0.3$ .

Pada Gambar 6 dimana manipulasi bagian gambar bunga dengan ukuran dan arah yang sama, penggunaan  $dr < 0.1$  memberikan hasil lebih baik dibandingkan penggunaan  $dr$  lainnya. Semakin besar nilai  $dr$  semakin kurang baik (semakin banyak kecocokan yang salah) hasil deteksi *copy-move* pada Gambar 6. Pada Gambar 7 dimana manipulasi mengubah ukuran bunga menjadi lebih kecil dan diputar sebesar 90 derajat, hasil terbaik didapatkan dari penggunaan  $dr < 0.3$ . Pada penggunaan  $dr < 0.1$ , tidak terdapat kecocokan sama sekali. Sedangkan pada penggunaan  $dr < 0.55$  dan  $dr < 0.8$  menghasilkan semakin banyak kecocokan yang salah. Pada Gambar 8 dimana manipulasi mengubah ukuran gambar menjadi besar dan diputar sebesar 180 derajat, hasil kecocokan yang benar baru

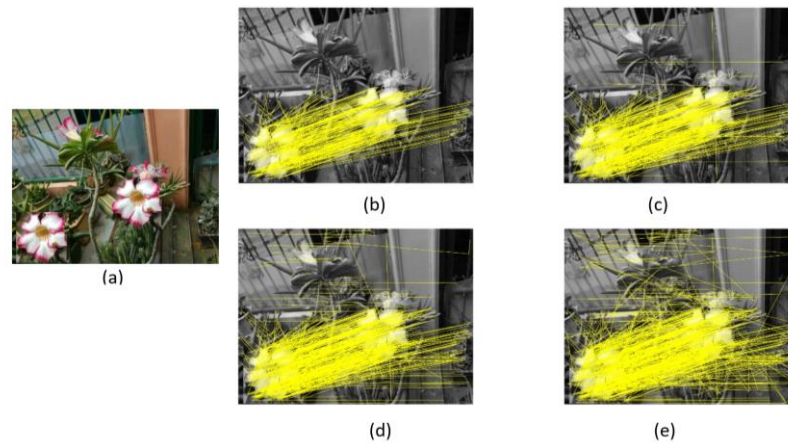


terlihat ketika menggunakan  $dr < 0.8$ . Tidak ada hasil kecocokan pada penggunaan  $dr < 0.1$ . Penggunaan  $dr < 0.3$  dan  $dr < 0.55$  memberikan hasil kecocokan yang salah.

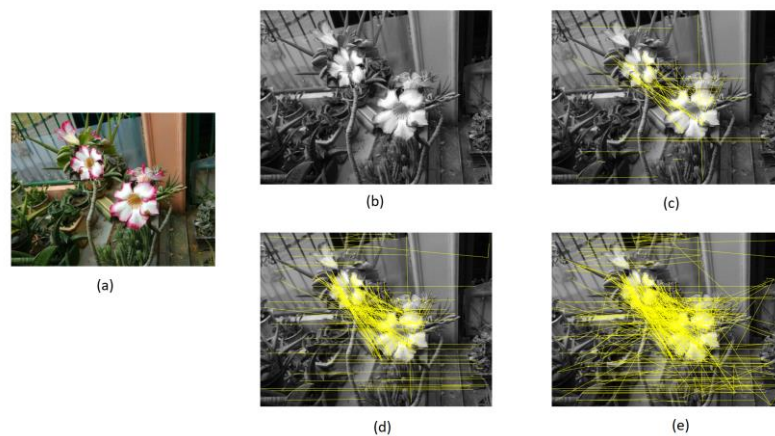
Metode SIFT oleh David Lowe [3] memberikan hasil terbaik ketika bagian bunga yang disalin tidak diubah baik ukuran dan arahnya dengan menggunakan perbandingan jarak antara hasil kedekatan pertama dan kedua diantara SIFT fitur vektor kurang dari 0.3. Metode ini juga masih dapat mendeteksi pemalsuan gambar hasil manipulasi ketika ukuran dan arah diubah dengan menyesuaikan perbandingan jarak  $dr$  walaupun terdapat beberapa hasil kecocokan yang salah.

Tabel 1. Contoh tabel

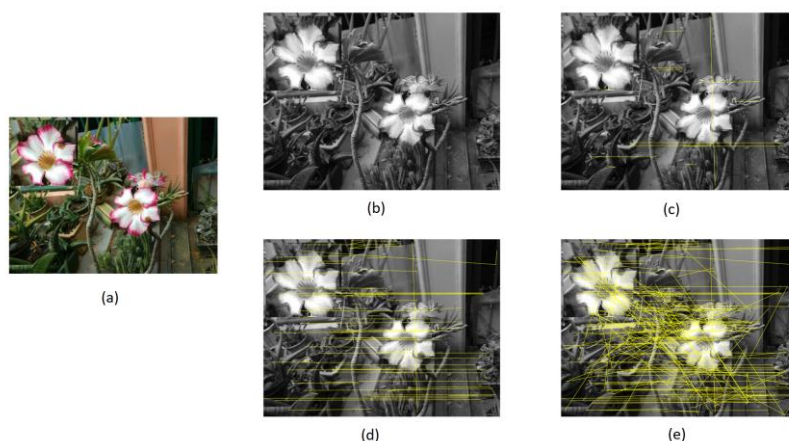
	Total Titik Kunci		
	Gambar manipulasi 1	Gambar manipulasi 2	Gambar manipulasi 3
Banyak Titik Kunci	4407	4333	4557



Gambar 6. Gambar asli manipulasi 1 (a); hasil dengan  $dr < 0.1$  (b); hasil dengan  $dr < 0.3$  (c); hasil dengan  $dr < 0.55$  (d); hasil dengan  $dr < 0.8$  (e).



Gambar 7. Gambar asli manipulasi 2 (a); hasil dengan  $dr < 0.1$  (b); hasil dengan  $dr < 0.3$  (c); hasil dengan  $dr < 0.55$  (d); hasil dengan  $dr < 0.8$  (e).



Gambar 8. Gambar asli manipulasi 3 (a); hasil dengan  $dr < 0.1$  (b); hasil dengan  $dr < 0.3$  (c); hasil dengan  $dr < 0.55$  (d); hasil dengan  $dr < 0.8$  (e).

## 5. Kesimpulan

Penelitian ini mencoba menggunakan metode SIFT yang dikembangkan oleh David Lowe untuk mendeteksi pemalsuan pada gambar yang telah dimanipulasi dengan penyerangan jenis *copy-move*. Hasil terbaik didapatkan beragam dengan menggunakan perbandingan jarak hasil kedekatan pertama dan kedua diantara SIFT fitur vektor,  $dr$ , bervariasi diantara  $dr < 0.1$  hingga  $dr < 0.8$ . Metode SIFT oleh David Lowe dapat mendeteksi gambar yang disalin ketika ukuran dan arah tidak diubah dan masih dapat mendeteksi ketika ada perubahan arah dan ukuran walaupun terdapat beberapa kecocokan yang salah.

## Daftar Pustaka

- [1] O. M. Al-Qershi dan Bee Ee Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," *Forensic science international*, 231.1 (2013): 284-295.
- [2] S. H. Lee, O. Tae-Woo, K. Kibom dan L. Hae-Yeoun, "Digital Camera Identification Using Sensor Pattern Noise." in *The Second International Conference on Information Security and Digital Forensics*, p. 30. 2015.
- [3] D. G. Lowe, "Distinctive image features from scale-invariant keypoints." *International journal of computer vision* 60.2 (2004): 91-110.
- [4] H. Huang, W. Guo dan Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Wuhan, 2008, pp. 272-276.
- [5] W. Burger dan M. J. Burge, *Principles of Digital Image Processing: Advanced Methods*, London: Springer-Verlag, 2013: 229-296.
- [6] R. Lionnie dan Mudrik Alaydrus. "Hierarchical Gaussian Scale-Space on Androgenic Hair Pattern Recognition." *TELKOMNIKA (Telecommunication Computing Electronics and Control)* 15.1 (2016): 522-530.