

# Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital

## (Application of SURF Technique in Image Forensic for Digital Photo Engineering Analysis)

Wicaksono Yuli Sulisty<sup>1</sup>, Imam Riadi<sup>2</sup>, Anton Yudhana<sup>3</sup>

<sup>1</sup>Program Studi Teknik Informatika – Universitas Ahmad Dahlan

<sup>2</sup>Program Studi Sistem Informasi – Universitas Ahmad Dahlan

<sup>3</sup>Program Studi Teknik Elektro – Universitas Ahmad Dahlan

<sup>1</sup>imam.riadi@is.uad.ac.id

<sup>2</sup>eyudhana@ee.uad.ac.id

<sup>3</sup>wicaksono1807048009@webmail.uad.ac.id

**Abstrak** - Perkembangan teknologi citra digital yang semakin maju membuat mudahnya merekayasa suatu citra. Perubahan pada citra membuat informasi yang disampaikan menjadi berubah dan rawan dimanfaatkan menjadi aksi kejahatan digital. Salah satu cara menyelesaikan kasus kejahatan digital ini menggunakan forensik citra. Penelitian ini menggunakan metode teknik pendeteksian rekayasa foto digital *Speeded Up Robust Features* (SURF). Tahapan pertama melakukan pengakuisisi data kemudian melakukan proses ekstraksi dengan hasil akuisisi tersebut. Hasil yang sudah didapat dianalisis menggunakan algoritma SURF, algoritma ini mendeteksi adanya manipulasi pada foto dengan tidak adanya *keypoint* pada beberapa objek yang tidak terhubung. Rekayasa foto digital dapat dipastikan menggunakan perbandingan kualitas citra pada setiap foto dengan perhitungan MSE, RMSE dan PSNR. Hasil perbandingan nilai kualitas didapat perbedaan antara nilai kualitas pada foto asli dan foto manipulasi, hal tersebut dapat membuktikan bahwa foto tersebut sudah dimanipulasi.

**Kata-kata kunci:** forensik, citra digital, SURF, rekayasa

*Abstract* - The development of increasingly advanced digital image technology makes it easy to engineer an image. Changes to the image make the information conveyed change and are prone to be used as digital crime. One way to solve digital crime cases is by using image forensics. This study uses the technique of detecting digital photo engineering *Speeded Up Robust Features* (SURF). The first stage is to acquire data and then carry out the extraction process with the results of the acquisition. The results that have been obtained are analyzed using the SURF algorithm; this algorithm detects manipulation of the photo in the absence of *keypoint* on some unconnected objects. Digital

*photo engineering can be ascertained using a comparison of image quality in each photo with MSE, RMSE, and PSNR calculations. The results of the comparison of the quality values obtained difference between the quality values on the original photo and photo manipulation; it can prove that the photo has been manipulated.*

**Key words:** forensic, digital image, SURF, manipulation

### I. PENDAHULUAN

Perkembangan teknologi citra digital yang semakin maju membuat mudahnya merubah atau memodifikasi foto sehingga pemalsuan citra semakin marak. Teknik manipulasi citra yang semakin berkembang membuat orang yang melihat merasa kesulitan untuk membedakan foto asli dan manipulasi [1]. Kegiatan manipulasi citra sering kali dilakukan sebelum citra tersebut dipublikasi [2]. Manipulasi citra memiliki tujuan seperti memperbaiki *background* dan memanipulasi bagian tertentu. Selain itu juga bisa digunakan hal-hal yang negatif seperti menyindir atau menjatuhkan orang lain dan menyebarkan berita hoaks [3].

Citra dapat diambil dengan kamera yang menghasilkan gambar persis sesuai dengan keadaan objek [4][5][6]. Citra atau gambar digital dapat digunakan sebagai media komunikasi untuk menyampaikan informasi. Keaslian suatu citra memiliki peran penting karena jika citra sudah dimanipulasi dapat merubah informasi yang disampaikan sebagai bentuk informasi visual [7]. Pengolahan citra digital dapat dibuat dan diedit dengan mudah menggunakan beberapa *tools*, seperti Adobe Photoshop, GIMP dan PhotoScape [8].

Kemajuan teknologi dalam bidang informasi, komunikasi dan media telah mengubah pola pikir dan perilaku masyarakat. Hal tersebut menyebabkan perubahan budaya, ekonomi dan sosial secara signifikan. Teknologi informasi saat ini bisa dikatakan sebagai pedang bermata dua, karena selain dapat memberi dampak negatif juga memberi dampak positif [9]. Berbagai aksi kejahatan yang menggunakan teknologi informasi dan internet sebagai medianya disebut dengan istilah *cybercrime* [10]. Maraknya kasus *cybercrime* seperti ujaran kebencian atau *cyberbully* sudah sangat tinggi di Indonesia. Jumlah kasus ujaran kebencian yang ditangani Polri selama 2017 adalah sebanyak 3.325 kasus, sementara pada tahun 2016 adalah 1.829 kasus sedangkan menurut suatu media berita untuk tahun 2018 sebanyak 4 ribuan kasus [11]. Data tersebut membuktikan bahwa kejahatan *cybercrime* ini semakin tahun semakin meningkat, untuk menghindari hal-hal tersebut diperlukan suatu langkah yang dapat memberikan kepastian dan penanganan terhadap kasus *cybercrime*. Hal itulah yang menyebabkan munculnya *digital forensics* untuk keperluan pembuktian secara hukum didalam suatu persidangan [12].

Forensik digital dapat membantu secara teknis pada pengumpulan bukti-bukti secara digital untuk disajikan dalam suatu persidangan yang sesuai dengan hukum yang berlaku [13]. Salah satu contoh bidang ilmu *digital forensics* adalah *image forensics* yang bertujuan untuk pengumpulan dan mencari fakta-fakta pembuktian dalam menentukan keaslian citra atau gambar [14]. Berbagai kasus kriminal dan pornografi yang melibatkan file gambar masih sering terjadi, oleh karena itu forensik terhadap gambar sebagai barang bukti menjadi kunci penting untuk membantu pengadilan dalam mengambil keputusan

Suatu kasus *cybercrime* yang terjadi akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti. Barang bukti *cybercrime* dapat berupa barang bukti digital dan barang bukti elektronik. Contoh barang bukti elektronik adalah *smartphone* dan contoh barang bukti digital adalah citra atau gambar [15][16]. Metode untuk pengangkatan barang bukti digital pada forensik digital dibagi menjadi dua teknik yaitu *live forensic* dan *static forensic* [17][18]. Akuisisi pada perangkat yang tidak aktif disebut *static forensic* sedangkan akuisisi perangkat secara langsung pada sistem yang berjalan disebut dengan *live forensic*.

Penelitian yang terdahulu diantaranya adalah penelitian tentang Fotoforensic, dengan hasil yang diperoleh bahwa fitur dari [www.fotoforensics.com](http://www.fotoforensics.com) dapat digunakan sebagai deteksi keaslian citra atau gambar

yang tepat. Fasilitas yang disediakan dari [fotoforensics.com](http://fotoforensics.com) dapat digunakan dan sangat efisien untuk mendeteksi keaslian foto terutama pada fitur ELA (Error Level Analysis) [19]. Penelitian tersebut hanya menunjukkan bagian foto yang pernah dimanipulasi dengan menampilkan perbedaan dan membandingkan gradien warna pada foto asli dan manipulasi. Perbedaan dengan penelitian ini yaitu pada proses forensik yang berjalan ketika terdapat suatu kasus yang melibatkan gambar pada suatu *device*, dan proses analisa menggunakan algoritma SURF serta pengukuran kualitas citra. Hal ini bertujuan untuk mendapatkan barang bukti digital yaitu foto yang pernah dimanipulasi dalam kasus *cybercrime*. Tujuan dari SURF adalah sebagai fitur *descriptor* yang dapat mencocokkan suatu objek dari dua gambar yang berbeda. Fitur gambar biasanya digunakan dalam pengambilan gambar, pencocokan gambar, deteksi objek, pengenalan situasi atau tempat [20]. Pengukuran kualitas citra dilakukan untuk membandingkan nilai foto asli dan manipulasi.

Analisis *image forensic* pada penelitian ini menggunakan metode *Speeded Up Robust Features* (SURF), dengan membuat skenario kasus *cybercrime* berupa bukti digital berupa *smartphone*. Proses forensik yang dilakukan berupa pengambilan barang bukti (akuisisi) dan analisis barang bukti digital yang didapat.

## II. METODE

### A. Alur Penelitian

Penelitian ini membuat suatu skenario yang menggunakan 4 buah foto yang sudah disiapkan, yang terdiri dari 2 buah foto asli dan 2 buah foto hasil manipulasinya. Keempat buah foto tersebut didapat dari sebuah barang bukti *smartphone* yang di indikasikan sebagai barang bukti elektronik pada kasus *cybercrime*. Proses forensik untuk pengambilan barang bukti digambarkan pada diagram alir pada Gambar 1.



**Gambar 1. Diagram alir proses pengambilan barang bukti**

Gambar 1 menunjukkan diagram alir dalam proses pengambilan barang bukti digital. Pengambilan barang bukti berawal dari barang bukti elektronik yang sudah didapat, kemudian diakuisisi semua datanya dan membuat *backup* untuk menjaga barang bukti digital. Gambar 2 merupakan diagram alir proses pendeteksian gambar.



**Gambar 2. Diagram alir proses pendeteksian gambar**

Gambar 2 menunjukkan diagram alir proses pendeteksian barang bukti digital berupa gambar. Proses pendeteksian diawali dengan penginputan barang bukti gambar. Barang bukti tersebut diproses menggunakan algoritma SURF untuk mendeteksi gangguan pada gambar. Proses selanjutnya membandingkan nilai kualitas citra yang berupa MSE, RMSE dan PSNR pada foto asli dan foto manipulasi kemudian dianalisis hasilnya sehingga didapat kesimpulan barang bukti pada kasus rekayasa foto digital.

### B. Speeded Up Robust Features (SURF)

SURF merupakan sebuah metode deteksi fitur yang menggunakan *keypoint* dari sebuah gambar atau citra [21]. *Keypoint* merupakan bagian-bagian dari sebuah citra yang nilainya kuat dan tetap ketika mengalami perubahan rotasi, *blurring*, skala, transformasi tiga dimensi, perubahan bentuk [22]. Metode SURF dapat mendeteksi fitur lokal yang stabil dalam tingkat skala gambar yang berbeda, tahan terhadap transformasi geometri dan variasi pencahayaan [23]. Metode SURF terdiri dari beberapa tahapan yaitu:

1) *Interest Point Detector*: Deteksi titik perhatian (*interest point*) digunakan untuk memilih titik yang mengandung banyak informasi dan sekaligus stabil terhadap gangguan lokal atau global dalam citra digital. Algoritma SURF, mempunyai *interest point detector* yang mempunyai sifat invarian terhadap skala, yaitu *blob detection*. *Blob* merupakan area pada citra digital yang memiliki sifat yang konstan atau bervariasi dalam kisaran tertentu [24].

2) *Scale Space Representation*: Ukuran citra yang tidak seragam menjadi faktor kesulitan dalam proses membandingkan fitur yang terdapat dalam sebuah citra. Terkait hal tersebut maka diperlukan suatu mekanisme tersendiri yang dapat menyelesaikan proses dan menangani perbedaan ukuran dengan menggunakan metode perbandingan skala. Metode *scale space* menggunakan citra yang diimplementasikan dalam bentuk sebuah *image pyramid* [25].

3) *Feature Description*: Fitur didefinisikan sebagai bagian yang mengandung banyak informasi pada sebuah citra. *Feature description* digunakan sebagai titik awal untuk algoritma deteksi objek. Tujuan dari proses deteksi fitur ini adalah untuk mendapatkan deskripsi dari fitur-fitur dalam citra yang diamati [25].

### III. HASIL DAN PEMBAHASAN

#### A. Akusisi Barang Bukti Digital

Penelitian ini menggunakan *hardware* dan *software* untuk mendukung proses forensik. Tahap ini merupakan proses merencanakan *hardware* dan *software* yang akan digunakan dan tindakan-tindakan yang akan dilakukan pada saat penelitian. Perencanaan diperlukan agar proses penelitian berjalan lancar termasuk dalam menentukan *tools* yang akan digunakan pada proses penelitian sehingga dapat diperoleh hasil penelitian yang valid, selain itu pada tahap ini juga dibuat skema tahap penelitian dan skema simulasi pengujian. *Hardware* dan *software* yang digunakan adalah sebagai berikut.

##### 1) Hardware

- Intel® Core™ i7-6700K CPU @ 4,00 Ghz
- RAM 32 GB
- Motherboard Gigabyte Technology Z179X-Gaming 5
- NVIDIA GeForce GTX 980 TI 6GB
- SSD 256 GB
- Monitor Samsung
- Keyboard dan Mouse Logitech
- PSU 1200 Watt
- EVERCROSS B75

##### 2) Software

- Matlab r2017a
- MOBILedit Forensic Express

Proses pertama yang dilakukan adalah *collection* dengan menggunakan barang bukti berupa *smartphone*. *Smartphone* yang digunakan adalah Evercross dengan sistem operasi Android Lolipop. Bahan *smartphone* yang digunakan seperti pada Gambar 3.

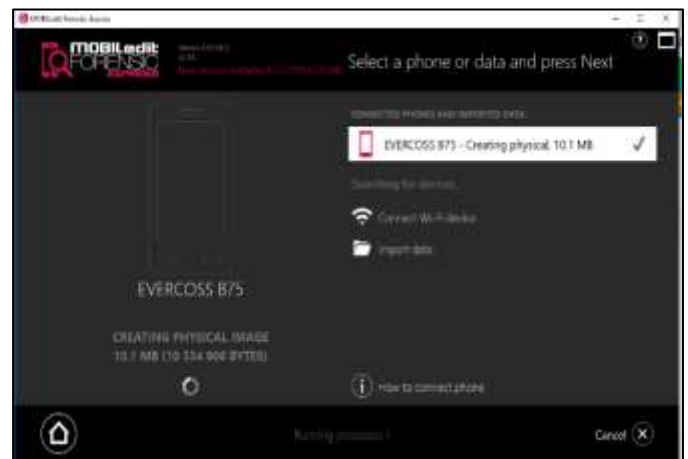


Gambar 3. *Smartphone* yang digunakan

Gambar 3 menunjukkan *smartphone* yang digunakan dalam penelitian ini. Setelah mendapatkan barang bukti elektronik tersebut maka harus dilakukan proses *cloning* dan *backup* untuk menjaga keaslian barang bukti, sehingga yang digunakan untuk menganalisis barang bukti digital adalah hasil *cloning* tersebut atau biasa disebut dengan proses akuisisi data seperti pada Gambar 4.

Gambar 4 menampilkan *tool* yang digunakan untuk proses *cloning*, *backup* dan ekstraksi data menggunakan MOBILedit Forensic Express. Proses akuisisi ini membutuhkan waktu yang cukup lama, tergantung dari kapasitas memori *smartphone* yang digunakan. Hasil dari proses ini adalah seperti pada Gambar 5.

Gambar 5 menunjukkan hasil yang didapat dari proses akuisisi data *smartphone*. Hasil yang didapat berupa file tipe Disc Image dan satu folder yang berisi ekstraksi dari *smartphone*. Setelah *smartphone* sudah melalui proses *collection* maka langkah selanjutnya adalah *Examination*, yaitu pengambilan dan penyaringan data pada bagian tertentu dari sumber data. Penelitian ini berfokus pada gambar, sehingga data yang diambil dari *smartphone* adalah foto-fotonya. Beberapa gambar yang sudah didapat adalah seperti pada Tabel I.



Gambar 4. Proses *clone* dan ekstraksi pada MOBILedit

Name	Date modified	Type	Size
EVERCROSS B75 (2019-07-09 17h01m00s)	7/9/2019 5:30 PM	File folder	
samsung SM-G130H (2019-07-08 22h03...)	7/8/2019 10:29 PM	File folder	
EVERCROSS B75	7/9/2019 4:53 PM	Disc Image File	15,267,840 ...
EVERCROSS B75.img_info	7/9/2019 4:53 PM	WinRAR ZIP archive	3 KB
samsung SM-G130H	7/8/2019 9:58 PM	Disc Image File	3,817,472 KB
samsung SM-G130H.img_info	7/8/2019 9:58 PM	WinRAR ZIP archive	2 KB

Gambar 5. Hasil *clone* dan ekstraksi pada MOBILedit

TABEL I  
FOTO YANG DIDAPAT DARI PROSES EKSTRAKSI

No	Foto	Penjelasan	Foto	Penjelasan
1		Foto Asli		Foto Manipulasi Image Splicing
	a		b	
2		Foto Asli		Foto Manipulasi Copy-move
	c		d	

Tabel 1. merupakan beberapa gambar yang didapat dari barang bukti elektronik yang berupa 2 buah foto asli dan 2 buah foto manipulasi berjenis *copy-move* dan *image splicing*.

### B. Analisis Pendeteksian

Foto yang didapat dari proses *examination* kemudian dianalisis menggunakan algoritma SURF dan perhitungan kualitas citra dengan menggunakan *tools* MATLAB, hal tersebut dilakukan untuk membuktikan apabila foto tersebut pernah dimanipulasi. Metode algoritma SURF yang digunakan adalah fungsi yang dapat membaca dua gambar dan menampilkan garis yang menghubungkan *keypoint* yang cocok. Cara kerja algoritma ini adalah dengan menginputkan dua foto sehingga dapat ditemukan *keypoint-keypoint* pada tiap objek pada foto sehingga dapat ditemukan mana objek yang tidak memiliki *keypoint* pada foto tersebut. Gambar 6. merupakan proses hasil penggunaan algoritma SURF.

Gambar 6 merupakan hasil yang didapat dari pendeteksian menggunakan algoritma SURF. Gambar (a)

terdapat satu buah objek orang pada foto asli, sedangkan pada foto manipulasi terdapat dua buah objek. Jika kedua buah foto tersebut asli maka masing-masing objek tersebut mempunyai *keypoint* yang terhubung, sedangkan pada gambar (a) ada satu buah objek yang tidak memiliki *keypoint* yang terhubung sehingga dapat simpulkan gambar tersebut merupakan foto manipulasi.

Hal tersebut juga berlaku sama seperti pada gambar (b) yang memiliki satu objek orang pada foto asli, sedangkan pada foto manipulasi terdapat tiga buah objek. Gambar (b) memiliki dua buah objek yang tidak memiliki *keypoint* yang terhubung sehingga dapat simpulkan gambar tersebut merupakan foto manipulasi.

Teknik lain yang dapat digunakan adalah Pengukuran kualitas citra kemudian membandingkan nilai kualitas dari kedua foto dari nilai MSE, RMSE dan PSNR. Perbedaan nilai kualitas pada kedua foto pembandingan dapat mendeteksi suatu manipulasi yang pernah dilakukan. Tabel 2 merupakan nilai kualitas citra pada keempat foto.



(a)



(b)

**Gambar 6. Hasil proses menggunakan algoritma SURF**

Tabel II menampilkan nilai MSE, RMSE dan PSNR dari masing-masing foto pada bahan penelitian. Jika foto a dibandingkan dengan foto b terdapat perbedaan dari ketiga nilai kualitas maka dapat dipastikan bahwa foto b merupakan foto yang sudah pernah dimanipulasi. Foto d merupakan foto manipulasi yang memiliki nilai kualitas citra yang berbeda, hal tersebut membuktikan bahwa dengan penambahan objek dari dalam maupun dari luar foto dapat merubah nilai kualitas citra sehingga foto tersebut sudah pasti pernah dimanipulasi. Beberapa foto setelah dimanipulasi mempunyai nilai PSNR lebih tinggi sehingga kualitasnya semakin bagus, namun hal tersebut sudah termasuk manipulasi citra. Tahap selanjutnya adalah menyimpulkan hasil analisis atau bisa disebut dengan proses *report*, berikut hasil dari *tools* forensik yang sudah didapat yang disajikan pada Tabel III.

Tabel III menunjukkan hasil yang didapat dari proses perbandingan antara foto asli dan manipulasi. Dua buah foto manipulasi yang disiapkan pada skenario dapat dideteksi menggunakan algoritma SURF dan

perbandingan kualitas citra menggunakan *software* MATLAB.

TABEL II  
HASIL PERBANDINGAN NILAI KUALITAS CITRA

No	Jenis Foto	MSE	RMSE	PSNR
1	Foto asli (a)	25.1016	5.01014	34.1678
	Foto manipulasi (b)	25.095	5.00949	34.1689
2	Foto asli (c)	25.4984	5.04959	34.0997
	Foto manipulasi (d)	25.5391	5.05362	34.0927

TABEL III  
PENDETEKSIAN REKAYASA FOTO

Perbandingan Foto	Algoritma SURF	Kualitas Citra
Foto a dan b	Terdeteksi	Terdeteksi
Foto c dan d	Terdeteksi	Terdeteksi

#### IV. PENUTUP

Hasil proses penelitian yang telah dilakukan menggunakan skenario kasus berupa *smartphone* didapat barang bukti digital berupa foto. Foto tersebut diproses dan dianalisis menggunakan algoritma SURF dan perbandingan kualitas citra. Proses analisis menggunakan algoritma SURF dapat mendeteksi adanya manipulasi pada foto dengan tidak ditemukannya *keypoint* pada beberapa objek yang tidak terhubung pada citra penelitian. Proses deteksi lainnya menggunakan perbandingan nilai kualitas citra dengan parameter perhitungan MSE, RMSE dan PSNR. Perbandingan nilai kualitas citra yang telah dilakukan didapat perbedaan antara nilai kualitas pada foto asli dan manipulasi. Perbedaan nilai kualitas citra dapat membuktikan bahwa foto tersebut benar-benar sudah dimanipulasi. Beberapa foto yang telah dimanipulasi mempunyai nilai PSNR lebih tinggi sehingga kualitasnya semakin bagus, namun hal tersebut sudah termasuk manipulasi citra. Berdasarkan pengujian yang dilakukan maka empat buah foto pada bahan penelitian terdapat dua foto yang manipulasi.

#### DAFTAR PUSTAKA

- [1] A. Y. Wijaya, S. Al Musayyab, and H. Studiawan, "Pengembangan Metode Block Matching Untuk Deteksi Copy-Move Pada Pemalsuan Citra," *JUTI J. Ilm. Teknol. Inf.*, vol. 15, no. 1, pp. 84–94, 2017.
- [2] P. E. Kresnha, E. Susilowati, and Y. Adharani, "Pendeteksian Manipulasi Citra Berbasis Copy-move Forgery Menggunakan Euclidean Distance dengan Single Value Decomposition," *Semin. Nas. Teknol. Inf. dan Multimed. 2016*, vol. 4, no. 1, pp. 6–7, 2016.
- [3] D. A. Febrianda, D. Andreswari, and E. P. Wulandari, "Sistem Autentifikasi Citra Digital Terintegrasi Dengan Error Level Analysis (Ela) Dan Color Filter Array (Cfa) Berbasis Web," vol. 4, no. 1, pp. 45–56, 2018.
- [4] Sunardi, A. Yudhana, and S. Saifullah, "Identity Analysis of Egg Based on Digital and Thermal Imaging: Image Processing and Counting Object Concept," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 1, pp. 200–208, 2017.
- [5] S. Saifullah, S. -, and A. Yudhana, "Analisis Perbandingan Pengolahan Citra Asli Dan Hasil Cropping Untuk Identifikasi Telur," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 3, pp. 341–350, 2018.
- [6] A. Yudhana, R. Umar, and F. M. Ayudewi, "The Monitoring of Corn Sprouts Growth Using the Region Growing Methods," *J. Phys. Conf. Ser.*, vol. 1373, no. 1, pp. 1–6, 2019.
- [7] M. M. Efendi, "Metode deteksi tepi block jpeg terkompresi untuk meningkatkan akurasi analisis manipulasi splicing pada citra berekstensi jpeg," Universitas Islam Indonesia, 2018.
- [8] Rosidin, "Analisis Pendeteksi Kecocokan Objek Pada Citra Digital Menggunakan Matlab Dengan Metode Algoritma SIFT," Universitas Islam Indonesia, 2018.
- [9] A. A. Agus and Riskawati, "Penanganan Kasus Cyber Crime di Kota Makasar( Studi Pada Kantor Kepolisian Resort Kota Besar Makassar)," *J. Supremasi*, vol. 11, no. 1, pp. 20–29, 2016.
- [10] Antoni, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online," *Nurani J. Kaji. Syari'ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018.
- [11] E. Chintia, R. Nadiyah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and N. A. Rakhmawanti, "Kasus Kejahatan Siber Yang Paling Banyak Terjadi Di Indonesia Dan Penanganannya," *J. Inf. Eng. Educ. Technol.*, vol. 2, no. 2, pp. 101–110, 2018.
- [12] K. Tanjung, "Analisis Citra Berformat JPEG Hasil Olahan Dari Citra Original Berdasarkan Metode Matching Block Dan Deteksi Tepi Block JPEG Terkompresi," Universitas Sumatra Utara, 2015.
- [13] A. Febriyanto and I. Sembiring, "Uji Perbandingan Tools Mobile Forensic Pada Platform Java, Blackberry dan Android," Universitas Kristen Satya Wacana, 2016.
- [14] R. Umar, A. Fadlil, and A. I. Putra, "Analisis Forensics Untuk Mendeteksi Pemalsuan Video," *J. Sains Komput. dan Inform.*, vol. 3, no. 2, pp. 193–200, 2019.
- [15] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *ELINVO (Electronics, Informatics, Vocat. Educ.)*, vol. 3, no. 1, pp. 70–82, 2018.
- [16] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic Tools Performance Analysis on Android-Based Blackberry Messenger using NIST Measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018.
- [17] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions Using Live Forensics Method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018.
- [18] I. M. Nasrulloh, S. Sunardi, and I. Riadi, "Analisis Forensik Solid State Drive (SSD) Menggunakan Framework Rapid Response," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, pp. 509–518, 2019.
- [19] F. Mahardika, A. D. Khatulistian, and A. P. Kuncoro, "Review Foto Forensic.com dengan Teknik Error Level Analysis dan JPEG untuk mengetahui Citra Asli," *J. Inform. J. Pengemb. IT Poltek Tegal*, vol. 03, no. 01, pp. 71–75, 2018.
- [20] M. Gunarso and L. A. Muharom, "Deteksi Objek pada Gambar Menggunakan Algoritma Speeded Up Robust Feature (SURF)," *J. Undergrad. Thesis, Univ. Muhammadiyah Jember*, 2016.

- [21] F. A. Lubis *et al.*, “Implementasi Metode Speed Up Features Dalam Mendeteksi Wajah,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 3, no. 4, pp. 22–27, 2016.
- [22] W. J. Nuryanto, “Pengenalan Wajah (Face Recognition) Dengan Menggunakan Metode Surf (Speeded Up Robust Features),” Universitas Muhammadiyah Surakarta, 2017.
- [23] R. Lionnie, T. M. Kadarina, and M. Alaydrus, “Analisis Metode SIFT dan SURF untuk Sistem Pendeteksi Gambar Termanipulasi Penyerangan Copy-Move Forgery,” *J. Telekomun. dan Komput.*, vol. 8, no. 3, pp. 183–195, 2018.
- [24] F. P. Hilman and U. Telkom, “Perbandingan Metode Surf Dan Sift Dalam Sistem Identifikasi Tanda Tangan,” *e-Proceeding Eng.*, vol. 2, no. 2, pp. 2467–2481, 2015.
- [25] H. P. Harahap, “Pendeteksi Objek pada Citra Menggunakan Pencocokan Titik-Titik Fitur berbasis Algoritma SURF dan MSER,” *Komputasi*, vol. 13, no. 2, pp. 71–79, 2016.