

Deteksi Foto Palsu Menggunakan *Tools Forensically*

Fajar Ramadhan^a, Erick Irawadi Alwi^b, Abdul Rachman Manga^c

Universitas Muslim Indonesia, Makassar, Indonesia

^a13020190222@umi.ac.id; ^berick.alwi@umi.ac.id; ^cabdulrachman.manga@umi.ac.id

Received: xx xx xxxx | Revised: xx xx xxxx | Accepted: xx xx xxxx | Published: xx xx xxxx

Abstrak

Maraknya foto palsu yang beredar di media sosial menjadi masalah digital yang hampir sebagian besar dijumpai saat ini, menjadikan sebuah foto dapat dimanipulasi dengan mudah sehingga dapat merubah informasi yang disampaikan menjadi berbeda dan membuatnya rawan digunakan untuk tindak kejahatan. Maka dari itu, penelitian ini bertujuan untuk menganalisis sebuah citra digital yang telah dimanipulasi atau direkayasa dengan menggunakan software atau program tertentu. Sedangkan alat analisisnya menggunakan *tools Forensically* yaitu *Forensically Beta* yang terdiri dari 3 metode utama yaitu *Error Level Analysis*, *Clone Detection* dan Metadata. Hasil yang diperoleh untuk setiap metode yaitu metode ELA dapat menampilkan tingkat kesalahan pada sebuah gambar yang menunjukkan terjadinya perubahan pada foto tersebut, metode *Clone Detection* mampu menangkap area pada citra dengan mengambil area yang berasal dari *frame* dan *size* yang sama sedangkan metode Metadata membantu mengidentifikasi dan mendeskripsikan gambar dengan memberikan informasi perangkat yang digunakan, tanggal pengambilan gambar, dan deskripsi foto lainnya. Kesimpulan dari penelitian ini yaitu ketiga metode yang digunakan sangat mendukung untuk digunakan dalam menganalisis foto palsu.

Kata kunci: *Forensically Beta*, *Error Level Analysis*, *Clone Detection*, Metadata.

Pendahuluan

Di era digital saat ini, manipulasi foto menjadi semakin mudah dengan ketersediaan berbagai perangkat lunak pengeditan foto yang canggih dapat menimbulkan pandangan lain dan membentuk opini publik. Namun, kemajuan teknologi pengeditan foto telah membuat manipulasi foto semakin mudah dan sulit dideteksi oleh siapa yang melihatnya [1]. Fenomena ini menimbulkan kekhawatiran serius, terutama ketika foto palsu digunakan untuk menyebarkan informasi yang menyesatkan, manipulasi opini publik, atau bahkan melakukan penipuan. Dengan banyaknya kejahatan yang dilakukan dengan manipulasi foto ini. Diperlukan sebuah mekanisme khusus untuk menganalisis dan menelusuri bukti-bukti digital yang ada [2].

Citra digital menjadi salah satu faktor pendukung dalam menyampaikan informasi sebagai bukti pendukung ataupun penguat gagasan, sehingga yang menerima informasi dapat lebih yakin dengan informasi yang disampaikan. Namun, beberapa orang rela melakukan pemalsuan atau modifikasi citra digital agar citra tersebut dapat dianggap sebagai bukti. Kasus seperti ini bisa dilakukan mengingat kemajuan aplikasi pengolah citra bisa didapatkan dimana saja, mulai dari yang gratis hingga yang berbayar [3].

Kemajuan teknologi saat ini dapat membantu orang untuk mengolah berbagai data sebagai sumber informasi yang dapat diakses dengan cepat dan mudah, tetapi disisi lain hal ini juga menyebabkan penggunaan data informasi menjadi tidak terkendali [4]. Dalam dunia digital saat ini, gambar merupakan data yang paling sering digunakan, mudahnya dalam mengakses berbagai perangkat lunak pengeditan foto membuat foto lebih mudah dimanipulasi [5]. Aktivitas pengolahan foto seperti, manipulasi dan penyuntingan dapat mempengaruhi keaslian suatu foto, yang pada akhirnya dapat mempengaruhi informasi visual yang disampaikan, dimana analisis dan prosesnya menggunakan *software* pada komputer, laptop maupun smartphone atau dengan metode lainnya yang sering digunakan dalam rekayasa sebuah citra digital [6].

Forensically adalah salah satu alat yang dapat digunakan untuk mendeteksi manipulasi foto. Alat ini menyediakan berbagai fitur analisis yang memungkinkan pengguna untuk mengidentifikasi tanda-tanda manipulasi, adapun fitur utama yang disediakan oleh *Forensically*, yaitu *Error Level Analysis* (ELA), *Clone Detection*, dan Metadata [7]. Dengan menggunakan *tools-tools* tersebut hal ini memudahkan untuk mengidentifikasi keaslian foto. Serta hasil yang di dapat dari *tools* tersebut dapat dimanfaatkan menjadi barang bukti digital [8].

Dengan adanya penelitian ini sangat membantu pengidentifikasian suatu foto serta menjaga integritas informasi di dunia digital [9]. Pemahaman yang mendalam tentang cara kerja metode ini, kita dapat meningkatkan

perlindungan terhadap informasi visual, memastikan bahwa foto yang kita lihat adalah representasi yang akurat dari keadaan sebenarnya [10].

Metode

Pada penelitian ini, untuk mendeteksi foto palsu menggunakan *tools Forensically*, digunakan sebuah *tools* deteksi *image* berbasis *online*, yaitu *Forensically Beta*. Untuk mendeteksi foto palsu menggunakan *Forensically Beta*, di gunakan tiga metode utama, yaitu: ELA,CD, dan Metadata [11].

A. Error Level Analysis

Error level Analysis (ELA) adalah teknik forensik yang digunakan untuk mengidentifikasi area dalam gambar yang mungkin telah diubah secara digital. Metode ini dilakukan dengan menganalisis tingkat kompresi dari berbagai bagian gambar. Ketika gambar JPEG disimpan, bagian-bagian yang berbeda dari gambar akan memiliki tingkat kompresi yang berbeda tergantung pada seberapa banyak mereka telah diubah. ELA dapat membantu menyoroti perbedaan ini [12].

1. Proses ELA:
 - a. Gambar diubah menjadi JPEG dengan tingkat kompresi tertentu.
 - b. Hasil gambar tersebut dibandingkan dengan gambar asli.
 - c. Perbandingan kompresi di setiap bagian gambar dianalisa dan di-*highlight*.
2. Interpretasi hasil
Area dengan tingkat kompresi berbeda dapat menunjukkan adanya manipulasi.
3. Parameter yang digunakan dalam *Forensically Beta* pada metode ELA ditunjukkan pada Tabel 1.

Tabel 1. Parameter *Error Level Analysis*

ELA	Parameter	Keterangan
<i>JPEG Quality</i>	90	Kualitas foto saat dilakukan analisa
<i>Error Scale</i>	20	Tingkat kesalahan analisa foto
<i>Opacity</i>	0.90	Transparansi <i>layer</i> pada sebuah foto untuk dapat dilalui cahaya

B. Clone Detection

Clone Detection dalam *Forensically Beta* adalah salah satu fitur yang digunakan untuk mendeteksi area dalam gambar yang mungkin telah disalin dan ditempelkan dari bagian lain dari gambar yang sama. Metode ini berguna untuk mengidentifikasi manipulasi gambar di mana elemen gambar telah diduplikasi untuk menyembunyikan atau mengubah konten [13].

1. Proses *Clone Detection*:
 - a. Algoritma mencari pola yang berulang dalam gambar.
 - b. Area yang diduplikasi di-*highlight*
2. Interpretasi hasil
Area dengan pola berulang dapat menunjukkan adanya manipulasi.
3. Parameter yang digunakan dalam *Forensically Beta* pada metode *Clone Detection* ditunjukkan pada Tabel 2.

Tabel 2. Parameter *Clone Detection*

Clone Detection	Parameter	Keterangan
<i>Minimal Similarity</i>	0.10	<i>Layer</i> pada foto yang memiliki kesamaan warna, bentuk dan ukuran
<i>Minimal detail</i>	1.00	<i>Layer</i> pada foto yang menampilkan <i>layer</i> tertentu yang dianggap paling penting untuk ditampilkan
<i>Minimal Cluster Size</i>	10	<i>Layer</i> atau bagian pada sebuah foto
<i>Block Size</i>	4	Ukuran <i>byte</i> pada sebuah foto
<i>Maximal Image Size</i>	1024	Ukuran keseluruhan sebuah foto

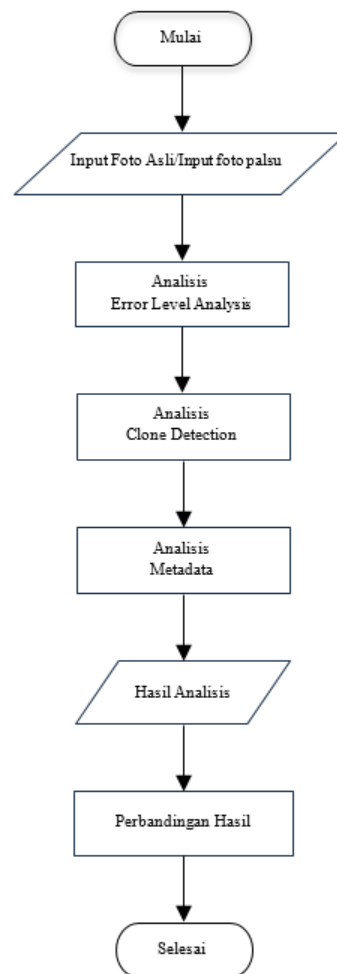
C. Metadata

Metadata adalah informasi tambahan yang disimpan bersama dengan file foto yang memberikan detail tentang file tersebut, seperti kapan dan dimana foto diambil, kamera atau perangkat yang digunakan, dan bahkan informasi tentang perangkat lunak yang digunakan untuk mengedit foto. Metadata dapat sangat

berguna dalam analisis forensik digital untuk memahami lebih banyak tentang asal-usul dan sejarah foto [14].

1. Proses Metadata
 - a. Metadata gambar diekstrak dan diperiksa.
 - b. Inkonsistensi atau perubahan Metadata dianalisis
2. Interpretasi hasil
Metadata yang tidak konsisten atau tidak wajar dapat menunjukkan adanya manipulasi

Perancangan



Gambar 1. *Flowchart*

Pada Gambar 1 menjelaskan alur dari penelitian ini, dari penginputan foto asli dan foto palsu kedalam *Forensically Beta*, lalu kedua foto tersebut dianalisis menggunakan metode ELA untuk melihat hasil kompresi pada kedua foto tersebut, selanjutnya diproses dengan metode *Clone Detection* untuk mendeteksi area pada foto yang mungkin telah dihapus atau ditambahkan, dan yang terakhir adalah foto diproses dengan metode Metadata untuk melihat detail dari *file* foto tersebut. Setelah didapatkan hasil dari proses pendeteksian kedua foto tersebut menggunakan beberapa *tools* pada *Forensically Beta*, Selanjutnya hasil analisis kedua foto diatas menggunakan ketiga metode tadi ditampilkan perbandingan dari kedua foto tersebut [15], [16].

orang-orang pada umumnya akan mengira bahwa Gambar 2 adalah foto palsu dan gambar 3 adalah foto asli, karena Gambar 3 (*Circle K*) adalah salah satu merek yang terkenal dan laku dipasaran. Pada pengujian ini penelitian akan melakukan pendeteksian yang akan membuktikan bahwa Gambar 2 adalah foto asli dan Gambar 3 adalah foto palsu.

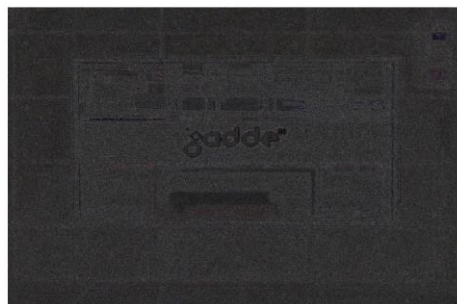


Gambar 2. Foto Asli

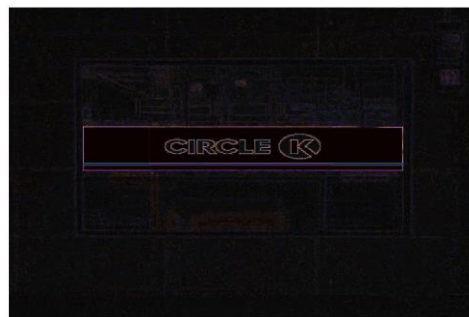


Gambar 3. Foto yang telah di edit

Pemodelan



Gambar 4. Hasil analisis ELA(foto asli)



Gambar 5. Hasil analisis ELA(foto palsu)

Pada Gambar 4 dan Gambar 5 adalah hasil analisis menggunakan metode ELA. Terlihat pada foto asli keseluruhan area pada foto memiliki warna yang sama, yang menandakan keseluruhan area foto masih memiliki tingkat kompresi yang sama, sedangkan pada foto palsu beberapa area pada foto memiliki warna

yang lebih mencolok dibanding area sekitarnya, yang menandakan adanya kemungkinan manipulasi pada foto tersebut.



Gambar 6. Hasil analisis *Clone Detection* (foto Asli)



Gambar 7. Hasil analisis *Clone Detection* (foto palsu)

Gambar 6 dan Gambar 7 adalah hasil analisis menggunakan metode Clone Detection. Setelah dilakukan analisis dengan *Clone Detection* terlihat pada foto asli *Clone Detection* tidak mendeteksi adanya *copy move* area pada foto tersebut, sedangkan pada foto palsu *Clone detection* menangkap adanya *copy move* pada area yang menampilkan merek produk yang menandakan bahwa area tersebut kemungkinan adalah area baru yang telah ditambahkan ke dalam foto tersebut. Analisis dengan metode *Clone Detection* disini semakin memperjelas dugaan hasil analisis pada metode ELA sebelumnya.

ImageWidth	4000
ImageHeight	3000
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	--
Model	--
Orientation	1
SamplesPerPixel	3
XResolution	72
YResolution	72
ResolutionUnit	2
Software	Adobe Photoshop CC 2018 (Windows)
ModifyDate	Wed Jul 24 2024 21:22:23 GMT+0800 (Central Indonesia Time)
YCbCrPositioning	1
GPSLatitudeRef	
GPSLatitude	0
GPSLongitudeRef	
GPSLongitude	0
GPSAltitudeRef	0
GPSAltitude	0
GPSTimeStamp	0,0,0
GPSProcessingMethod	

Gambar 8. Hasil analisis Metadata (asli)

Gambar 8 dan Gambar 9 adalah hasil analisis dengan metode Metadata. Pada Metadata foto asli menampilkan informasi alat yang digunakan dan waktu foto tersebut diambil, sedangkan pada Metadata foto palsu tidak terdapat informasi alat yang digunakan untuk pengambilan foto, tetapi terdapat informasi *software* yang digunakan untuk melakukan editing serta waktu foto tersebut di edit. Analisis dengan Metadata ini menjadi pelengkap hasil analisis pada kedua metode sebelumnya.

ImageWidth	4000
ImageHeight	3000
BitsPerSample	8,8,8
PhotometricInterpretation	2
Make	--
Model	--
Orientation	1
SamplesPerPixel	3
XResolution	72
YResolution	72
ResolutionUnit	2
Software	Adobe Photoshop CC 2018 (Windows)
ModifyDate	Wed Jul 24 2024 21:22:23 GMT+0800 (Central Indonesia Time)
YCbCrPositioning	1
GPSTimeStamp	0,0,0
GPSLatitudeRef	0
GPSLongitudeRef	0
GPSAltitudeRef	0
GPSTimeStamp	0,0,0
GPSProcessingMethod	

Gambar 9. Hasil analisis Metadata (foto palsu)

Kesimpulan

Berdasarkan hasil deteksi yang dilakukan menggunakan *tools forensically*, dengan menggunakan alat *Forensically Beta*, menunjukkan potensi yang signifikan dalam mendeteksi keaslian gambar. Analisis mendalam dengan berbagai metode, yaitu ELA, *Clone Detection*, dan Metadata, memberikan pemahaman yang lebih baik mengenai karakteristik foto asli dan palsu.

Temuan utama dari pengujian ini dengan menggunakan *tools Forensically Beta* dan menerapkan metode ELA, CD dan Metadata baik dalam menyaring informasi terkait foto palsu sebelum konten tersebut disebar. ELA mampu mendeteksi tingkat kompresi suatu foto, yang seringkali merupakan indikasi manipulasi, *Clone Detection* baik dalam mengidentifikasi area *copy move* atau area duplikasi pada foto, yang merupakan teknik manipulasi yang umum digunakan, metadata memberikan informasi perangkat yang digunakan dan waktu pada saat foto tersebut diambil, yang dimana metadata melengkapi hasil pengujian metode sebelumnya.

Daftar Pustaka

- [1] A. M. Afdal, Y. Salim, and A. R. Manga, "Analisis Bukti Digital Forensik Pada Discord Menggunakan Metode National Institute of Standards Technology," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 3, no. 4, pp. 293–300, 2022.
- [2] M. Adam, E. I. Alwi, and I. As'ad, "Analisis Forensik Terhadap Serangan Ddos Ping of Death Pada Server," 2022.
- [3] M. R. Al-Fajri, Caruddin, and D. Yusup, "Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.)*, vol. 6, no. 2, pp. 84–90, 2021.
- [4] A. Firdonsyah and D. Wijayanto, "Analisis Forensik Rekayasa Dokumen Digital dengan Metode NIST," 2022.
- [5] B. Cahya, I. Sahid, M. Kadarman, and R. Hermansyah, "Pemanfaatan Picture Analyzer Untuk Mengidentifikasi Perubahan Pada Gambar Yang Telah Diubah," 2023.
- [6] M. H. Kesuma Arta, I. G. Bagati Kusuma, M. R. Rasyid Askar, B. G. Kurnia Dyatmika, D. Riani, and Lady Hasiani Siahaan, "Analisis Citra Digital Dengan Tools Image Forensic Berupa Fotoforensic, Jpegsnoop, Ghio, Dan Forensically," 2019.
- [7] Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta," *J. Ilm. Matrik*, vol. 21, no. 1, pp. 54–63, 2019.
- [8] S. Moh, M. E. Muhamad, and Salman, "Perbandingan hasil analisa foto hoax menggunakan metode exif/Metadata, reverse image dan forensics," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, No.1, no., pp. 1–5, 2022.
- [9] A. B. Permadi, F. R. Adi Suty, and M. R. Eka Saputra, "Analisis Efektivitas Ingest Module Dalam Mendeteksi Dan Memulihkan Bukti Digital Yang Disamarkan Terenkripsi," 2023.
- [10] L. A. Permana, F. Hakim, Y. A. Subhi, and P. Rivaldo, "Analisis Forensik Keaslian Gambar Menggunakan Autopsy," 2023.
- [11] D. Astria Farook, R. Umar, and I. Riadi, "Deteksi Keaslian Citra Menggunakan Metode Error Level Analysis (ELA) dan Principal Component Analysis (PCA)," *Format J. Ilm. Tek. Inform.*, vol. 8, no. 2, p. 132, 2019.
- [12] I. Sudianto and N. Anwar, "Analisa Forensik Citra Menggunakan Metode Error Level Analysis dan Block Matching," *JSTIE (Jurnal Sarj. Tek. Inform.)*, vol. 11, no. 1, p. 40, Feb. 2023.
- [13] H. Bisri and M. I. Marzuki, "Forensik Citra Digital Menggunakan Metode Error Level Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar," *G-Tech J. Teknol. Terap.*, vol. 7, no. 2, pp. 586–

- 595, 2023.
- [14] K. Nur Isnaini, H. Ashari, and A. P. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 3, no. 2, pp. 72–81, 2020.
- [15] K. Eka Purnama, C. Rozikin, and A. Ali Ridha, "Analisis Forensic Citra Digital Menggunakan Teknik Error Level Analysis Dan Metadata Berdasarkan Metode Nist," *JATI (Jurnal Mhs. Tek. Inform., vol. 7, no. 2, pp. 1100–1107, 2023.*
- [16] F. Harahap, "Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic . org Dengan Metode Error Level Analysis (ELA)," *TIN Terap. Inform. Nusan.*, vol. 2, no. 3, pp. 159–164, 2021.