JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

# PEMANFAATAN FORENSICALLY BETA DAN METADATA2GO DALAM ANALISIS KEASLIAN FOTO DIGITAL

**Maria Chatrin Bunaen[1,*], Ryan Putranda Kristanto[1]**

[1]Teknik Informatika, Universitas Katolik Darma Cendika Surabaya,
maria.chatrin@student.ukdc.ac.id, ryan@ukdc.ac.id

**ABSTRAK**

Maraknya penyebaran gambar digital di era internet saat ini mendorong perlunya verifikasi terhadap keaslian gambar, terutama untuk mencegah penyebaran hoaks dan pencemaran nama baik. Penelitian ini bertujuan menganalisis keaslian gambar digital menggunakan dua alat bantu, yaitu Forensically Beta dan Metadata2Go. Forensically Beta digunakan untuk menganalisis elemen visual seperti tingkat error, pencahayaan, pola kloning, dan noise pada gambar. Sementara Metadata2Go mengekstraksi metadata untuk mengetahui informasi tersembunyi dari gambar seperti waktu pembuatan, perangkat, dan riwayat pengeditan. Hasil penelitian menunjukkan bahwa gambar yang dianalisis telah dimodifikasi dan tidak berasal dari kamera digital secara langsung. Kombinasi dari analisis visual dan metadata terbukti efektif dalam mendeteksi pemalsuan gambar digital secara praktis dan cepat. Temuan ini berkontribusi nyata dalam mendukung proses verifikasi konten visual di dunia jurnalistik, serta dapat dimanfaatkan oleh aparat penegak hukum digital dalam mengidentifikasi bukti manipulasi pada kasus kejahatan siber.

**Kata Kunci**: Analisis Citra, *Forensically Beta*, Forensik Digital, Manipulasi Gambar, Metadata2go

***ABSTRACT***

*The widespread circulation of digital images in today's internet era requires verification of image authenticity, particularly to prevent hoaxes and defamation. This study aims to analyze the authenticity of digital images using two web-based tools: Forensically Beta and Metadata2Go. Forensically Beta was used to examine visual elements such as error levels, lighting gradients, clone patterns, and noise distribution. Metadata2Go extracted hidden metadata to identify information such as creation time, device used, and editing history. The results indicate that the analyzed image had been modified and was not originally captured using a digital camera. The combination of visual analysis and metadata proved effective in detecting digital image forgery in a practical and efficient manner.*

***Keywords****: Digital Forensics, Forensically Beta, Image Analysis, Image Manipulation, Metadata2go*

## PENDAHULUAN

Kemajuan teknologi digital memudahkan masyarakat dalam memproduksi dan menyebarkan informasi visual dalam bentuk gambar atau foto. Namun, di balik kemudahan tersebut, muncul tantangan baru berupa maraknya manipulasi foto digital yang sulit dideteksi dengan mata biasa. Gambar-gambar yang dimanipulasi dapat disalahgunakan untuk menyebarkan hoaks, merusak reputasi seseorang, atau menjadi alat dalam tindak kejahatan siber. Untuk mengatasi hal tersebut, pendekatan forensik digital digunakan sebagai metode penyelidikan bukti elektronik yang dilakukan secara sistematis, terstruktur, dan dapat dipertanggungjawabkan di pengadilan. Forensik digital tidak hanya melibatkan analisis perangkat keras dan perangkat lunak, tetapi juga

memeriksa file digital seperti gambar yang dicurigai telah dimanipulasi. Salah satu cabang penting dalam forensik digital adalah forensik citra digital, yang berfokus pada proses analisis dan validasi keaslian gambar. Citra digital sangat rentan terhadap perubahan, dan tanpa metode yang tepat, sulit membuktikan apakah gambar telah dimodifikasi atau tidak. Oleh karena itu, deteksi manipulasi citra menjadi bagian penting dalam proses investigasi forensik (Harahap, 2021).

Untuk membantu analisis tersebut, tersedia alat bantu gratis seperti Forensically Beta, platform berbasis web yang menyediakan berbagai fitur analisis gambar seperti *Error Level Analysis (ELA)*, *Clone Detection*, *Noise Analysis*, *Luminance Gradient*, dan *Magnifier*. Fitur-fitur ini bekerja dengan cara menganalisis pola pencahayaan, struktur kompresi, hingga kemiripan visual dalam gambar untuk mengungkap adanya potensi manipulasi (Sulistyo et al., 2025). Selain itu, analisis metadata juga menjadi bagian penting dalam proses forensik gambar digital. Alat seperti Metadata2Go dapat membaca metadata tersembunyi dari sebuah gambar, seperti waktu pengambilan gambar, perangkat yang digunakan, serta jejak software pengedit. Metadata ini sering kali menyimpan informasi yang dapat mengindikasikan adanya pengubahan file, meskipun gambar secara visual tampak asli (Bisri & Marzuki, 2023).

Dengan menggabungkan analisis visual menggunakan Forensically Beta dan pemeriksaan metadata melalui Metadata2Go, penelitian ini bertujuan untuk menguji efektivitas kedua alat tersebut dalam menganalisis keaslian gambar digital. Meskipun sejumlah studi sebelumnya telah membahas deteksi manipulasi citra digital, sebagian besar hanya berfokus pada salah satu pendekatan, baik analisis visual maupun metadata secara terpisah. Belum banyak penelitian yang secara eksplisit mengevaluasi kombinasi kedua metode ini dalam satu kerangka analisis untuk mendeteksi manipulasi gambar secara lebih komprehensif. Oleh karena itu, penelitian ini mengisi celah tersebut dengan mengeksplorasi sinergi antara analisis visual dan metadata guna memberikan pendekatan yang lebih akurat, praktis, dan aplikatif dalam konteks verifikasi gambar digital, khususnya untuk mendukung upaya mitigasi hoaks visual dan investigasi kejahatan siber.

## TINJAUAN PUSTAKA

### Forensik Digital

Forensik digital adalah proses ilmiah yang digunakan untuk mengumpulkan, menganalisis, dan melaporkan data digital sebagai alat bukti dalam penyelidikan kejahatan siber. Dalam konteks ini, citra digital merupakan salah satu bentuk bukti digital yang sangat penting, namun rentan terhadap manipulasi dan kerusakan informasi. Oleh karena itu, penting bagi penyelidik untuk menggunakan pendekatan forensik dalam memverifikasi keaslian citra (Hartawan et al., 2022; Iman et al., 2020). Penyelidik forensik tidak cukup hanya bergantung pada perangkat lunak otomatis, tetapi juga perlu memahami proses identifikasi, ekstraksi, dan analisis data untuk dapat mempertanggungjawabkan hasilnya secara hukum (Wibowo, 2023). Proses ini membutuhkan pengetahuan mendalam tentang struktur file digital, sistem file, serta metadata yang menyertainya. Selain itu, penggunaan metode seperti *Error Level Analysis (ELA)*, *Clone Detection (CD)*, dan analisis metadata EXIF menjadi sangat krusial dalam mengungkap adanya indikasi manipulasi gambar secara teknis (Bisri & Marzuki, 2023).

Teknik-teknik ini memungkinkan penyelidik untuk mendeteksi area yang telah diedit, pola penyalinan dalam gambar, serta perubahan atribut teknis yang tidak sesuai dengan citra asli. Dengan demikian, forensik citra digital tidak hanya berguna dalam

membongkar kasus pemalsuan visual di media sosial, tetapi juga memainkan peran penting dalam mendukung proses hukum dengan bukti yang dapat diverifikasi secara ilmiah. Pengetahuan forensik ini harus dikombinasikan dengan keterampilan teknis dan pemahaman konteks digital, agar bukti yang disajikan di pengadilan benar-benar akurat, sahih, dan tidak menimbulkan keraguan terhadap integritas investigasi.

**Forensik Citra Digital**

Forensik citra digital merupakan bagian dari forensik digital yang berfokus pada analisis gambar atau foto untuk mendeteksi adanya rekayasa atau manipulasi. Tujuan utamanya adalah untuk memastikan keaslian informasi visual yang terkandung dalam gambar. Teknik ini sangat diperlukan karena manipulasi citra tidak selalu dapat dideteksi secara visual oleh manusia (Bisri & Marzuki, 2023; Harahap, 2021). Salah satu metode yang umum digunakan adalah Error Level Analysis (ELA). ELA bekerja dengan menyimpan ulang gambar dalam tingkat kompresi tertentu, lalu membandingkan tingkat kesalahan (error) antar area gambar. Area yang telah dimanipulasi akan menunjukkan tingkat error yang lebih tinggi dibandingkan dengan bagian asli gambar (Harahap, 2021; Wicaksono et al., 2022).

**Tools Forensik: Forensically Beta**

Forensically Beta adalah aplikasi berbasis web yang menyediakan berbagai fitur untuk mendeteksi manipulasi gambar digital, di antaranya ELA, Clone Detection, Noise Analysis, Luminance Gradient, dan Magnifier. Penggunaan tool ini dapat membantu penyelidik menemukan bagian gambar yang tidak konsisten secara struktur visual atau pencahayaan. Fitur *Clone Detection* sangat berguna dalam menemukan pola pengulangan atau salinan area dalam gambar, sementara *Luminance Gradient* membantu mengungkap perubahan gradasi cahaya yang mencurigakan (*Forensically Beta*, 2025). Dalam penelitian sebelumnya, penerapan Forensically Beta berhasil membedakan antara citra asli dan yang dimanipulasi, khususnya pada manipulasi jenis *image splicing* yang menghasilkan bintik gelap pada hasil ELA, berbeda dengan bintik terang pada gambar asli. Tools ini tersedia secara online dari website https://29a.ch/photo-forensics/#forensic-magnifier.

**Analisis Metadata Gambar: Metadata2Go**

Metadata merupakan informasi tersembunyi yang tersimpan dalam sebuah file digital. Pada gambar, metadata umumnya mencakup informasi seperti tanggal pembuatan, perangkat kamera, lokasi pengambilan, dan aplikasi yang digunakan untuk penyuntingan. Informasi ini dapat digunakan untuk melacak apakah gambar telah diedit atau diubah dari kondisi aslinya (Riadi & Muthohirin, 2022). Metadata2Go adalah alat berbasis web yang dapat digunakan untuk membaca metadata secara menyeluruh tanpa perlu menginstal perangkat lunak tambahan. Dengan bantuan metadata, penyelidik dapat mengetahui apakah terdapat perbedaan antara waktu pengambilan gambar dengan waktu terakhir modifikasi, atau apakah file gambar pernah dibuka di aplikasi pengedit tertentu (*Metadata2Go*, 2025). Tools dapat diakses di website https://www.metadata2go.com.

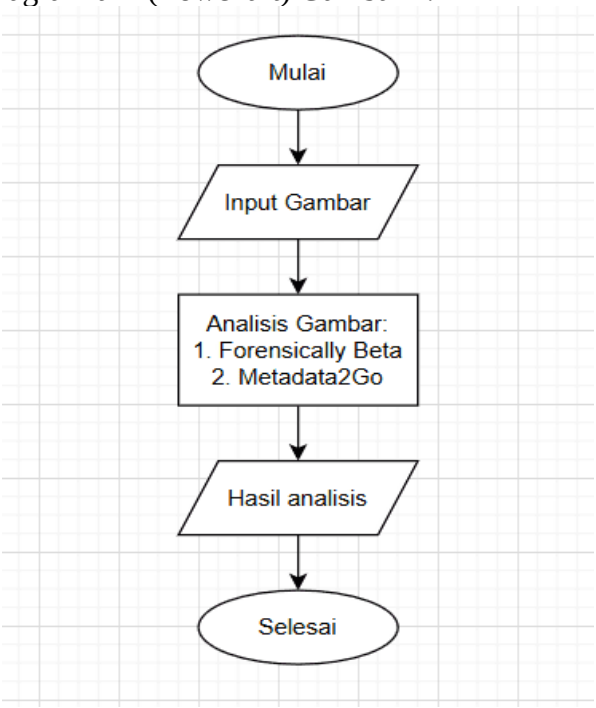
JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

**Metode Tambahan: *NIST* dan *SURF***

Selain ELA dan metadata, terdapat metode lain yang digunakan dalam forensik citra digital, seperti standar analisis dari NIST (*National Institute of Standards and Technology*). Metode ini menggabungkan penggunaan berbagai tools seperti *ExifTools* dan *VideoCleaner*, yang berfokus pada pemeriksaan metadata, hash, serta kejelasan visual citra sebagai bukti digital (Isnaini et al., 2020). Prosedur ini juga mendukung prinsip *repeatability* dan *verifiability*, dua komponen penting dalam akuntabilitas forensik digital. Selain itu, teknik deteksi menggunakan *Speeded-Up Robust Features* (SURF) telah diterapkan untuk membedakan antara citra asli dan hasil manipulasi, dengan mendeteksi ketidakhadiran *keypoints* pada objek hasil rekayasa yang secara alami seharusnya muncul di citra asli (Sulistyo et al., 2020). Pendekatan ini dinilai efektif karena memungkinkan pengujian citra secara spasial dan struktural, terutama dalam konteks identifikasi manipulasi berbasis copy-paste dan pemalsuan lokal.

## METODE PENELITIAN

Proses penelitian ini dilakukan secara bertahap dan sistematis untuk memastikan bahwa setiap gambar digital dianalisis dengan metode yang sesuai. Tahapan penelitian digambarkan dalam diagram alir (flowchart) Gambar 1.




**Gambar 1.** Tahapan Penelitian

Tahapan pada penelitian sebagaimana Gambar 1 dimulai dengan menentukan gambar-gambar digital yang akan dianalisis. Gambar dipilih berdasarkan dugaan adanya manipulasi atau ketidakwajaran isi visual, seperti ketidaksesuaian pencahayaan, bayangan yang tidak alami, atau objek yang tampak disalin dan ditempelkan. Input gambar dimasukkan ke dalam dua alat bantu digital, yaitu *Forensically Beta* dan *Metadata2Go*, sebagai input untuk dilakukan analisis lebih lanjut. Tahapan ini bertujuan untuk memastikan bahwa setiap gambar melalui proses verifikasi baik secara visual maupun teknis. Analisis gambar dilakukan pada tahap 1) *Forensically Beta* digunakan untuk menganalisis struktur visual gambar seperti tingkat error (*Error Level*

*Analysis/ELA*), pola duplikasi (*Clone Detection*), distribusi noise, serta pencahayaan dan orientasi objek. Hasil dari ELA dapat menunjukkan bagian gambar yang mengalami kompresi ulang atau penyisipan elemen asing; 2) *Metadata2Go* digunakan untuk mengekstraksi metadata tersembunyi dalam gambar, termasuk informasi waktu pengambilan, jenis perangkat, dan perangkat lunak pengeditan. Perubahan atau ketidaksesuaian pada metadata dapat menjadi indikasi bahwa file telah dimodifikasi. Hasil analisis dari kedua proses tersebut dibandingkan untuk mengidentifikasi tanda-tanda manipulasi. Indikator seperti noise tambahan, keselarasan pencahayaan, atau perbedaan *timestamp* dan *software editing history* menjadi bukti pendukung. Temuan ini lalu dikategorikan ke dalam kelompok: asli, dicurigai manipulasi ringan, dan manipulasi berat berdasarkan indikator teknis. Penelitian diakhiri setelah seluruh gambar dianalisis dan hasilnya dicatat serta disimpulkan dalam laporan. Data hasil analisis kemudian disusun dalam format tabel dan narasi untuk mendukung interpretasi, serta sebagai bahan evaluasi terhadap efektivitas alat yang digunakan.

## HASIL DAN PEMBAHASAN

Penelitian dilakukan dengan gambar digital yang dicurigai telah mengalami manipulasi visual. Gambar dianalisis menggunakan dua alat utama: Forensically Beta dan Metadata2Go. Analisis dilakukan secara visual dan teknis untuk mengungkap keaslian konten berdasarkan struktur gambar dan informasi metadata yang tertanam di dalamnya. Gambar 2 merupakan gambar digital yang dicurigai telah mengalami menipulasi.

**Gambar 2.** Gambar Digital

Gambar 2 menampilkan elemen visual yang tidak konsisten, seperti pencahayaan yang tidak wajar, kontur objek yang kabur, atau detail yang tampak tertempel. Selain itu, hasil ekstraksi metadata mengindikasikan adanya penggunaan perangkat lunak pengedit tertentu, perubahan waktu modifikasi, serta ketidaksesuaian data kamera, yang memperkuat dugaan bahwa gambar tersebut telah dimanipulasi.

### Hasil Analisis Forensically Beta

1. *Error Level Analysis (ELA)*
   Hasil analisis yang dilakukan pada fitur ELA: (a) Tingkat error tinggi pada bagian objek manusia menunjukkan perbedaan kompresi dibanding latar; (b)

JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

Umumnya, hal ini menandakan bahwa bagian tersebut telah dimodifikasi atau ditempel dalam gambar asli; (c) Latar belakang yang seragam menunjukkan kompresi konsisten, khas gambar asli. Hasil ELA menunjukkan indikasi manipulasi di area tubuh dan wajah subjek dapat dilihat pada Gambar 3.

**Gambar 3.** ELA

2. *Clone Detection*

Melalui *Clone Detection*, ditemukan adanya banyak blok persegi hitam tersebar secara tidak merata di area gambar. Hasil analisis (a) Blok-blok hitam menunjukkan area yang kemungkinan besar tidak memiliki pasangan atau tidak cocok secara struktur dengan bagian gambar lainnya; (b) Tidak ditemukan pola pengulangan atau garis penghubung antar area (yang biasanya menunjukkan *copy-move forgery*). Hasil ini bisa berarti gambar tidak mengalami manipulasi berbasis kloning, atau parameter deteksi terlalu ketat, sehingga sistem gagal mendeteksi kemiripan lemah.

**Gambar 4.** *Clone Detection*

*Clone Detection* tidak menunjukkan indikasi kloning secara langsung, tetapi hasil tidak dapat menjadi acuan tunggal tanpa dikombinasikan dengan fitur lain. hasil gambar dapat dilihat pada Gambar 4.

JUPITER
Teknologi Informatika & Komputer
Vol. 6 No. 2 Agustus 2025
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

3. *Noise Analysis*
   Area objek (khususnya pakaian dan tangan) memiliki noise yang jauh lebih tinggi daripada latar belakang. Hasil analisis (a) Noise yang tidak merata adalah ciri umum gambar yang telah dimodifikasi; (b) Latar belakang menunjukkan noise rendah dan konsisten menguatkan bahwa area tersebut asli; (c) Area dengan noise tinggi kemungkinan besar mengalami penyesuaian lokal atau penggabungan dari sumber lain. Distribusi noise tidak merata menunjukkan manipulasi visual pada bagian tertentu dapat dilihat pada Gambar 5.

**Gambar 5.** *Noise Analysis*

4. *Luminance Gradient*
   Garis-garis kontur dan transisi cahaya tampak sangat tajam pada bagian wajah, tangan, dan pakaian. Hasil analisis (a) Luminansi tidak konsisten antara objek (subjek manusia) dan latar; (b) Ketidakwajaran pencahayaan ini bisa berarti perbedaan sumber cahaya yang tidak alami; (c) Kontur terang di wajah dan tubuh terlalu menonjol, menandakan bahwa objek tersebut kemungkinan ditambahkan atau dimanipulasi secara terpisah dari latar. *Luminance Gradient* memperkuat dugaan bahwa objek manusia dalam gambar adalah hasil manipulasi digital pada Gambar 6.

**Gambar 6.** *Luminance Gradient*

**Hasil Analisis Metadata2Go**

Berdasarkan metadata yang berhasil diekstraksi, diketahui bahwa gambar digital tidak dibuat menggunakan kamera digital secara langsung, melainkan melalui aplikasi desain grafis Canva. Informasi ini memperkuat dugaan bahwa gambar tersebut telah dimodifikasi atau disusun ulang, dan bukan merupakan hasil foto otentik. Tidak ditemukannya informasi kamera atau lokasi juga menunjukkan bahwa metadata asli dari gambar kemungkinan telah dihapus atau tidak pernah ada. Berikut adalah hasil yang didapat dari Metadata2Go.

1. Informasi teknis file
   Nama file: Edit.png
   Tipe file: *PNG (Portable Network Graphics)*
   Ukuran: 4.1 MB
   Resolusi gambar: 1536 x 2048 piksel
   Kedalaman warna: 8-*bit*
   Tipe warna: RGB dengan alpha (transparansi)
   Megapiksel: 3.1 MP
   Tanggal dibuat: 20 April 2025
2. Alat dan aplikasi yang digunakan
   Pembuat gambar: *Canva*
   Creator Tool: Canva (Renderer)
   User ID & Template: Terdeteksi adanya ID pengguna dan template dari Canva, meskipun kosong pada bagian template.
3. Identitas *file*
   Judul file: *Desain tanpa judul - 1*
   Author: Maria Chatrin Bunaen
   Ads ID dan FB ID: Terdeteksi ada data dari sistem iklan digital (kemungkinan dari ekspor berbasis platform yang terhubung dengan sosial media).

Temuan metadata ini tidak hanya menunjukkan bahwa gambar telah disusun melalui aplikasi grafis, tetapi juga membuka kemungkinan bahwa gambar tersebut pernah digunakan atau disiapkan untuk distribusi digital melalui kanal sosial media atau iklan. Hal ini mengindikasikan pentingnya metadata dalam menelusuri asal-usul gambar, konteks penggunaannya, serta potensi manipulasi yang tidak terdeteksi secara visual.

**Pembahasan**

Temuan dalam penelitian ini menunjukkan bahwa analisis visual dan metadata saling melengkapi dalam mengungkap indikasi manipulasi gambar digital. Fitur seperti Error Level Analysis (ELA), Noise Analysis, dan Luminance Gradient menunjukkan anomali visual yang tidak konsisten dengan pola pencahayaan alami gambar yang otentik. Meskipun fitur Clone Detection tidak secara eksplisit mendeteksi duplikasi area dalam gambar, hasil dari fitur-fitur lainnya tetap menunjukkan adanya ketidakwajaran yang signifikan. Ketidaksesuaian metadata seperti hilangnya informasi perangkat kamera, serta munculnya jejak perangkat lunak pengedit seperti *Canva* memperkuat dugaan bahwa gambar telah melalui proses modifikasi digital. Jika dibandingkan dengan penelitian (Harahap, 2021), yang lebih berfokus pada deteksi visual semata melalui ELA dan analisis noise, penelitian ini menawarkan pendekatan yang lebih menyeluruh dengan menggabungkan bukti visual dan metadata sebagai dua lapisan validasi. Sementara itu, studi (Sulistyo et al., 2018) menekankan peran *Forensically Beta* dalam mengungkap

artefak manipulasi visual, namun belum memadukannya dengan analisis metadata secara langsung. Penelitian ini memperkuat dan memperluas temuan tersebut dengan membuktikan bahwa integrasi antara visual forensik dan metadata mampu meningkatkan keandalan dalam mendeteksi manipulasi secara halus dan tersembunyi.

Validasi silang antara fitur visual dan metadata dalam penelitian ini menunjukkan konsistensi hasil: area yang dicurigai mengalami gangguan visual (ELA dan noise tinggi) umumnya berlokasi pada bagian gambar yang tidak memiliki keterkaitan logis dalam pencahayaan atau tekstur, dan ketidaksesuaian tersebut diperkuat oleh metadata yang mengindikasikan penggunaan software desain. Korelasi ini menambah keyakinan bahwa gambar telah direkayasa secara digital. Lebih jauh, hasil penelitian mencerminkan realitas baru di era digital, di mana pemalsuan gambar tidak selalu dilakukan dengan teknik kasar yang mudah dikenali. Manipulasi kini lebih banyak dilakukan secara halus melalui aplikasi desain populer yang secara otomatis membersihkan metadata asli dan menyamarkan jejak teknis. Oleh karena itu, penting bagi analisis forensik digital untuk terus mengadaptasi metode dan memperkaya parameter deteksi. Pendekatan multi-fitur seperti yang digunakan dalam penelitian ini terbukti lebih efektif dalam meningkatkan akurasi deteksi dan memperkuat kredibilitas hasil investigasi, terutama dalam konteks penegakan hukum digital dan verifikasi informasi publik.

## PENUTUP

### Simpulan

Penelitian ini menunjukkan bahwa penggunaan Forensically Beta dan Metadata2Go merupakan pendekatan yang efektif dalam menganalisis keaslian foto digital. Melalui fitur-fitur seperti *Error Level Analysis*, *Clone Detection*, *Noise Analysis*, dan *Luminance Gradient*, Forensically Beta mampu mendeteksi indikasi manipulasi visual pada area tertentu dalam gambar. Di sisi lain, Metadata2Go mengungkap informasi tersembunyi terkait waktu pembuatan file, perangkat yang digunakan, serta aplikasi pengedit gambar. Hasil analisis menunjukkan bahwa gambar yang diteliti telah mengalami proses pengeditan dan tidak berasal dari kamera digital secara langsung, melainkan dibuat menggunakan aplikasi desain grafis. Kombinasi antara analisis visual dan metadata terbukti menjadi metode yang saling melengkapi dalam membuktikan keaslian gambar digital. Temuan ini menegaskan pentingnya penerapan metode forensik digital sebagai langkah awal yang efektif dalam proses investigasi keaslian gambar, khususnya dalam ranah hukum, jurnalistik, serta edukasi publik. Dengan pendekatan yang tepat, analisis forensik gambar dapat memberikan kontribusi nyata dalam memerangi penyebaran informasi palsu dan meningkatkan kepercayaan terhadap bukti digital.

### Saran

Penelitian selanjutnya disarankan untuk memperluas objek studi dengan menggunakan lebih banyak sampel gambar dari berbagai sumber, termasuk hasil tangkapan layar, gambar beresolusi rendah, dan konten dari platform media sosial. Selain itu, integrasi perangkat lunak forensik tambahan seperti JPEGsnoop, FotoForensics, atau ExifTool diharapkan dapat memperkaya hasil analisis dan meningkatkan akurasi deteksi manipulasi. Peningkatan literasi digital juga menjadi hal yang penting untuk diperhatikan. Masyarakat perlu dibekali kemampuan dasar dalam mengenali ciri-ciri gambar palsu agar tidak mudah terpengaruh oleh konten visual yang menyesatkan. Untuk itu, perlu adanya

kerja sama lintas sektor dalam menyediakan pelatihan, modul edukatif, serta kampanye kesadaran publik yang berkelanjutan.

Pengembangan sistem deteksi otomatis berbasis kecerdasan buatan (*Artificial Intelligence*) juga direkomendasikan guna meningkatkan efisiensi dan akurasi dalam memverifikasi keaslian gambar digital secara masif dan berkelanjutan. Di samping itu, kolaborasi antara akademisi, pengembang perangkat lunak, dan penegak hukum sangat diperlukan untuk menciptakan ekosistem verifikasi digital yang komprehensif, terintegrasi, dan mudah diakses oleh publik. Dukungan regulasi dan kebijakan yang jelas dari pemerintah terkait pemalsuan konten digital juga menjadi aspek krusial yang perlu diperjuangkan untuk menanggulangi penyebaran disinformasi secara sistemik.

## REFERENSI

Bisri, H., & Marzuki, M. I. (2023). Forensik Citra Digital Menggunakan Metode Error Level Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar. *G-Tech: Jurnal Teknologi Terapan*, *7*(2), 586–595. https://doi.org/10.33379/gtech.v7i2.2363

*Forensically Beta*. (2025). Retrieved May 9, 2025, from https://29a.ch/photo-forensics/#forensic-magnifier

Harahap, F. (2021). *Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic.org Dengan Metode Error Level Analysis (ELA)* (Vol. 2, Issue 3).

Hartawan, M. S., Suhardjono, Ridwansyah, Riyanto, V., & Putra, A. S. (2022). *Digital Forensik (Informasi dan Kasus)*. https://repository.bsi.ac.id/repo/files/394717/download/NASKAH-DIGITAL-FORENSIK-SIAP-CETAK.pdf

Iman, N., Susanto, A., & Inggi, R. (2020). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi Dan Komputer*, *9*(3), 186. https://doi.org/10.22441/incomtech.v9i3.7210

Isnaini, K. N., Ashari, H., & Kuncoro, A. P. (2020). *Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST*. https://s.id/jurnalresistor

*Metadata2Go*. (2025). Retrieved May 9, 2025, from https://www.metadata2go.com/

Riadi, I., & Muthohirin, B. F. (2022). Forensi Digital [*Forensik Email*]. Yogyakarta: Diandra Kreatif. https://eprints.uad.ac.id/59619/1/Cetakan-ke-3-Buku-Forensik-Email.pdf

Sulistyo, W. Y., Pratiwi, S. A., Haedar, M., & Hidayatullah, Z. (2025). Analisis Forensik Citra di Platform X Menggunakan Metode Digital Forensic Research Workshop (DFRWS). *Idealis: Indonesia Journal Information System*, 8(1), 10-20. https://doi.org/10.36080/idealis.v8i1.3293.https://jom.fti.budiluhur.ac.id/IDEALIS/article/view/3293

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2020). Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital *(Application of SURF Technique in Image Forensic for Digital Photo Engineering Analysis) Idealis: Indonesia Journal Information System*, 8(2). https://doi.org/10.30595/juita.v8i2.6602. https://jurnalnasional.ump.ac.id/index.php/JUITA/article/view/6602

Wibowo, A. (2023). *Digital Forensik* (oseph Teguh Santoso). Yayasan Prima Agus Teknik Bekerja sama dengan Universitas Sains & Teknologi Komputer.

Wicaksono, A., Mardiyantoro, N., & Sibyan, H. (2022). *Penerapan Metode Error Level Analysis Untuk Mendeteksi Modifikasi Citra Digital*. *1*(1). https://ojs.unsiq.ac.id/index.php/biner