

## **ANALISIS DIGITAL FORENSIK METADATA PADA REKAYASA DIGITAL IMAGE SEBAGAI BARANG BUKTI DIGITAL**

**Mansuestus Fransiskus<sup>1</sup>, Noviyanti. P<sup>2</sup>**

<sup>1,2</sup>Teknologi Informasi, Institut Shanti Bhuna Bengkayang

**E-mail: zfrantpts@gmail.com<sup>1</sup>, noviyanti@shantibhuana.ac.id<sup>2</sup>**

### **Abstrak**

Perkembangan zaman digital telah mengubah segala hal, termasuk dalam hal fotografi. Foto digital memiliki keunggulan dan kekurangan, termasuk kemampuan untuk dimanipulasi dengan *software* editing sehingga sulit membedakan antara foto asli dan hasil manipulasi. Foto rekayasa tersebut dapat dengan mudah menyebar melalui media sosial dan menimbulkan kecemasan serta keraguan terhadap kebenaran berita. Motif-motif seperti politik, agama, dan motif pribadi dapat menjadi alasan seseorang melakukan rekayasa foto. Keberadaan berbagai *software* editing yang mudah digunakan memudahkan proses rekayasa foto. Dalam bidang penelitian, forensik citra digital digunakan sebagai metode ilmiah untuk memperoleh bukti-bukti yang dapat digunakan dalam menentukan keaslian sebuah gambar. Penelitian ini bertujuan untuk mendeteksi adanya pemalsuan pada foto digital dengan menggunakan pendekatan tersebut. Penelitian ini menggunakan analisa dengan sebuah *Tools Offline* yaitu Metadata++. Hasil yang di dapat dari penelitian ini yaitu perbedaan Metadata antara foto asli dan foto manipulasi yang menunjukkan adanya perubahan dari kedua foto tersebut.

### **Abstract**

The development of the digital age has changed everything, including photography. Digital photos have advantages and disadvantages, including the ability to be manipulated with editing software, making it difficult to distinguish between the original and the manipulated photos. The engineered photo can easily spread through social media and cause anxiety and doubt about the veracity of the news. Motives such as politics, religion, and personal motives can be reasons for someone to do photo engineering. The existence of various easy-to-use editing software facilitates the photo engineering process. In the field of research, digital image forensics is used as a scientific method to obtain evidence that can be used to determine the authenticity of an image. This study aims to detect forgery in digital photos using this approach. This study uses offline analysis with an Offline Tool, namely Metadata++. The results obtained from this study are the difference in metadata between the original photo and the manipulated photo, which indicates a change in the two photos.

### **Info Naskah:**

Naskah masuk: 16 Juli 2023

Direvisi: 27 Juli 2023

Diterima: 13 Desember 2023

### **Keywords:**

Digital Photos;  
Digital image forensics;  
Editing software;  
Metadata;  
Software;  
Tools Offline;

**\*Penulis korespondensi:**

**Nama Penulis**

zfrantpts@gmail.com

## 1. Pendahuluan

Perkembangan zaman yang semakin maju mengubah segalanya menjadi digital, termasuk urusan foto. Foto digital memiliki banyak keunggulan dan juga kekurangan, seperti kemampuannya untuk dimanipulasi dengan *software* editing sehingga foto hasil editan dapat terlihat asli seperti nyata. Bentuk editan dapat bervariasi, mulai dari melakukan *cropping*, meningkatkan kecerahan, memasang *background*, hingga memanipulasi bagian-bagian tertentu. Teknik manipulasi foto yang semakin canggih kadang-kadang sangat sulit untuk membedakan antara foto asli dan foto hasil manipulasi [1].

Foto yang sudah direkayasa dapat dengan mudah tersebar di berbagai *platform* media sosial. Penyebaran foto rekayasa ini dapat menyebabkan kecemasan di kalangan masyarakat dan membuat mereka meragukan kebenaran berita tersebut. Hal ini disebabkan karena gambar dan video dapat dengan mudah direkayasa. Motif-motif yang beragam dapat menjadi alasan seseorang melakukan rekayasa foto, seperti motif politik, agama, dan motif pribadi untuk memfitnah seseorang. Sebagai contoh, dalam kasus pornografi, gambar atau video dapat direkayasa dan dimanipulasi sehingga menyerupai seseorang, yang pada akhirnya dapat merusak nama dan reputasi orang tersebut. Adanya berbagai *software* editing yang tersedia, seperti *Photoshop*, *Corel Draw*, dan bahkan *Paint*, memungkinkan untuk melakukan rekayasa foto dengan mudah [2].

Forensik digital merupakan kegiatan investigasi yang dilakukan dalam penanganan kasus kejahatan dunia maya. Menurut [3], Digital Forensik merupakan suatu proses ilmiah atau usaha ilmiah yang menggunakan prinsip-prinsip ilmu untuk mengumpulkan, menganalisis, dan menyajikan bukti dalam konteks proses pengadilan guna mendukung pengungkapan kejahatan. Hal ini dilakukan dengan memastikan bahwa bukti yang diungkapkan telah disahkan oleh hukum dan peraturan yang berlaku.

Penggunaan Digital forensik sangat luas dan dapat diterapkan dalam berbagai keperluan, tidak hanya untuk menangani kasus kriminal yang melibatkan hukum. Misalnya, digunakan untuk melakukan rekonstruksi insiden keamanan komputer, memecahkan masalah terkait perangkat keras dan perangkat lunak, serta melakukan upaya pemulihan kerusakan sistem. Melalui digital forensik, seseorang dapat memiliki keahlian teknis dalam mengumpulkan bukti secara digital yang dapat disajikan dalam persidangan sesuai dengan hukum yang berlaku. Digital forensik dapat dibagi menjadi beberapa bagian, seperti *Disk Forensics*, *Network Forensics*, *Mobile Forensics*, *Image Forensics*, dan *System Forensics* [1].

Pada pertengahan 1980-an, bidang forensik digital mulai berkembang seiring dengan pemahaman dari beberapa lembaga penegak hukum bahwa peran komputer akan menjadi penting dalam penyelidikan kejahatan masa depan [4].

Penelitian sebelumnya yang menjadi acuan penelitian ini dilakukan, terdapat beberapa penelitian yang telah dilakukan sebelumnya, penelitian yang dilakukan oleh [5], dalam penelitian ini, digunakan metode *Latent Semantic Analysis* untuk mengekstraksi kata-kata dari metadata file. Kemudian, kata-kata tersebut direpresentasikan dalam bentuk vektor

dan matriks agar dapat digunakan dalam deteksi duplikasi file dan analisis metadata dari berbagai jenis file dalam media penyimpanan. Hasil penelitian menunjukkan bahwa metode *Latent Semantic Analysis* efektif dalam mendeteksi metadata file yang duplikasi pada berbagai jenis media penyimpanan, sehingga meningkatkan kegunaan dan aksesibilitas media penyimpanan tersebut secara signifikan.

Pada penelitian [6], Penelitian ini mengevaluasi sejauh mana metadata dapat efektif dan dapat diandalkan dalam mendeteksi rekayasa digital pada gambar. Selain itu, penelitian ini akan mengidentifikasi pola dan karakteristik khusus dalam metadata yang dapat digunakan sebagai tanda atau indikator rekayasa digital pada gambar, dengan tujuan mengembangkan metode atau alat otomatis untuk mengenali rekayasa digital berdasarkan analisis metadata.

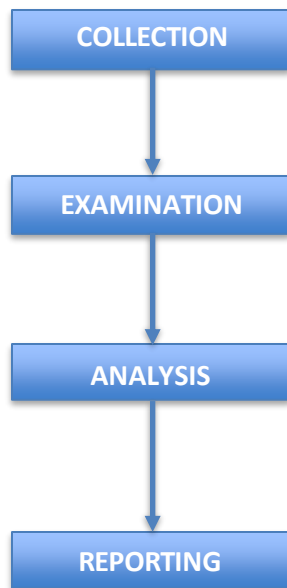
Penelitian [7] menjelaskan hasil analisis video rekaman kamera CCTV mengungkapkan karakteristik bukti digital dan informasi metadata yang digunakan untuk memberikan penjelasan terstruktur dan komprehensif. Selain itu, hasil investigasi digital forensik juga memberikan acuan yang dapat dipertanggungjawabkan dalam pengelolaan informasi data yang diperoleh, sehingga dapat digunakan sebagai bukti yang sah dalam persidangan.

Perbedaan penelitian ini dengan penelitian yang sebelumnya yaitu penelitian yang menganalisis Metadata dua gambar serupa yang akan digunakan sebagai barang bukti di persidangan. Proses analisis ini menggunakan Metode NIST dan untuk Analisis nya, peneliti menggunakan *Tools* offline yaitu Metadata++ sebagai *Tools* untuk mengecek Metadata pada sebuah foto/gambar.

Tujuan penelitian ini adalah menganalisis metadata dari file gambar digital yang telah mengalami rekayasa atau manipulasi. Penelitian ini bertujuan untuk mengidentifikasi dan memahami perubahan yang terjadi pada metadata setelah terjadinya rekayasa digital pada gambar. Mengevaluasi efektivitas dan keandalan metadata dalam mendeteksi rekayasa digital pada gambar. Penelitian ini akan memeriksa apakah metadata dapat memberikan petunjuk yang jelas dan konsisten mengenai rekayasa digital yang terjadi pada gambar. Mengidentifikasi pola dan karakteristik metadata yang dapat digunakan sebagai tanda atau indikator rekayasa digital pada gambar. Meningkatkan keandalan dan kegunaan barang bukti digital dalam proses hukum. Dengan mengkaji metadata pada rekayasa digital *image*, penelitian ini dapat memberikan sumbangan penting dalam bidang forensik digital untuk meningkatkan integritas dan validitas barang bukti digital yang digunakan dalam persidangan.

## 2. Metode Penelitian

Dalam penelitian ini, metode penelitian akan mengikuti pedoman dan persyaratan yang tercantum dalam Standar Nasional Indonesia (SNI) 27037:2014. Beberapa penelitian sebelumnya telah menggunakan prosedur akuisisi sesuai dengan SNI 27037:2014, dengan menerapkan metode investigasi NIST (*National Institute of Standards Technology*) untuk menganalisis metadata rekaman kamera CCTV sebagai bukti digital [8]. Berikut merupakan tahapan analisis Metode NIST :



Gambar 1. Diagram Alir Analisis Forensik Digital

Gambar 1 merupakan diagram alir analisis forensik digital yang terdiri dari 4 tahapan berikut:

**Collection** (pengumpulan) Merupakan tahap pengumpulan data melibatkan serangkaian kegiatan yang bertujuan untuk mengumpulkan data yang mendukung proses penyidikan dalam mencari barang bukti kejahatan digital. Pada tahap ini, dilakukan pengambilan data dari sumber data yang relevan dan menjaga integritas barang bukti agar tidak mengalami perubahan.

**Examination** (Pemeriksaan) Pada tahap ini, bukti digital yang telah dikumpulkan akan diperiksa secara rinci. Ini melibatkan analisis metadata, struktur file, dan komponen penting lainnya. Tujuannya adalah untuk memahami konten dan karakteristik bukti digital serta mengidentifikasi bukti potensial yang relevan dengan kasus yang sedang diselidiki.

**Analysis** (Analisis) Tahap analisis melibatkan pengolahan dan penafsiran data yang telah dikumpulkan. Ahli forensik digital menggunakan teknik dan alat analisis yang sesuai untuk menggali informasi yang tersembunyi atau terhapus, mengidentifikasi pola, dan menghubungkan bukti digital dengan kejadian yang terjadi. Analisis ini membantu dalam membangun rangkaian kejadian dan mendukung pembuatan kesimpulan yang valid.

**Reporting** (Pelaporan) Tahap pelaporan melibatkan penyusunan laporan yang jelas dan terperinci tentang temuan forensik digital. Laporan ini berisi informasi tentang metodologi yang digunakan, hasil analisis, temuan utama, dan kesimpulan yang dapat digunakan sebagai bukti dalam proses hukum. Laporan ini juga harus memenuhi standar forensik digital dan dapat dipahami oleh pihak non-teknis.

### 3. Hasil dan Pembahasan

#### 3.1 Collection

Di tahap yang pertama ini dilakukan pengumpulan data yang merupakan barang bukti yang akan diidentifikasi. Barang bukti yang dimaksud berupa gambar/foto digital asli dan

yang sudah di manipulasi. Berikut Merupakan Gambar yang akan dianalisis Metadata nya.



Gambar a : Foto asli.




Gambar b : Foto hasil editing

Gambar a merupakan gambar asli yang akan dianalisis Metadata nya untuk membuktikan keaslian gambar tersebut, sedangkan gambar b merupakan gambar yang sudah di manipulasi dan akan di analisis metadatanya untuk membuktikan apakah gambar tersebut merupakan gambar manipulasi yang sudah diedit menggunakan *Software Editing*.


#### 3.2 Examination

Di tahap yang kedua ini akan dilakukan pemeriksaan pada kedua gambar tersebut dengan memeriksa Metadata dari kedua foto yang akan menjadi barang bukti. Pemeriksaan ini akan dibantu oleh *Tools Metadata++* yang merupakan *tools offline* dapat digunakan untuk mengecek Metadata dari sebuah gambar digital. Dari pemeriksaan Metadata yang dilakukan akan diketahui asal dari gambar tersebut. Berikut merupakan *screenshot* gambar dari *Tools Metadata++*.



Field	Value	Status
Artist	013b	✓
Copyright	8298	✓
Make	010f	✓ Canon
Model	0110	✓ Canon EOS 1300D
ModifyDate	0132	✓ 2021:12:24 21:43:46
Orientation	0112	✓ Horizontal (normal)
ResolutionUnit	0128	inches
XResolution	011a	✓ 72
YCbCrPositioning	0213	✓ Co-sited
YResolution	011b	✓ 72

Gambar 2 : Metadata foto.gambar asli



Field	Value	Status
Make	010f	✓ Canon
Model	0110	✓ Canon EOS 1300D
ModifyDate	0132	✓ 2023:04:25 11:36:53
Orientation	0112	✓ Horizontal (normal)
ResolutionUnit	0128	inches
Software	0131	✓ Adobe Photoshop CS4 Windows
XResolution	011a	✓ 72
YCbCrPositioning	0213	✓ Co-sited
YResolution	011b	✓ 72

Gambar 3 : Metadata foto/gambar hasil *Editing*.

Gambar 2 merupakan Metadata dari foto/gambar asli dan gambar 3 merupakan Metadata gambar palsu hasil *editing*. Metadata yang digunakan ini adalah *Image File Directory Main Image* Pada kedua gambar akan digunakan sebagai barang bukti yang telah di cek Metadata nya menggunakan *Tools Metadata++*.

### 3.3 Analysis

Pada tahap ini akan melihat perbandingan dari kedua foto yang telah di di cek Metadata nya dengan sebuah *Tools Offline* yaitu *Metadata++*, berikut ini merupakan tabel analisis kedua foto tersebut.



Tabel 1. Analisis Metadata Gambar a dan Gambar b

Metadata	Gambar 1	Gambar 2
Make	Canon	Canon
Model	Canon EOS 13000	Canon EOS 13000
ModifyDate	2021:12:24	2023:04:25
Orientation	Horizontal(normal )	Horizontal(normal )
ResolutionUnit	inches	inches
Software	-	Adobe Photoshop Windows

### 3.4 Reporting

Setelah dilakukan tahapan *analysis* dari kedua foto yang digunakan kita dapat mengetahui cara membandingkan ke dua foto tersebut. Dan berikut ini merupakan hasil *report* dari simulasi yang dilakukan dengan menggunakan kedua *tools* yaitu *Metadata++* ditampilkan dalam bentuk tabel sebagai berikut :

Tabel 2. Laporan Hasil Analisis Metada Gambar a dan Gambar b

	Barang Bukti	Metadata	Status
Gambar a		1. Canon EOS 13000 2. 2021:12:24	Asli
Gambar b		1. Adobe Photoshop Windows 2. 2023:04:25	Terbukti Hasil Editing

Dari hasil *report* simulasi kita dapat mengetahui perbedaan antara foto asli dan foto palsu dengan melihat metadata. Pada foto asli metadata foto tersebut diambil dari kamera Canon EOS 1300D dan pada foto palsu merupakan hasil rekayasa dari *photoshop*. Dan terdapat juga perbedaan data *ModifyDate* pada kedua foto tersebut, dimana pada foto asli Data *ModifyDate*-nya adalah 2021:12:24 yang artinya foto tersebut di ambil pada tanggal 24 Desember 2021. Sedangkan pada foto hasil *editing* memiliki data *ModifyDate* yang berbeda yaitu 2023:04:25 yang artinya bahwa foto tersebut dimanipulasi.

### 4. Kesimpulan

Kedua foto tersebut telah di-*scan* menggunakan sebuah *Tools Offline* yaitu *Metadata++* yang menghasilkan metadata dari kedua foto tersebut, dimana pada foto yang pertama belum mengalami perubahan data seperti data *ModifyDate*-nya masih belum berubah dan tidak ada *software* yang menunjukkan bahwa foto tersebut telah di manipulasi. Sedangkan pada foto kedua telah mengalami perubahan pada Metadata dimana foto tersebut telah di-*edit* menggunakan *Software Adobe Photoshop* dan data *ModifyDate* juga sudah berubah. Dalam analisis bukti, terungkap bahwa dari dua foto yang digunakan sebagai barang bukti, ternyata salah satunya telah mengalami rekayasa. Bahan foto yang di gunakan masih menggunakan foto asli dan foto manipulasi hasil *editing* dari foto asli, bukan menggunakan foto yang telah beredar di media sosial dan internet.

Untuk penelitian selanjutnya, disarankan untuk menggunakan foto-foto yang tersebar luas di media sosial dan internet sebagai sampel, sehingga hanya dengan menggunakan satu foto, dapat dilakukan deteksi kepalsuan secara efektif. Diharapkan dengan pendekatan ini, dapat dikembangkan alat dan teknik baru yang berbeda guna mencari perbandingan dari berbagai alat forensik gambar yang tersedia, dengan tujuan menemukan solusi terbaik dalam mendeteksi manipulasi foto.

### Daftar Pustaka

- [1] I. Riadi, A. Yudhana, and W. Y. Sulistyo, "Analisis Image Forensics Untuk Mendeteksi Pemalsuan Foto Digital," *Mob. Forensics*, vol. 1, no. 1,

p. 13, 2019, doi: 10.12928/mf.v1i1.703.

[2] M. R. Al-Fajri, C. M. Kom, 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, doi: 10.32528/justindo.v6i2.5120.

[3] M. F. Abdillah, "ANALISIS PERBANDINGAN DATA RECOVERY MENGGUNAKAN TOOLS FORENSIK BERBASIS OPEN SOURCE PADA LINUX," 2022.

[4] M. Unik and V. G. Larenda, "Analisis Investigasi Android Forensik Short Message Service (SMS) Pada Smartphone," *JOISIE (Journal Inf. Syst. Informatics Eng.)*, vol. 3, no. 1, p. 10, 2019, doi:10.35145/joisie.v3i1.414.

[5] E. Erlin, B. H. Fikri, S. Susanti, and T. A. Fitri, "Deteksi Duplikasi Metadata File pada Media

Penyimpanan menggunakan Metode Latent Semantic Analysis," *INOVTEK Polbeng - Seri Inform.*, vol. 5, no. 1, p. 119, 2020, doi: 10.35314/isi.v5i1.1375.

[6] A. R. Kelrey *et al.*, "Source Image," vol. 9, no. 3, pp. 1873–1883, 2022.

[7] D. Mualfah and R. A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 257–267, 2020, doi: 10.31849/digitalzone.v11i2.5174.

[8] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.