

## ANALISIS FORENSIC CITRA DIGITAL MENGGUNAKAN TEKNIK *ERROR LEVEL ANALYSIS* DAN METADATA BERDASARKAN METODE NIST

Karolina Eka Purnama, Chaerur Rozikin, Azhari Ali Ridha

Program Studi Informatika S1, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang

Jl. HS. Ronggo Waluyo, Telukjambe Timur, Karawang, Indonesia

1910631170197@student.unsika.ac.id

### ABSTRAK

Saat ini, terjadi peningkatan yang signifikan dalam perubahan citra yang berasal dari citra asli yang mudah dimanipulasi. Situasi ini dimanfaatkan oleh pihak yang tidak bertanggung jawab. Kemudahan dalam memanipulasi, mengubah, atau menghapus informasi asli dari citra digital menimbulkan keraguan terhadap keaslian dan integritas citra yang digunakan. Tujuan dari penelitian ini adalah membuktikan keaslian bukti digital melalui analisis menggunakan Digital Forensik berdasarkan alur metode NIST. Alur penelitian mencakup pemahaman latar belakang masalah, pengumpulan data, identifikasi, penerapan metode NIST, dan pelaporan hasil. Objek penelitian ini adalah foto yang dimasukkan dalam bukti digital yang diambil atau dipotret menggunakan kamera *Canon EOS 700D*, penelitian ini menggunakan *tools forensically beta* dan *jpegsnoop* untuk mengidentifikasi metadata dan analisis tingkat kesalahan. Hasil metadata foto manipulasi terdiri dari *Luminance* (ID Tujuan 0) dan *Chrominance* (ID Tujuan 1) dalam tabel 8x8 dengan angka 8-bit. Nilai tinggi pada tabel menunjukkan pembagian kasar dan penurunan kualitas, menunjukkan *assessment class 3*, dimana foto teridentifikasi telah dilakukan pengeditan menggunakan *software editing Photoshop*. Hasil *error level analysis* menunjukkan foto manipulasi terlihat lebih gelap, objek yang sudah dimanipulasi lebih menonjol, dan hasil tekstur menggunakan *histogram equalization* terlihat kacau.

**Kata kunci:** Foto, Error Level Analysis, Metadata, NIST

### 1. PENDAHULUAN

Dengan kemajuan teknologi di zaman sekarang membuat dunia digital berkembang dengan cepat khususnya di era digital. Pemanfaatan teknologi saat ini membantu memudahkan pekerjaan manusia. Kemajuan teknologi telah memudahkan kita untuk memahami data dalam bentuk informasi atau gambar. Ada banyak aplikasi yang memungkinkan pengolahan gambar menjadi lebih mudah [1]. Peningkatan teknologi citra digital yang semakin maju memudahkan untuk mengubah atau menyesuaikan foto sehingga manipulasi gambar semakin sering terjadi. Semakin sulit bagi masyarakat untuk membedakan antara foto asli dan hasil manipulasi karena teknik manipulasi gambar terus berkembang [2].

Pengumpulan, analisis, dan pelaporan data digital merupakan inti dari forensik digital. Ada banyak kegunaan untuk investigasi forensik digital. Investigasi ilmiah kejahatan atau deteksi umum kejahatan keduanya disebut sebagai bidang ilmu forensik atau forensik. Munculnya forensik berasal dari timbulnya perilaku kriminal, ilegal dan tidak pantas. Dalam konteks forensik digital, di Indonesia sendiri sudah banyak kasus yang ditangani dengan menggunakan forensik digital. Misalnya, kasus korupsi dengan melakukan investigasi terhadap media komunikasi yang digunakan dalam melakukan transaksi, kasus peretasan sistem informasi, kasus pemalsuan citra digital dan masih banyak kasus lainnya [3]. Dengan cara pandang yang salah, sikap terhadap teknologi akan mengubah perilaku manusia.

Khususnya di beberapa negara berkembang, sejauh mana teknologi dapat mendorong perilaku kejahatan meningkat seiring dengan perkembangannya [4].

Salah satu kejahatan dunia maya berupa penipuan online yaitu kasus *forensic image* dimana berupa pemalsuan citra, dimana citra digital yang telah dimanipulasi mudah terjadi di ruang lingkup kejahatan sosial [5]. Citra asli modifikasi sulit ditentukan keasliannya, sehingga sulit untuk mengidentifikasi pemalsuan citra dalam penyebaran digital. Terdapat berbagai tujuan untuk manipulasi citra digital, mulai dari tujuan kesenangan, pemasaran, hingga kejahatan yang dapat memperdayai penyelidik. Contoh kasus pemalsuan citra digital adalah penyebaran foto yang melibatkan pejabat, artis, publik figur ataupun masyarakat biasa dengan konten sensitif yang dapat menimbulkan kehebohan di masyarakat [6].

Penelitian ini bertujuan untuk mengkaji citra digital yang telah dimanipulasi atau direkayasa selama proses pengambilan gambar menggunakan perangkat lunak atau program digital. Beberapa perangkat lunak atau alat yang dapat digunakan untuk menganalisis keaslian citra digital adalah *fotoforensic*, *forensically beta*, dan *jpegsnoop* [7].

Forensik IT mengkaji metode ilmiah untuk mencari bukti digital. TI Forensik bertujuan untuk mengumpulkan bukti yang dapat diandalkan dari media digital yang dapat digunakan di pengadilan [8]. Analisis forensik digital memiliki ruang lingkup yang sangat luas, sehingga dapat dikategorikan berdasarkan sifat fisik dan logisnya. Forensik seluler, forensik audio, forensik video, forensik gambar, dan forensik

dunia maya semuanya termasuk dalam ruang lingkup forensik komputer. Penelitian ini akan berkonsentrasi pada forensik citra, khususnya forensik file citra digital sebagai bentuk bukti digital, sehingga penelitian ini berjudul “Analisis Forensik Citra Digital Menggunakan *Error Level Analysis* dan Metadata Berdasarkan Metode NIST”.

## 2. TINJAUAN PUSTAKA

### 2.1. Analisis

Analisis merupakan suatu proses engurai subjek menjadi berbagai bagiannya dan memeriksa hubungan antara bagian-bagian itu dan bagian-bagian itu sendiri untuk memahami makna keseluruhan dengan benar adalah cara lain untuk mendefinisikan analisis. Analisis adalah pengelompokan informasi, pengurutan, pengolahan, dan peringkasan agar lebih mudah dibaca.

### 2.2. Citra Digital

Citra digital dapat dihasilkan dari peralatan digital seperti kamera digital, sehingga dapat dengan mudah diolah di dalam komputer. Citra digital digunakan sebagai bukti dalam persidangan dan forensik digital karena datanya mengandung berbagai informasi[9]. Hal ini disebabkan oleh adanya sistem sampling dan kuantisasi pada peralatan tersebut, yang berfungsi untuk mengubah *citra kontinu* menjadi digital dan mengubah intensitas analog menjadi intensitas diskrit di dalamnya. Oleh karena itu, pemrosesan tambahan dapat dilakukan dengan menggunakan perangkat lunak komputer[10].

### 2.3. Bukti Digital

Pembuktian bukti tindak kejahatan tentunya memiliki kriteria, termasuk dalam proses pembuktian bukti yang diperoleh dari komputer [11]. Dengan adanya bidang ilmu forensik citra digital dapat membantu berbagai pihak seperti penegak hukum, investigasi, dan media[12].

### 2.4. Image Forensic

Bidang studi baru yang disebut forensik gambar bertujuan untuk mengekstrak informasi dari gambar untuk menentukan keasliannya juga dikenal sebagai keaslian gambar digital. Tujuan dari adanya investigasi kejahatan foto adalah untuk menemukan, mengidentifikasi, atau mencari foto yang terbukti rekayasa. Tujuan lainnya adalah untuk melindungi keaslian citra digital dalam bentuk foto atau gambar dari kejahatan atau penyalahgunaan foto atau gambar.

### 2.5. Digital Forensic

*Digital Forensic* adalah pembuatan bukti file digital untuk digunakan di pengadilan perdata atau pidana merupakan fokus utama bidang forensik digital ilmu komputer[13]. Digital forensik juga dapat disebut sebagai metode yang terkait dengan proses pemulihan dan penyelidikan terhadap bukti digital yang ditemukan [14].

### 2.6. Error Level Analysis

ELA adalah metode atau teknik forensik untuk menemukan bagian gambar atau foto yang telah diubah dengan menyimpan ulang gambar pada tingkat kualitas tertentu di antara berbagai tingkat kompresi terkomputerisasi[15]. Metode ini digunakan untuk mendeteksi manipulasi gambar secara visual dan telah berkembang dalam bidang ilmu forensik digital [16]. Dengan pemeriksaan *error level analysis*, dapat diketahui daerah mana yang dirancang atau diubah dari gambar, karena dalam pemeriksaan tingkat kesalahan, dengan asumsi ada daerah yang tidak sama dengan yang lain, seperti permukaan, batas, dan varietas, ini terjadi karena berbagai tingkat tekanan [17].

### 2.7. Metadata

Metadata merupakan informasi terstruktur yang berfungsi untuk menjelaskan, memberikan penjelasan, mempermudah pencarian, serta memudahkan penggunaan dan pengelolaan informasi. Metadata ini berisi data tentang item-item dalam suatu informasi yang digunakan untuk mencatat/informasi keperluan pengurus nantinya dalam suatu kumpulan data [18]. Detail tentang tanggal dan waktu penemuan, kamera atau ponsel yang digunakan untuk mengambil gambar, dan keterangan lainnya biasanya disertakan sebagai salah satu detail tambahan yang melengkapi dan menjelaskan suatu data tertentu untuk sebuah foto atau gambar [19].

### 2.8. Forensically Beta

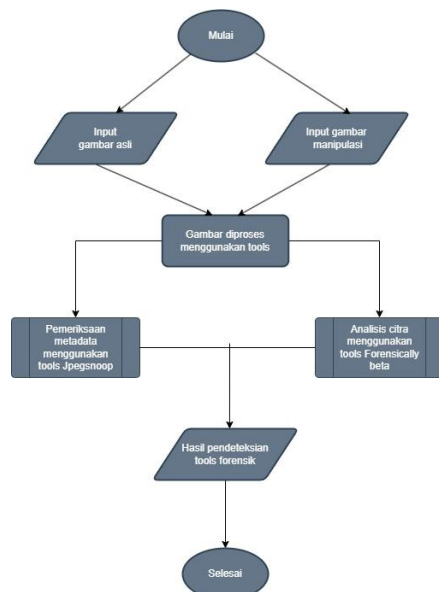
*Forensically Beta* merupakan sebuah *tools* gratis yang dapat digunakan untuk analisis forensik file gambar atau foto. *Forensically beta* ini berfungsi sebagai kaca pembesar yang berguna untuk membantu melihat detail dari sebuah gambar atau foto.

### 2.9. Jpegsnoop

*JPEGSnoop* adalah sebuah perangkat lunak yang digunakan untuk mengetahui apakah suatu foto asli atau tidak dengan melihat metadata pada file gambar yang sedang diperiksa. Alat yang dibuat mempunyai tujuan untuk mengungkapkan detail-detail pada suatu gambar sehingga dapat dilihat apakah gambar tersebut asli atau palsu. Dengan menggunakan alat *JPEGSnoop*, kita dapat mengekstrak berbagai informasi penting seperti pengaturan kualitas *JPEG*, pengaturan resolusi *JPEG*, metadata *EXIF*, dari suatu gambar [20].

## 3. METODE PENELITIAN

Pada bagian ini memuat metode yang digunakan pada pembuatan skripsi. Untuk analisis deteksi keaslian citra digital dalam bentuk foto atau gambar, metodologi yang digunakan adalah metode *National Institute of Standards and Technology* (NIST). Tahapan metode NIST terdiri dari *Collection*, *Examination*, *Analysis*, dan *Reporting*.



Gambar 1. Alur flowchart pendeteksian

Berdasarkan metode *National Institute of Standards Technology (NIST)*, terdapat 4 langkah dalam pengolahan dan identifikasi keaslian citra digital yaitu tahapan pengumpulan data/mengidentifikasi, tahap mengolah informasi, tahap analisis, dan terakhir tahap pelaporan bukti. Pada alur proses metode NIST ini alat yang dipergunakan untuk melakukan analisis pada gambar digital adalah sebuah skenario yang terdiri dari beberapa langkah. Pertama, persiapkan dua jenis file gambar asli dan gambar yang telah dimanipulasi. Kemudian, kedua jenis file pada gambar atau foto dimasukkan ke dalam *tools* yang digunakan dan lakukan deteksi keaslian gambar. Selanjutnya, bandingkan hasil deteksi dari kedua jenis gambar tersebut dengan menggunakan teknik *Error Level Analysis*. Gambar 1. Adalah flowchart yang menunjukkan bagaimana keaslian citra digital ditentukan.

## 4. HASIL DAN PEMBAHASAN

### 4.1. Hasil penelitian

Hasil penelitian yang telah dilakukan yaitu berupa image forensic untuk membandingkan foto asli dan foto yang sudah dimanipulasi dengan berdasarkan metode forensik. Pada penelitian ini dimana menyelesaikan kasus penyebaran foto untuk pemeriksaan foto tersebut dan juga akan melakukan perbandingan pada foto asli dan foto yang telah dimanipulasi.

### 4.2. Skenario kasus

Sebagai pembanding temuan dalam penelitian ini, foto yang merupakan hasil manipulasi dan asli akan dijadikan sebagai bukti dalam penelitian ini. Berikut adalah merupakan sumber-sumber bukti yang akan digunakan dalam penelitian ini:



Gambar 2. Foto pertama

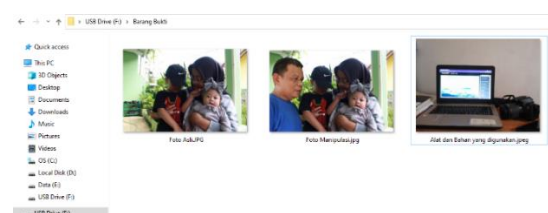
Foto pertama merupakan foto asli yang dipotret oleh korban menggunakan kamera digital. Lalu ada pelaku yang memanipulasi foto tersebut untuk dijadikan seolah-olah foto yang dimanipulasi itu foto asli tanpa editan.



Gambar 3. Foto kedua

### 4.3. Collection

Tahapan pertama pada penelitian ini dilakukan pengumpulan data berupa barang bukti yang terdapat pada flashdisk milik korban yang berisi foto asli dan foto yang telah dimanipulasi. Foto yang diambil menggunakan kamera digital dengan model *Canon EOS 700D*. Barang bukti milik korban tersebut akan dipindahkan ke pc/laptop penguji untuk diteliti dan dibandingkan hasilnya antara foto asli dan foto yang telah dimanipulasi.



Gambar 4. Bukti di flashdisk korban

### 4.4. Examination

Evaluasi terhadap foto akan dilakukan dengan memeriksa metadata dari kedua foto yang menjadi bukti penelitian pada tahap pemeriksaan atau dikenal juga dengan tahap identifikasi. Investigasi terkait metadata akan dilakukan dengan bantuan salah satu alat forensik, yaitu *tools Jpegsnoop*.

Tahap identifikasi utama metadata dilakukan menggunakan *tools Jpegsnoop* agar metadata foto lebih teridentifikasi dengan baik. Tahap identifikasi diawali dengan pemeriksaan informasi mengenai kamera yang digunakan, tanggal dan waktu pemotretan, dan informasi pemeriksaan lainnya.

```

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
OFFSET: 0x00000000

*** Marker: APPI (xFFE1) ***
OFFSET: 0x00000002
Length = 27200
Identifier = [Exif]
Identifier TIFF = 0x[49492A00 08000000]
Endian = Intel (little)
TAG Mark x002A = 0x002A

EXIF IFD0 @ Absolute 0x00000014
Dir Length = 0x000C
[Make] = "Canon"
[Model] = "Canon EOS 700D"
[Orientation] = 1 = Row 0: top, Col 0: left
[XResolution] = 72/1
[YResolution] = 72/1
[ResolutionUnit] = Inch
[DateTime] = "2023:05:06 10:54:24"
[Artist] = "SMILECREATIVE31"
[VCbCrPositioning] = Co-sited
[Copyright] = "SMILECREATIVE31"
[ExifOffset] = @ 0x0168
[GPSOffset] = @ 0x242A
Offset to Next IFD = 0x00002B2C

EXIF IFD1 @ Absolute 0x00002B38
Dir Length = 0x0006
[Compression] = JPEG
[XResolution] = 72/1
[YResolution] = 72/1
[ResolutionUnit] = Inch
[JpegIFOffset] = @ +0x2B8C = @ 0x2B98
[JpegIFByteCount] = 0x[00003EAA] / 16042
Offset to Next IFD = 0x00000000

```

Gambar 5. Metadata awal foto asli

```

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
OFFSET: 0x00000000

*** Marker: APPI (xFFE1) ***
OFFSET: 0x00000002
Length = 7777
Identifier = [Exif]
Identifier TIFF = 0x[49492A00 08000000]
Endian = Intel (little)
TAG Mark x002A = 0x002A

EXIF IFD0 @ Absolute 0x00000014
Dir Length = 0x0012
[IFD0.0x0100] = 3456
[IFD0.0x0101] = 2304
[IFD0.0x0102] = 8, 8, 8
[IFD0.0x0106] = 1
[Make] = "Canon"
[Model] = "Canon EOS 700D"
[Orientation] = 1 = Row 0: top, Col 0: left
[IFD0.0x0115] = 3
[XResolution] = 720000/10000
[YResolution] = 720000/10000
[ResolutionUnit] = Inch
[Software] = "Adobe Photoshop 22.2 (Windows)"
[DateTime] = "2023:05:09 19:46:32"
[Artist] = "SMILECREATIVE31"
[VCbCrPositioning] = Co-sited
[Copyright] = "SMILECREATIVE31"
[ExifOffset] = @ 0x0164
[GPSOffset] = @ 0x0524
Offset to Next IFD = 0x00000538

EXIF IFD1 @ Absolute 0x00000544
Dir Length = 0x0006
[Compression] = JPEG
[XResolution] = 72/1
[YResolution] = 72/1
[ResolutionUnit] = Inch
[JpegIFOffset] = @ +0x0596 = @ 0x05A2
[JpegIFByteCount] = 0x[000018C3] / 639
Offset to Next IFD = 0x00000000

```

Gambar 6. Metadata awal foto manipulasi

Pada bagian awal identifikasi untuk informasi dari foto asli dan manipulasi keduanya sama-sama berasal dari foto yang dipotret menggunakan kamera *canon* dengan model *Canon EOS 700D*. Perbedaan dari kedua foto tersebut dilihat dari keterangan tag *exif Date Time* atau yang menunjukkan tanggal dan waktu pengambilan foto yang teridentifikasi dari kedua foto tersebut berbeda, dan juga pada foto manipulasi teridentifikasi adanya rancang bangun menggunakan perangkat lunak, hasil pemeriksaan foto manipulasi terdeteksi foto tersebut sudah dirancang menggunakan *software editing* yaitu *Adobe Photoshop 22.2 Windows*, Dari hasil kompresi foto terdeteksi berekstensi *JPEG* baik untuk foto asli maupun hasil foto manipulasi.

```

*** Marker: APP13 (xFFED) ***
OFFSET: 0x0001248
Length = 10450
Identifier = [Photoshop 3.0]
SRSM [0x0401] Name="" Len=[0x0471] DefinedName="IPTC-GMA record"
IPTC [0x020001] Record Version = 0
IPTC [0x020002] By-line = "SMILECREATIVE31"
IPTC [0x020003] Date Created = "20230506"
IPTC [0x020004] Time Created = "20230506"
IPTC [0x020005] Copyright Notice = "SMILECREATIVE31"
SRSM [0x0402] Name="" Len=[0x0411] DefinedName="Caption digest"
Caption digest = [0x7F 9A 11 47 79 48 48 E6 A3 03 C9 03 FD 09 6C 5F | ...0yB.....1_
SRSM [0x0403] Name="" Len=[0x0E3] DefinedName="Print Information"
Print Information
[0x00 00 00 10 00 00 00 01 00 00 00 00 00 08 70 72 | .....PT
[0x00 4E 74 4F 75 74 70 75 74 00 00 00 00 08 00 00 | ..nchnp.....
[0x00 50 73 74 53 42 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F | ..FetBho.....n
[0x00 65 45 45 45 45 00 00 00 00 00 00 00 49 4E | ..eetm.....Ete.
[0x00 00 43 4C 72 4D 00 00 00 00 0F 70 72 49 4E 74 53 | ..CtM.....printS
[0x00 75 74 45 48 4E 42 49 74 42 4F 4F 4F 4F 4F 4F | ..etamBho.....
[0x00 0B 70 72 49 4E 74 45 72 4E 61 6D 45 54 45 50 | ..printetNewTEX
[0x00 00 00 00 00 00 00 00 0F 70 72 49 4E 74 | .....print
[0x00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
SRSM [0x0404] Name="" Len=[0x0220] DefinedName="Print Style"
Print Style
[0x00 00 00 10 00 00 00 01 00 00 00 00 00 12 70 72 | .....PT
[0x00 4E 74 4F 75 74 70 75 74 4F 70 74 49 4E 4F 73 | ..nchnp.....p
[0x00 00 00 17 00 00 00 00 43 70 74 4E 42 4F 4F 4F 4F | .....GpsBho
[0x00 00 00 00 43 4C 42 42 42 42 4F 4F 4F 4F 4F 4F | .....C
[0x00 00 52 47 73 42 42 4F 4F 4F 4F 4F 4F 4F 4F 4F | ..BpsBho.....C
[0x00 4E 43 42 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F | ..nchnp.....C
[0x00 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F 4F | ..Bho.....Bho
[0x00 00 00 00 00 00 4E 4F 74 74 42 4F 4F 4F 4F 4F | .....BpsBho..
[0x00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
SRSM [0x0405] Name="" Len=[0x0013] DefinedName="ResolutionInfo structure"
ResolutionInfo structure
Width unit = inch
Vertical resolution = 72 pixels per inch
Height unit = inch
SRSM [0x0406] Name="" Len=[0x000E] DefinedName="Print scale"
Print scale
Style = centered
X location = 0.00000
Y location = 0.00000
Scale = 1.00000

```

Gambar 7. Identifier photoshop

Pada gambar 7. Metadata pada keterangan Identifier: *[Photoshop 3.0]*: menunjukkan identifikasi secara keseluruhan pada foto manipulasi, keterangan ini memberikan informasi tentang struktur dan konten dari file Photoshop, termasuk metadata foto, informasi pencetakan, gaya cetakan, dan informasi resolusi.

```

*** Marker: DQT (xFFDB) ***
Define a Quantization Table.
OFFSET: 0x00007446
Table length = 132
-----
Precision=8 bits
Destination ID=0 (Luminance)
DQT, Row #0: 1 1 1 1 1 2 3 3
DQT, Row #1: 1 1 1 1 1 3 3 3
DQT, Row #2: 1 1 1 1 1 2 3 3
DQT, Row #3: 1 1 1 1 2 3 4 4
DQT, Row #4: 1 1 2 3 3 5 5 4
DQT, Row #5: 1 2 3 3 4 5 5 4
DQT, Row #6: 2 3 4 4 5 6 6 5
DQT, Row #7: 4 4 5 5 5 5 5 5
Approx quality factor = 97.29 (scaling=5.41 variance=1.48)
-----
Precision=8 bits
Destination ID=1 (Chrominance)
DQT, Row #0: 1 1 1 1 2 5 5 5
DQT, Row #1: 1 1 1 3 5 5 5 5
DQT, Row #2: 1 1 3 5 5 5 5 5
DQT, Row #3: 2 3 5 5 5 5 5 5
DQT, Row #4: 5 5 5 5 5 5 5 5
DQT, Row #5: 5 5 5 5 5 5 5 5
DQT, Row #6: 5 5 5 5 5 5 5 5
DQT, Row #7: 5 5 5 5 5 5 5 5
Approx quality factor = 97.51 (scaling=4.97 variance=0.11)

```

Gambar 8. Hasil kualitas foto asli

Gambar 8. Mengidentifikasi foto asli pada bagian definisi dari *Quantization Table* (Tabel Kuantisasi) pada suatu data gambar dengan ukuran 132 *byte* dimulai dari *offset* 0x00007446. Terdapat dua jenis tabel kuantisasi pada gambar tersebut dengan presisi 8 *bit* dan *ID* destinasi 0 (untuk *luminance* atau kecerahan) dan *ID* destinasi 1 (untuk *chrominance* atau warna). Masing-masing tabel kuantisasi memiliki 8 baris dan 8 kolom. Setiap nilai pada tabel kuantisasi menentukan skala kuantisasi untuk koefisien transformasi yang telah dikuantisasi. Selain itu, pada tabel kuantisasi tersebut juga terdapat perkiraan faktor kualitas dengan skala dan variansinya untuk setiap jenis tabel kuantisasi. Faktor kualitas berkaitan dengan seberapa baik gambar tersebut dapat direkonstruksi kembali tanpa kehilangan banyak informasi, semakin tinggi faktor kualitas, semakin sedikit kehilangan informasi yang terjadi pada gambar.

```

*** Marker: DQT (xFFD8) ***
Define a Quantization Table.
Offset: 0x0000482
Table length = 132
----
Precision=8 bits
Destination ID=0 (Luminance)
DQT, Row #0: 6 4 7 11 14 17 22 17
DQT, Row #1: 4 5 6 10 14 19 12 12
DQT, Row #2: 7 6 8 14 19 12 12 12
DQT, Row #3: 11 10 14 19 12 12 12 12
DQT, Row #4: 14 14 19 12 12 12 12 12
DQT, Row #5: 17 19 12 12 12 12 12 12
DQT, Row #6: 22 12 12 12 12 12 12 12
DQT, Row #7: 17 12 12 12 12 12 12 12
Approx quality factor = 83.88 (scaling=32.24 variance=430.71)
----
Precision=8 bits
Destination ID=1 (Chrominance)
DQT, Row #0: 7 9 19 34 20 20 17 17
DQT, Row #1: 9 12 19 14 14 12 12 12
DQT, Row #2: 19 19 14 14 12 12 12 12
DQT, Row #3: 34 14 14 12 12 12 12 12
DQT, Row #4: 20 14 12 12 12 12 12 12
DQT, Row #5: 20 12 12 12 12 12 12 12
DQT, Row #6: 17 12 12 12 12 12 12 12
DQT, Row #7: 17 12 12 12 12 12 12 12
Approx quality factor = 85.11 (scaling=21.78 variance=377.49)

```

Gambar 9. Hasil kualitas foto manipulasi

Gambar 9. merupakan tabel hasil *Quantization* untuk format gambar yang dikompresi menggunakan algoritma *JPEG*. Tabel tersebut terdiri dari dua bagian, yaitu untuk *Luminance* (ID Tujuan 0) dan *Chrominance* (ID Tujuan 1). Nilai-nilai yang lebih besar dalam tabel menyebabkan pembagian menjadi lebih kasar dan mengurangi kualitas gambar. Sebaliknya, nilai-nilai yang lebih kecil dalam tabel menghasilkan pembagian yang lebih halus dan kualitas gambar yang lebih baik. Kualitas kompresi gambar dapat diatur melalui nilai-nilai dalam tabel, dengan nilai yang lebih besar menghasilkan kompresi yang lebih rendah (kualitas yang lebih buruk) dan nilai yang lebih kecil menghasilkan kompresi yang lebih tinggi (kualitas yang lebih baik).

```

*** Searching Compression Signatures ***
Signature: 01A2A9C366F7E7B00DAE5D5B83230
Signature (Rotated): 01F9F8F8F121D1D34F7F1A3BC24F
File Offset: 0 bytes
Chroma subsampling: 4:1
EXIF Make/Model: OK [Canon] [Canon EOS 700D]
EXIF Makernotes: NONE
EXIF Software: NONE

Searching Compression Signatures: (3347 built-in, 5 user(*) )

EXIF.Make / Software      EXIF.Model      Quality      Subcomp Match?
-----
CMK [Canon]              [Canon EOS 40D]  [false]      [Yes]
CMK [Canon]              [Canon EOS 450D] [false]      [Yes]
CMK [Canon]              [Canon EOS 500D] [false]      [Yes]
CMK [Canon]              [Canon EOS 50D]  [false]      [Yes]
CMK [Canon]              [Canon EOS 550D] [false]      [Yes]
CMK [Canon]              [Canon EOS 5D]   [false]      [Yes]
CMK [Canon]              [Canon EOS 5D Mark II] [false] [Yes]
CMK [Canon]              [Canon EOS 5D Mark III] [false] [Yes]
CMK [Canon]              [Canon EOS 600D] [false]      [Yes]
CMK [Canon]              [Canon EOS 60D]  [false]      [Yes]
CMK [Canon]              [Canon EOS 7D]   [false]      [Yes]
CMK [Canon]              [Canon EOS DIGITAL REBEL X3] [false] [Yes]
CMK [Canon]              [Canon EOS DIGITAL REBEL T1i] [false] [Yes]
CMK [Canon]              [Canon EOS REBEL T2i] [false] [Yes]
CMK [Canon]              [Canon EOS REBEL T3i] [false] [Yes]
CMK [Canon]              [Canon EOS-1D Mark III] [false] [Yes]
CMK [Canon]              [Canon EOS-1D Mark III] [false] [Yes]
CMK [Canon]              [Canon EOS 700D] [false]      [Yes]
CMK [Canon]              [Canon EOS 700D] [false]      [Yes]

Based on the analysis of compression characteristics and EXIF metadata:
ASSESSMENT: Class 3 - Image has high probability of being original

```

Gambar 10. Hasil kompresi foto asli

Gambar 10. Merupakan keterangan yang mengacu pada proses pencarian tanda-tanda kompresi pada sebuah file gambar, serta analisis metadata *EXIF* yang terkait. Yang membuktikan jelas bahwa foto ini asli terdapat pada keterangan *EXIF Make/Model*, menunjukkan informasi tentang merek dan model kamera yang digunakan untuk mengambil gambar, dalam metadata *EXIF*. *EXIF Makernotes* menunjukkan bahwa metadata *EXIF makernotes* ada dalam file gambar, dan pada bagian keluaran *EXIF Software* menunjukkan perangkat lunak *EXIF* yang digunakan untuk mengedit atau memanipulasi gambar, dan pada keterangan *software* mengidentifikasi “NONE” dimana foto tidak adanya campur tangan menggunakan *software editing*.

```

*** Searching Compression Signatures ***
Signature: 01A2A9C366F7E7B00DAE5D5B83230
Signature (Rotated): 01F9F8F8F121D1D34F7F1A3BC24F
File Offset: 0 bytes
Chroma subsampling: 4:1
EXIF Make/Model: OK [Canon] [Canon EOS 700D]
EXIF Makernotes: NONE
EXIF Software: OK [Adobe Photoshop 22.2 (Windows)]

Searching Compression Signatures: (3347 built-in, 6 user(*) )

EXIF.Make / Software      EXIF.Model      Quality      Subcomp Match?
-----
SW [Adobe Photoshop]     [Save As 00]    [false]      [Yes]
*SW [Adobe Photoshop 22.2 (Win)] [false] [Yes]

NOTE: Photoshop 1B2 detected
NOTE: EXIF Software field recognized as from editor
Based on the analysis of compression characteristics and EXIF metadata:
ASSESSMENT: Class 1 - Image is processed/edited

```

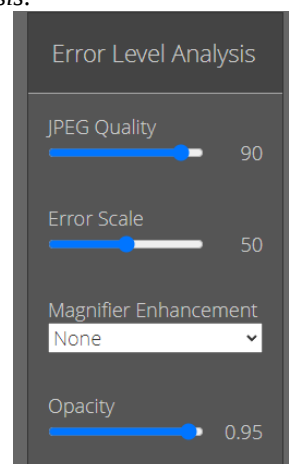
Gambar 11. Hasil kompresi foto manipulasi

Keterangan pada foto manipulasi memberikan informasi terkait hasil pencarian kompresi pada sebuah file gambar atau hasil akhir dari identifikasi. Hasil identifikasi yang jelas dapat dilihat di bagian *EXIF Make/Model*, dimana informasi tersebut membuktikan pembuat dan model perangkat yang digunakan untuk mengambil gambar. Dalam contoh ini, pembuat kamera adalah *Canon* dan modelnya adalah *Canon EOS 700D*. *EXIF Makernotes* memberikan informasi tambahan yang terkait dengan perangkat pembuat gambar. Dalam contoh ini, tidak ada informasi tambahan yang ditemukan. Akan tetapi, pada bagian *software* terdeteksi yang digunakan untuk memproses gambar. Dalam contoh ini, perangkat lunak yang digunakan adalah *Adobe Photoshop 22.2 (Windows)*. Pada tabel keterangan *EXIF Make/Software*, yaitu membuktikan hasil akhir informasi tentang pembuat perangkat (*Make*) dan perangkat lunak (*Software*) yang terkait dengan gambar.

Berdasarkan analisis karakteristik kompresi dan metadata *EXIF*, gambar tersebut diklasifikasikan sebagai “Class 1 - Image is processed/edited”, yang berarti gambar tersebut telah diolah atau diedit menggunakan perangkat lunak seperti *Adobe Photoshop*.

#### 4.5. Analysis

Sebelumnya, kedua file foto sudah diperiksa untuk melihat metadata dari kedua gambar tersebut. Pada tahapan ini akan dilakukan pengamatan untuk menganalisis kedua gambar untuk mencari tingkat kesalahan pada foto atau menerapkan teknik *Error Level Analysis*.



Gambar 12. Indikator ELA

Gambar 12. merupakan pengaturan untuk foto asli dan manipulasi. Foto manipulasi dalam forensically beta mulai dianalisis dengan menurunkan kualitas jpeg menjadi 90, skala kesalahan dinaikan menjadi 50, dan kegelapan diturunkan menjadi 0.95, untuk mencari tingkat kesalahan pada kedua foto tersebut.



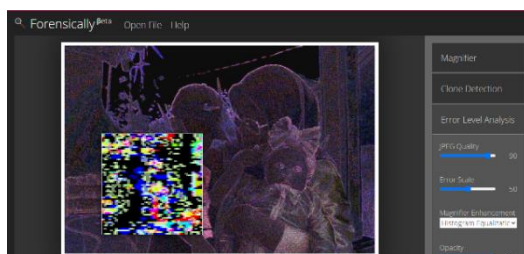
Gambar 13. Hasil ELA foto asli

Kemudian mendapatkan hasil foto asli terlihat lebih terang dan banyaknya bintik-bintik putih pada foto, serta tidak menghilangkan objek di sekitarnya. Pada foto manipulasi setelah diatur dengan tingkatan yang sama dengan foto asli memiliki perubahan yaitu foto menjadi lebih terlihat gelap dan banyaknya bintik-bintik hitam pada foto pada objek yang telah diedit.

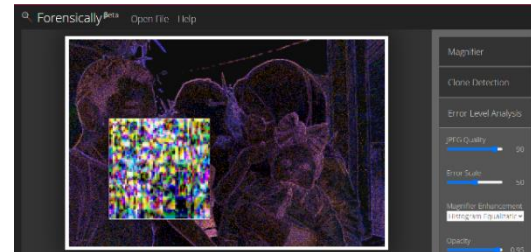


Gambar 14. Hasil ELA foto manipulasi

Untuk melihat perbedaan tekstur dari kedua foto tersebut melakukan pengaktifan *histogram equalization* pada bagian *magnifier enhancement*. Dengan menggeser kursor ke daerah yang akan diamati tekstur tampak lebih kacau di area yang direkayasa daripada di area lain atau area asli.



Gambar.15 Tekstur daerah foto asli



Gambar.16 Tekstur daerah foto manipulasi

Dari hasil mengamati kedua foto berupa foto asli dan foto manipulasi mendapatkan hasil analisis dimana foto asli terlihat lebih terang dan adanya bintik putih serta objek latar belakang foto terlihat lebih jelas dan tidak adanya perubahan bentuk. Sedangkan foto manipulasi, foto terlihat gelap dan banyaknya bintik-bintik hitam di bagian yang termanipulasi serta objek latar belakang pun sudah tidak terlihat jelas.

#### 4.6. Reporting

Untuk setiap foto dapat ditarik kesimpulan dari penelitian yang telah dilakukan. Untuk kesimpulan pada kedua foto bisa dilihat pada gambar tabel dibawah ini.

Tabel 1. Report hasil

| Pelaporan                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                      |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| Deteksi Citra                                                                                              | Teknik Error Level Analysis                                                                                                                                                                                                                                                                                                                                                                                                              | Metadata                             |
| <p>Foto Asli</p>        |  <ul style="list-style-type: none"> <li>• Citra asli dengan <i>Forensically beta</i></li> <li>• Mengatur <i>JPEG Quality</i> menjadi 90</li> <li>• <i>Error scale</i> 50</li> <li>• Merendahkan <i>Opacity</i> menjadi 0.95</li> <li>• Foto terlihat lebih banyak bintik-bintik putih dan objek latar belakang foto terlihat lebih jelas</li> </ul> | <p>Assignment Class 3 = Original</p> |
| <p>Foto Manipulasi</p>  |  <ul style="list-style-type: none"> <li>• Pengaturan dalam citra sama seperti deteksi pada foto asli</li> <li>• Citra terdeteksi manipulasi gambar terlihat gelap dan banyak bintik-bintik hitam dan foto yang sudah dimanipulasi terlihat menonjol</li> </ul>                                                                                      | <p>Assignment Class 1 = Edited</p>   |

Tabel 1. Berisi informasi tentang deteksi manipulasi gambar menggunakan teknik *Error Level Analysis* dan analisis metadata pada dua foto, yaitu foto asli dan foto manipulasi. Deteksi gambar dilakukan dengan menganalisis tingkat kesalahan dalam kompresi *JPEG* menggunakan teknik *Error Level Analysis* untuk mengungkap tanda-tanda manipulasi pada kedua foto. Selain itu, analisis metadata juga dilakukan untuk memberikan petunjuk tambahan tentang keaslian dan pengeditan gambar.

Hasil deteksi pada foto asli menunjukkan adanya bintik-bintik putih dan objek latar belakang yang masih terlihat jelas. Hasil analisis metadata pada foto asli menunjukkan kelas penilaian 3, yang mengindikasikan bahwa foto tersebut asli.

Namun, pada foto manipulasi terlihat perbedaan dengan foto asli. Terdeteksi adanya manipulasi gambar dengan penambahan objek baru sehingga terlihat seperti foto asli. Foto manipulasi ini memiliki ciri-ciri seperti citra yang gelap, banyak bintik hitam pada area foto, dan objek manipulasi yang menonjol. Hasil analisis metadata menunjukkan kelas penilaian 1, yang menunjukkan bahwa foto tersebut telah mengalami proses edit.

## 5. KESIMPULAN DAN SARAN

Dalam kasus ini, salah satu dari dua foto yang dijadikan barang bukti ternyata merupakan hasil manipulasi. Pemindaian dilakukan menggunakan *Jpegsnoop* untuk mengidentifikasi kedua foto dan mendapatkan metadata. Foto utama atau foto asli teridentifikasi berasal dari kamera digital model *Canon EOS 700D* dan dinyatakan sebagai foto original (*assessment class 3*). Sebaliknya, metadata pada foto kedua atau foto manipulasi menunjukkan bahwa foto tersebut telah diedit menggunakan *Adobe Photoshop* dan dinyatakan sebagai foto manipulasi (*assessment class 1*).

Setelah mendapatkan metadata, dilakukan analisis tingkat kesalahan (*error level analysis*) dengan bantuan *Forensically beta*. *Error level analysis* digunakan untuk mengidentifikasi area yang berbeda dalam foto yang dapat menunjukkan tanda-tanda manipulasi, seperti perbedaan tekstur dan warna pada objek yang ditambahkan.

Untuk penelitian selanjutnya, disarankan untuk menggunakan teknik analisis lain seperti *noise analysis*, *principal component analysis* (PCA), dan alat lainnya untuk eksplorasi citra forensik. Terdapat banyak alat selain *Forensically beta* dan *Jpegsnoop* yang dapat digunakan untuk melakukan lebih banyak proses pemeriksaan dalam penelitian selanjutnya. Dan juga disarankan untuk peneliti selanjutnya menganalisis lebih dalam menentukan tekstur histogram gambar dan juga *pixel* gambar.

## DAFTAR PUSTAKA

- [1] Wicaksono, A., Mardiyantoro, N., & Sibyan, H. (2022). Biner : Jurnal Ilmiah Informatika dan Komputer, vol. 1, no. 1, pp. 62-69, Jan. 2022.

Penerapan Metode Error Level Analysis Untuk Mendeteksi Modifikasi Citra Digital. Biner : Jurnal Ilmiah Informatika dan Komputer, vol. 1, no. 1, pp. 62-69, Jan. 2022.

- [2] A. Firdonsyah and D. Wijayanto, "Analisis Forensik Rekayasa Dokumen Digital dengan Metode NIST," *INFORMAL Informatics J.*, vol. 7, no. 2, p. 121, 2022.
- [3] Iman, N., Susanto, A., & Ingg, R. (2019). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *Jurnal Telekomunikasi dan Komputer*, vol. 9, no. 3, p. 186, Jan. 2019.
- [4] S Nawawi, H. P., Carudin, C., & Yusup, D. (2022). Analisis Penemuan Barang Bukti Digital Melalui Rekaman Suara Menggunakan Praat Dengan Metode Audio Forensik. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, 7(1), 10–19. <https://doi.org/10.32528/justindo.v7i1.5368>
- [5] Gangwar, D. P., & Pathania, A. (2018). Authentication of Digital Image using Exif Metadata and Decoding Properties. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, December, 335–341. <https://doi.org/10.32628/cseit183815>
- [6] Harahap, F. (2021). Deteksi Foto Manipulasi Dengan Tools Forensicallybeta dan Imageforensic.org Dengan Metode Error Level Analysis (ELA). *TIN: Terapan Informatika Nusantara*, 2(3), 159–164.
- [7] Irwansyah, I., & Yudiastuti, H. (2019). Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop Dan Forensically Beta. *Jurnal Ilmiah Matrik*, 21(1), 54–63. <https://doi.org/10.33557/jurnalmatrik.v21i1.518>.
- [8] A. C. S. Joel Panjaitan, "Analisis Kinerja Forensic Acquisition Tools Untuk Membuat Imaging File Pada Masalah IT Forensik," *JUTISAL (Jurnal Tek. Inform. Komput. Universal)*, vol. Vol. 1, no. No. 2, pp. 17–25, 2021.
- [9] H. A. A. P. K. Khairunnisak Nur Isnaini, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST," *Jurnal Resistor*, vol. Vol. 3 No 2, no. Oktober 2020, pp. 72–81, 2020.
- [10] Apriliani, A., Hijjayanti, K., & Suhairoh, S. (2020). Analisis Keaslian Citra Dengan Menggunakan Exif Metadata. *CESS (Journal of Computer Engineering, System and Science)*, 5(1), 84. <https://doi.org/10.24114/cess.v5i1.15600>
- [11] Mubara, M. F., Rusmana, D., & Ladjamuddin, S. M. (2020). Evidence Of The Case Of Crime DDos Using Forensic Digital File Analysis System Method. *Incomtech: Jurnal Penelitian Teknologi Informatika dan Komunikasi*, 9(2), 38–47.

- [12] Al Caruban, R., Sugiantoro, B., & Prayudi, Y. (2018). Analisis Pendeteksi Kecocokan Objek Pada Citra Digital Dengan Metode Algoritma Sift Dan Histogram Color Rgb. *Cyber Security Dan Forensik Digital*, 1(1), 20–27. <https://doi.org/10.14421/csecurity.2018.1.1.1235>
- [13] Faroek, D. A, Umar, R., Riadi, I. (2019). Deteksi Keaslian Citra Menggunakan Metode Error Level Analysis (ELA) dan Principal Component Analysis (PCA). *Jurnal Ilmiah Teknik Informatika*, vol. 8 Nomor 2, 2019.
- [14] P. Mahardika Sulaksono and B. Santoso, “Static Forensic Pada USB Mass Storage Menggunakan Forensics Toolkit Imager,” *J. Komput. Terap.*, vol. 8, no. Vol. 8 No. 1 (2022), pp. 132–142, 2022.
- [15] I. Gede, N. B. Darmawan, G. Made, A. Sasmitha, and P. Wira Buana. (2019). Pengembangan Metode Pendeteksi Modifikasi Citra Menggunakan Metode Error Level Analysis. *Jurnal Ilmiah Merpati*, vol. 7, no. 1, 2019.
- [16] Rahman, F. M., Putra, R. R. J., & Wihardi, Y. (2020). Analisis Statistik dan Implementasi Image Masking Berdasarkan Hasil Error Level Analysis pada Gambar Digital. *JATIKOM: Jurnal Aplikasi Dan Teori Ilmu Komputer*, 3(1), 22–28.
- [17] I. P. Wiratama, A. Suharso, and C. Rozikin, “Akuisisi Bukti Digital Dan Deteksi Keaslian Citra Pada Whatsapp Menggunakan Metode NIST Dan ELA,” *J. Sains Komput. Inform.*, vol. 5, no. 2, pp. 712–726, 2021.
- [18] I. Sopiandi, “Menggali Informasi Metadata Pada Citra Digital Yang Tersembunyi,” *Infotech J.*, vol. 3, no. 2, p. 236707, 2017.
- [19] Putra, A. I., Umar, R., & Fadlil, A. (2018). Forensic Analysis Video Metadata Authenticity Detection Using Exiftool. *Seminar Nasional Informatika 2018 (SemnasIF 2018)*, 2018(November), 21–25.
- [20] Parveen, A., Khan, Z. H., & Ahmad, S. N. (2020). Classification And Evaluation Of Digital Forensic Tools. *Telkomnika (Telecommunication Computing Electronics and Control)*, 18(6), 3096–3106. <https://doi.org/10.12928/TELKOMNIKA.v18i6.15295>.