Jurnal Mobile and Forensics (MF)
Vol. 1, No. 1, Maret 2019, pp. 13-21
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: http://dx.doi.org/10.12928/mf.v1i1.703

DETEKSI PEMALSUAN FOTO DIGITAL MENGGUNAKAN IMAGE FORENSICS

[1]Imam Riadi, [2]Anton Yudhana, [3]Wicaksono Yuli Sulistyo
[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[2]Program Studi Teknik Elektro, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan Yogyakarta, Indonesia
e-m ail: imam.riadi@is.uad.ac.id[1], eyudhana@ee.uad.ac.id[2], wicaksono1807048009@webmail.uad.ac.id[3]

Abstrak

Perkembangan foto yang semakin maju membuatnya memiliki banyak keunggulan dan kekurangan, salah satunya adalah mudahnya dimanipulasi dengan *software editing*. Perubahan foto dapat dibuat atau diedit dengan mudah, sehingga dapat merubah informasi yang disampaikan menjadi berbeda dan membuatnya rawan digunakan untuk tindak kejahatan. Forensik citra digital merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan keaslian image. Hal ini menjadi dasar penelitian ini untuk mendeteksi pemalsuan foto digital. Penelitian ini menggunakan analisa dengan 3 *tools forensics* yaitu FotoForensics, ForensicallyBeta dan Opanda IExif. Hasil yang didapat dari penelitian ini adalah terdeteksinya perbedaan metadata dan perbedaan kontras antara foto asli dan foto manipulasi yang menunjukan adanya perubahan pada foto tersebut.

Kata Kunci: *foto digital, pemalsuan foto, digital forensics, image forensics, tools forensics*

PENDAHULUAN

Perkembangan zaman yang semakin maju membuat semuanya sudah serba digital, termasuk urusan foto. Foto digital memiliki banyak keunggulan sekaligus kekurangan seperti bisa dimanipulasi dengan *software editing*, sehinga foto hasil editan bisa terlihat asli seperti nyata (Zam, 2015). Bentuk editan yang bisa bermacam-macam, mulai dari sekedar melakukan *cropping*, meningkatkan kecerahan, memasang *background*, dan memanipulasi bagian tertentu. Teknik manipulasi foto yang semakin bagus, terkadang sangat sulit untuk membedakan foto asli dengan foto hasil manipulasi (Febrianda, Andreswari, & Wulandari, 2018).

Kemajuan pada *software editing* membuatnya lebih mudah bagi seseorang untuk memanipulasi suatu gambar. Manipulasi gambar dikategorikan menjadi tiga jenis, yaitu *image spilicing*, manipulasi gambar *copy-move* dan *retouching image* (Fadlil, Riadi, & Sari, 2017). Manipulasi citra adalah kegiatan yang sering kali dilakukan seblum citra tersebut dipublikai, umumnya karena memiliki tujuan tertentu seperti untuk menyindir seseorang dan memperbaiki penampilan (Kresnha, Susilowati, & Adharani, 2016). Salah satu jenis pemalsuan citra paling umum dilakukan adalah teknik *copy-move* karena sangat mudah dan efektif. *Copy-move* merupakan pemalsuan citra dengan cara membuat suatu objek menghilang dari gambar yang menutupinya dengan blok kecil disalin dari bagian yang sama (Wijaya, Musayyab, & Studiawan, 2017). Kejahatan berbasis teknologi mengalami peningkatan dalam berbagai modus, oleh karena itu diperlukan suatu mekanisme ilmiah untuk menganalisis dan menelusuri bukti-bukti digital yang ada (Saputra & Widiyasono, 2017).

Received 10 April 2019; Revised 20 September 2019; Accepted 20 September 2019

Citra merupakan representasi dari suatu objek atau kejadian (Zulfan, Arnia, & Muharar, 2018). Citra juga bisa disebut sebagai output dari alat perekaman, seperti kamera analog maupun digital (Saifullah, Sunardi, & Yudhana, 2018). Citra atau gambar digital digunakan sebagai media komunikasi untuk penyampaian informasi sehingga keaslian suatu citra memiliki peran yang penting (Efendi, 2018). Pengolahan *image* pada citra digital dapat dibuat atau diedit dengan mudah, tanpa meninggal petunjuk visual oleh penggunanya, seperti Adobe Photoshop, Picasa dan PhotoScape. Kemudahan dalam membuat dan merubah suatu citra dapat merusak kredibilitas keaslian gambar dalam berbagai aspek, sehingga membuat rawan untuk digunakan untuk tindak kejahatan karena perubahan gambar tersebut dapat merubah informasi yang disampaikan menjadi berbeda (Rosidin, 2018).

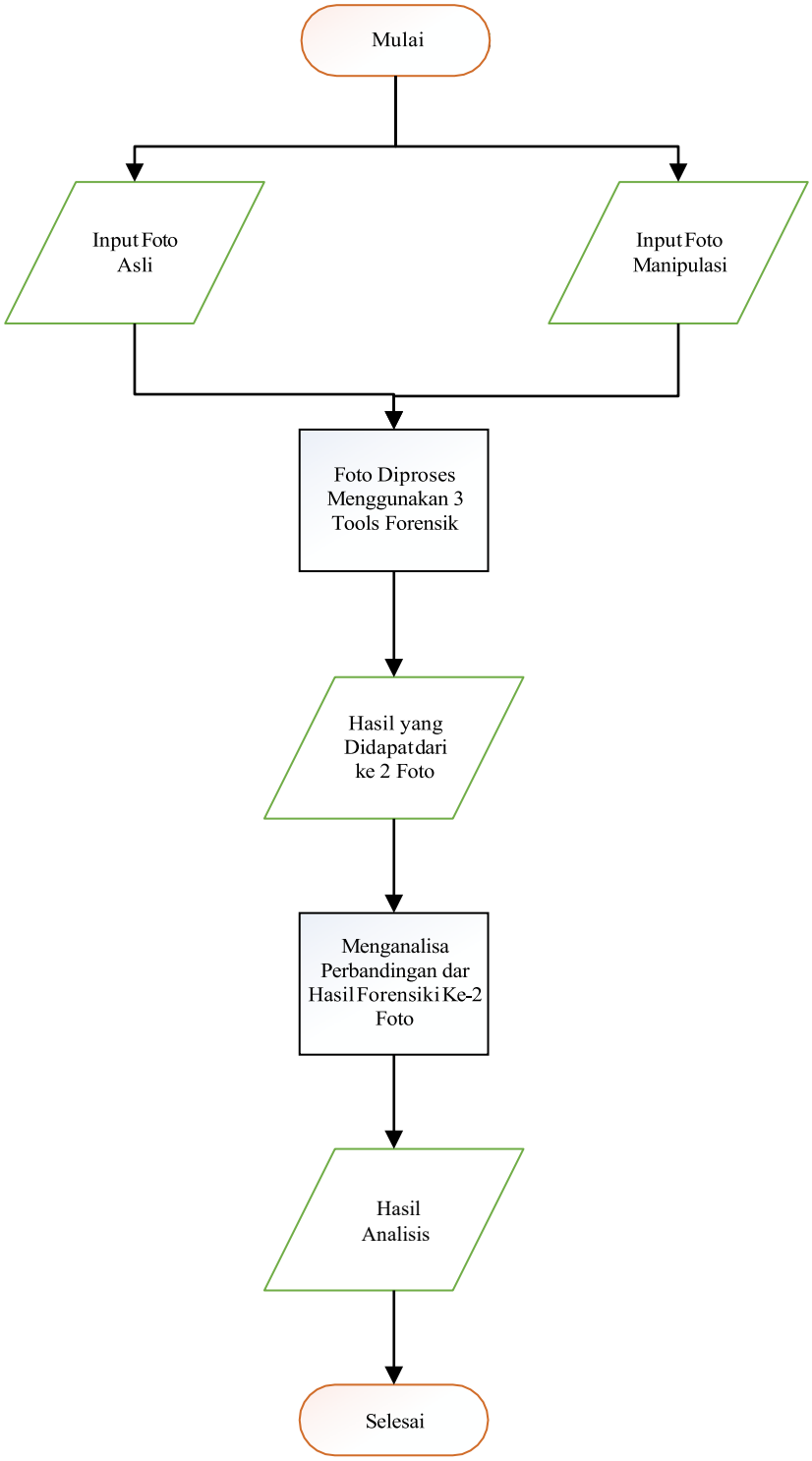
Digital forensics merupakan aktifitas yang berhubungan dengan dokumentasi, identifikasi, penyaringan, pengambilan barang bukti digital dalam kejahatan komputer (Saputra & Widiyasono, 2017). *Digital forensics* mempunyai banyak kegunaan dan dapat ditempatkan dalam berbagai keperluan, bukan hanya untuk menangani kasus kriminal yang melibatkan hukum, seperti rekontruksi perkara insiden keamanan komputer, pemecahan masalah yang melibatkan *hardware* dan *software*, dan upaya pemulihan kerusakan *system* (Silalahi & Sembiring, 2017). *Digital forensics* memberikan suatu keahlian secara teknis pada pengumpulan bukti-bukti secara digital untuk disajikan dalam suatu persidangan yang sesuai dengan hukum yang berlaku (Febriyanto & Sembiring, 2016). *Digital forensics* dapat dibagi lagi menjadi beberapa bagian, seperti *Disk Forensics*, *Network Forensics*, *Mobile Forensics*, *Image Forensics* dan *System Forensics* (Ruci Meiyanti & Ismaniah, 2015). Salah satu kasus yang sering terjadi untuk penggunaan *digital forensics* adalah pada kasus *cybercrime*. *Cybercrime* memiliki sifat efisien dan cepat serta sehingga menyulitkan bagi pihak penyelidik dalam melakukan penangkapan terhadap pelakunya. Hal ini disebabkan karena kurangnya pemahaman dan pengetahuan dalam penanggulangan *cybercrime*. Dalam ini hal ini perlu adanya penataan hukum dan proses pengawasan masyarakat terhadap setiap aktivitas yang diduga berkaitan dengan kejahatan *cybercrime* tersebut (Agus & Riskawati, 2016).

Bidang ilmu forensik citra digital akan membantu para penegak hukum, intelijen, investigasi swata dan media. Semakin majunya teknologi *image* pada saat ini mengangkat isu-isu baru dan tantangan dalam menentukan keaslian *image*. Forensik citra digital merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan keaslian *image* (Sulistyo, Riadi, & Yudhana, 2018). Berbagai kasus kriminal dan pornografi yang melibatkan file gambar masih kerap terjadi, oleh karena itu forensik terhadapat gambar sebagai barang bukti menjadi kunci penting untuk membantu pengadilan dalam mengambil keputusan (Sahera, 2016).

Penelitian yang akan dilakukan merupakan penelitian lanjutan dari penelitian yang sebelumnya oleh Wicaksono Yuli Sulistyo, Imam Riadi dan Anton Yudhana pada tahun 2018 yang berjudul "Analisis Deteksi Keaslian Citra Menggunakan Teknik *Error Level Analysis* Dengan ForensicallyBeta". Sedangkan pada penelitian ini akan menggunakan 3 *tools*, yaitu FotoForensics untuk teknik *error level analysis*, ForensicallyBeta untuk teknik *clone detection* dan Opanda IExif untuk analisis metadata.

METODE PENELITIAN

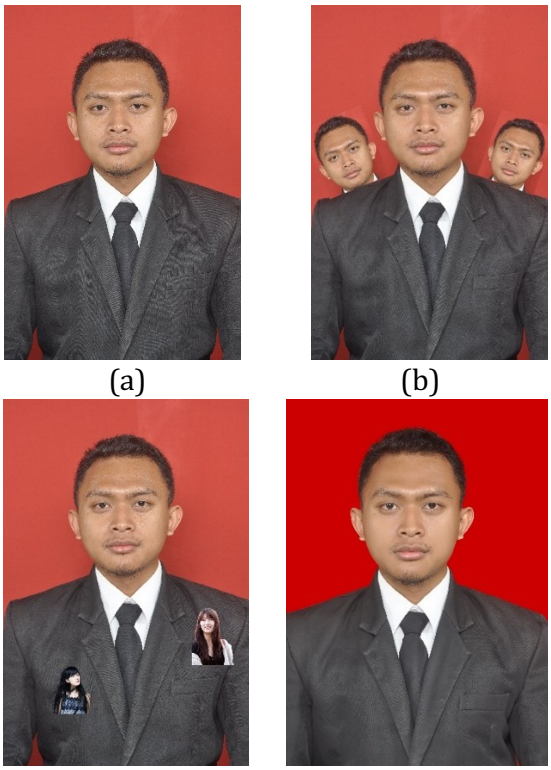
Penelitian ini menggunakan skema sendiri untuk proses pendeteksian *image* dalam mendapatkan suatu bukti digital yang digunakan untuk dianalisa. Gambar 1. merupakan skema *flowchart* dalam proses forensik pendeteksian.



Gambar 1. Alur *Flowchart* Proses Pendeteksian

Parameter yang digunakan untuk pendeteksian *image forensics* ini adalah metadata dan perbedaan kontras antara foto asli dengan foto manipulasi. Penelitian ini menggunakan 3 buah *tools*, yaitu FotoForensics untuk teknik *error level analysis*, ForensicallyBeta untuk teknik *noise analysis* dan Opande IExif untuk analisis metadata.

Gambar 2. merupakan bahan penelitian yang disiapkan untuk skenario pendeteksian. Gambar tersebut terdapat 1 buah foto asli dan 3 foto dengan perbedaan manipulasi masing-masing.



(a) (b)

(c) (d)

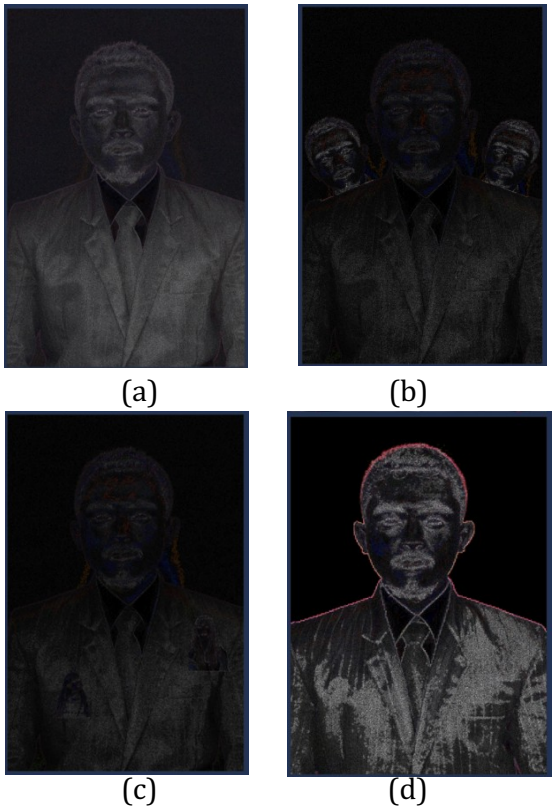
Gambar 2. Foto Bahan Penelitian (a) asli (b) *copy-move* (c) *image splicing* (d) *image retouching*

HASIL DAN PEMBAHASAN

Proses pendeteksian diawali dengan membuat scenario berupa menyiapkan 4 foto yang merupakan 1 foto asli dan 3 foto dengan jenis manipulasi masing- masing. Kemudian semua foto tersebut diproses menggunakan ketiga *tools* yang sudah siapkan. Hasil dari 3 *tools* yang didapat adalah sebagai berikut.

FotoForensics

Percobaan dengan *tools* pertama bernama FotoForensics yaitu sebuah *tools online* yang bisa diakses pada http://fotoforensics.com/, pada FotoForensics ini menggunakan teknik *level error analysis* untuk pendeteksiannya. Berikut adalah hasil dari FotoForensics:



(a) (b)

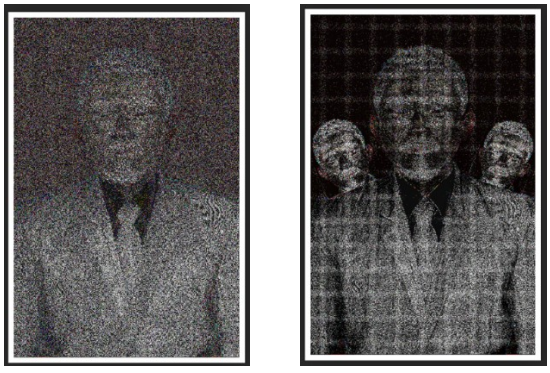
(c) (d)

Gambar 3. Hasil FotoForensics (a) asli (b) *copy-move* (c) *image splicing* (d) *image retouching*

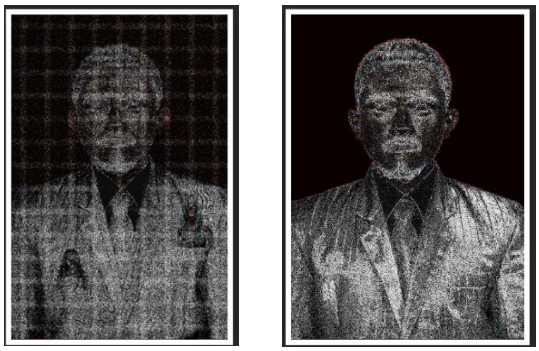
Gambar 3. menunjukan hasil setelah diproses menggunakan FotoForensics menggunakan teknik *error level analysis*, dari keempat foto diatas terlihat jelas perbedaan kontras antara foto asli dengan 3 foto manipulasi lainya terutama untuk manipulasi *image retouching* yang mempunyai perbedaan kontras dibackground serta terdapat garis merah pada tepian objek.

ForensicallyBeta

Percobaan dengan *tools* kedua bernama ForensicallyBeta yaitu sebuah *tools online* yang bisa diakses pada https://29a.ch/photo-forensics, pada ForensicallyBeta ini menggunakan teknik *noise analysis* untuk pendeteksiannya. Berikut adalah hasil dari ForensicallyBeta:



(a) (b)



(c) (d)

Gambar 4. Hasil ForensicallyBeta (a) asli (b) *copy-move* (c) *image splicing* (d) *image retouching*

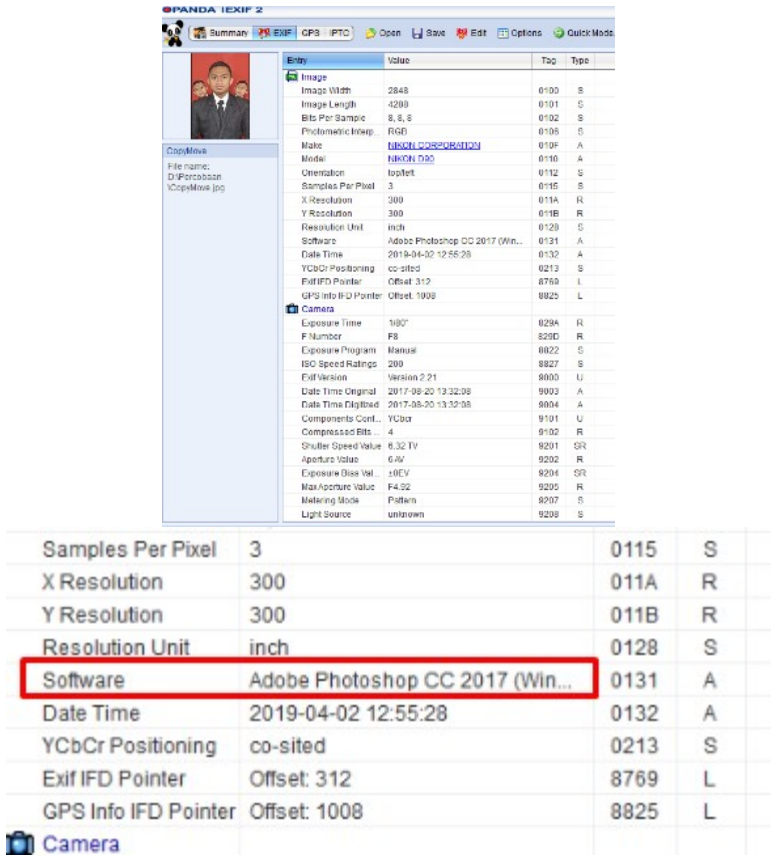
Gambar 4. menunjukan hasil setelah diproses menggunakan ForensicallyBeta menggunakan teknik *noise analysis*, dari keempat foto diatas terdapat perbedaan kontras kembali seperti dengan FotoForensics. Gambar dengan manipulasi *image spilicing* terlihat ada sedikit perbedan kontras ditengah-tengah foto objek, sedangkan untuk gambar *copy-move* dan *image retouching* sangat terlihat jelas perbedaan perbedaan kontrasnya.

Opanda IExif

Percobaan dengan *tools* ketiga bernama Opanda IExif yaitu sebuah *tools offline* yang dapat digunakan untuk mengecek metadata suatu gambar. Proses pendeteksiannya adalah dengan membandingkan masing-masing metadata pada setiap foto. Berikut adalah hasil dari Opanda IExif.

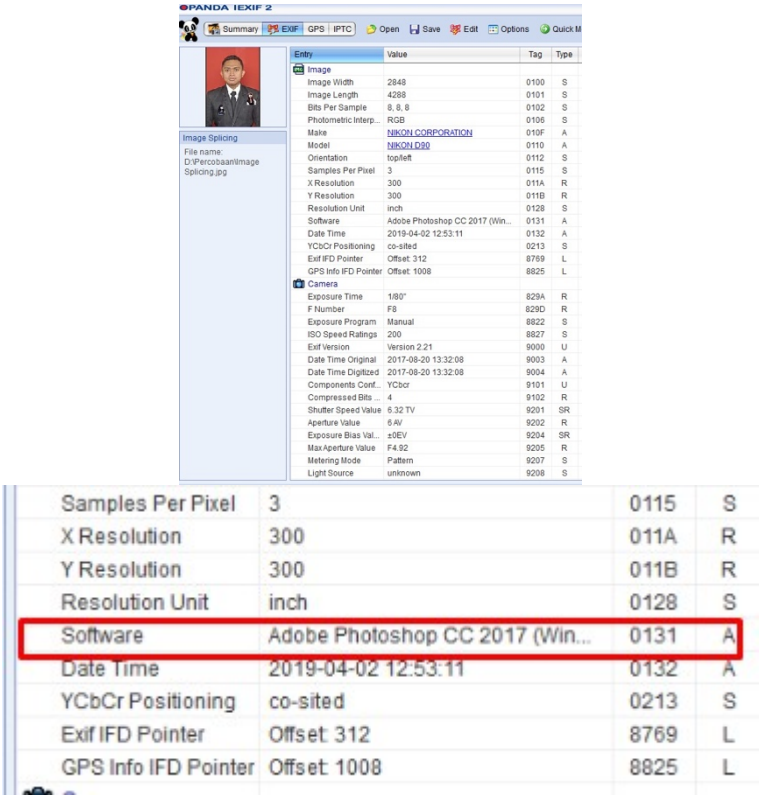
Image			
Make	NIKON CORPORATION	010F	A
Model	NIKON D90	0110	A
Orientation	left/bottom	0112	S
X Resolution	300	011A	R
Y Resolution	300	011B	R
Resolution Unit	inch	0128	S
Software	Ver.1.00	0131	A
Date Time	2017-08-20 13:32:08	0132	A
YCbCr Positioning	co-sited	0213	S
Exif IFD Pointer	Offset: 228	8769	L
GPS Info IFD Pointer	Offset: 32492	8825	L

(a)


PANDA IEXIF 2
Summary
EXIF
GPS
IPTC
Open
Save
Edit
Options
Quick Mode
Entry
Value
Tag
Type
Image
Image Width 2848 0100 S
Image Length 4288 0101 S
Bits Per Sample 8, 8, 8 0102 S
Photometric Interp... RGB 0106 S
Make NIKON CORPORATION 010F A
Model NIKON D90 0110 A
Orientation top/left 0112 S
Samples Per Pixel 3 0115 S
X Resolution 300 011A R
Y Resolution 300 011B R
Resolution Unit inch 0128 S
Software Adobe Photoshop CC 2017 (Win... 0131 A
Date Time 2019-04-02 12:55:28 0132 A
YCbCr Positioning co-sited 0213 S
Exif IFD Pointer Offset: 312 8769 L
GPS Info IFD Pointer Offset: 1008 8825 L
Camera
Exposure Time 1/80" 829A R
F Number F8 829D R
Exposure Program Manual 8822 S
ISO Speed Ratings 200 8827 S
Exif Version Version 2.21 9000 U
Date Time Original 2017-08-20 13:32:08 9003 A
Date Time Digitized 2017-08-20 13:32:08 9004 A
Components Conf... YCbcr 9101 U
Compressed Bits ... 4 9102 R
Shutter Speed Value 6.32 TV 9201 SR
Aperture Value 6 AV 9202 R
Exposure Bias Val... ±0EV 9204 SR
Max Aperture Value F4.92 9205 R
Metering Mode Pattern 9207 S
Light Source unknown 9208 S
CopyMove
File name:
D:\Percobaan
\CopyMove.jpg

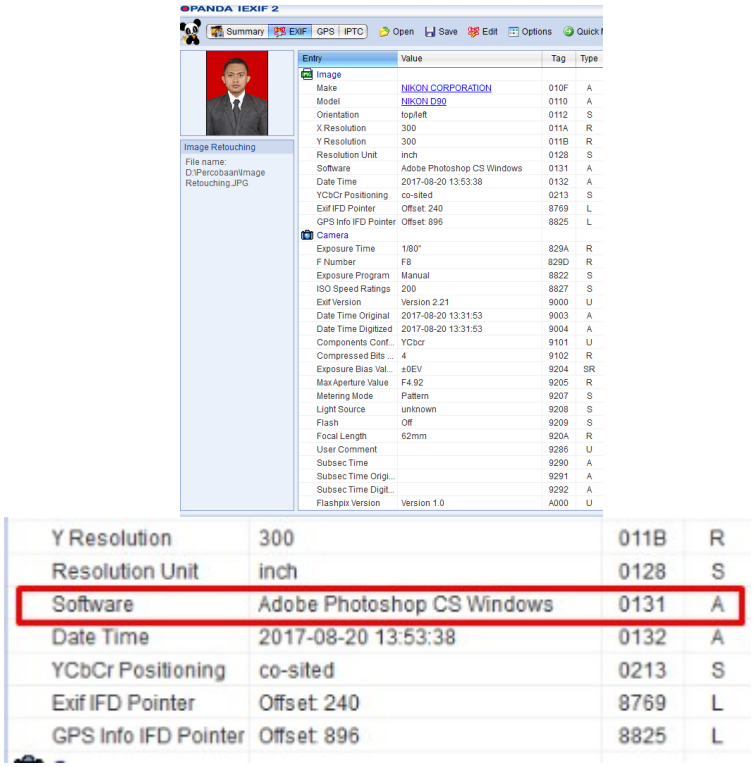
Samples Per Pixel 3 0115 S
X Resolution 300 011A R
Y Resolution 300 011B R
Resolution Unit inch 0128 S
Software Adobe Photoshop CC 2017 (Win... 0131 A
Date Time 2019-04-02 12:55:28 0132 A
YCbCr Positioning co-sited 0213 S
Exif IFD Pointer Offset: 312 8769 L
GPS Info IFD Pointer Offset: 1008 8825 L
Camera

(b)


PANDA IEXIF 2
Summary
EXIF
GPS
IPTC
Open
Save
Edit
Options
Entry
Value
Tag
Type
Image
Image Width 2848 0100 S
Image Length 4288 0101 S
Bits Per Sample 8, 8, 8 0102 S
Photometric Interp... RGB 0106 S
Make NIKON CORPORATION 010F A
Model NIKON D90 0110 A
Orientation top/left 0112 S
Samples Per Pixel 3 0115 S
X Resolution 300 011A R
Y Resolution 300 011B R
Resolution Unit inch 0128 S
Software Adobe Photoshop CC 2017 (Win... 0131 A
Date Time 2019-04-02 12:53:11 0132 A
YCbCr Positioning co-sited 0213 S
Exif IFD Pointer Offset: 312 8769 L
GPS Info IFD Pointer Offset: 1008 8825 L
Camera
Exposure Time 1/80" 829A R
F Number F8 829D R
Exposure Program Manual 8822 S
ISO Speed Ratings 200 8827 S
Exif Version Version 2.21 9000 U
Date Time Original 2017-08-20 13:32:08 9003 A
Date Time Digitized 2017-08-20 13:32:08 9004 A
Components Conf... YCbcr 9101 U
Compressed Bits ... 4 9102 R
Shutter Speed Value 6.32 TV 9201 SR
Aperture Value 6 AV 9202 R
Exposure Bias Val... ±0EV 9204 SR
Max Aperture Value F4.92 9205 R
Metering Mode Pattern 9207 S
Light Source unknown 9208 S
Image Splicing
File name:
D:\Percobaan\Image
Splicing.jpg

Samples Per Pixel 3 0115 S
X Resolution 300 011A R
Y Resolution 300 011B R
Resolution Unit inch 0128 S
Software Adobe Photoshop CC 2017 (Win... 0131 A
Date Time 2019-04-02 12:53:11 0132 A
YCbCr Positioning co-sited 0213 S
Exif IFD Pointer Offset: 312 8769 L
GPS Info IFD Pointer Offset: 1008 8825 L

(c)



(d)

Gambar 5. Hasil Opanda IExif (a) asli (b) *copy-move* (c) *image splicing* (d) *image retouching*.

Gambar 5. menunjukan hasil setelah diproses menggunakan Opanda IExif menggunakan teknik analysis metadata. Keempat gambar diatas sudah menunjukan perbedaan metadata, perbedaan foto asli dengan ketiga foto manipulasi terdapat pada kolom software, yaitu Adobe Photoshop. Hal tersebut menunjukan bahwa ketiga foto tersebut sudah pernah dimanipulasi.

KESIMPULAN

Kesimpulan yang didapat dari penelitian ini adalah *tools* yang sudah digunakan dari ketiga *tools* dapat memberikan hasil pendeteksian. Komparasi ketiga *tools* berhasil dilakukan dengan masing-masing analisis yang sudah berjalan, sehingga didapat hasil pendeteksian foto. Bahan foto yang digunakan masih menggunakan foto asli dan foto manipulasi yang diedit dari foto asli, bukan dari foto yang sudah beredar di media sosial dan internet

Saran untuk penelitian selanjutnya adalah menggunakan foto yang beredar di media sosial dan internet sehingga cukup menggunakan 1 foto sudah bisa mendeteksi kepalsuan foto tersebut. Sehingga diharapkan dapat menggunakan tools dan teknik yang berbeda sehingga dapat mencari perbandingan *tools image forensics* yang terbaik.

DAFTAR PUSTAKA

[1] Agus, A. A., & Riskawati. (2016). Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). Jurnal Supremasi, 11(1), 20–29.

[2] Efendi, M. M. (2018). Metode deteksi tepi block jpeg terkompresi untuk meningkatkan akurasi analisis manipulasi splicing pada citra berekstensi jpeg. Universitas Islam Indonesia.

[3] Fadlil, A., Riadi, I., & Sari, T. (2017). Image Forensic for detecting Splicing Image with Distance Function. 169(5), 6–10.

[4] Febrianda, D. A., Andreswari, D., & Wulandari, E. P. (2018). Sistem Autentifikasi Citra Digital Terintegrasi Dengan Error Level Analysis (Ela) Dan Color Filter Array (Cfa) Berbasis Web. 4(March 2016), 45–56.

[5] Febriyanto, A., & Sembiring, I. (2016). Uji Perbandingan Tools Mobile Forensic Pada Platform Java, Blackberry dan Android. Universitas Kristen Satya Wacana.

[6] Kresnha, P. E., Susilowati, E., & Adharani, Y. (2016). Pendeteksian Manipulasi Citra Berbasis Copy-move Forgery Menggunakan Euclidean DIstance dengan Single Value Decomposition. Seminar Nasional Teknologi Informasi Dan Multimedia 2016, 6–7.

[7] Rosidin. (2018). Analisis Pendeteksi Kecocokan Objek Pada Citra Digital Menggunakan Matlab Dengan Metode Algoritma SIFT. Universitas Islam Indonesia.

[8] Ruci Meiyanti, & Ismaniah. (2015). Perkembangan Digital Forensik. Jurnal Kajian Ilmial UBJ, 15(September 2015).

[9] Sahera, C. (2016). Forensik Gambar dan Video. 1–26. Retrieved from http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23214314- Report.pdf

[10] Saifullah, S., -, S., & Yudhana, A. (2018). Analisis Perbandingan Pengolahan Citra Asli Dan Hasil Croping Untuk Identifikasi Telur. Jurnal Teknik Informatika Dan Sistem Informasi, 2(3). https://doi.org/10.28932/jutisi.v2i3.512

[11] Saputra, A. P., & Widiyasono, N. (2017). Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba). Jurnal Teknik Informatika Dan Sistem Informasi, 3(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

[12] Silalahi, V. A., & Sembiring, I. (2017). Analisis Digital Forensics Investigation Pada Bukti Digital Steganography. Universitas Kristen Satya Wacana.

[13] Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Keaslian Citra Menggunakan Teknik Level Error Analysis Dengan ForensicallyBeta. 2018(November), 154–159.

[14] Wijaya, A. Y., Musayyab, S. Al, & Studiawan, H. (2017). Pengembangan Metode Block Matching Untuk Deteksi Copy-Move Pada Pemalsuan Citra. JUTI: Jurnal Ilmiah Teknologi Informasi, 15(1), 84.

[15] Zam, E. (2015). Image Forensics. Jakarta: Jasakom.

[16] Zulfan, Arnia, F., & Muharar, R. (2018). Deteksi Pemalsuan Citra dengan Teknik Copy-Move Menggunakan Metode Ordinal Measure dari Koefisien Discrete Cosine Transform. Jurnal Nasional Teknik Elektro, 5(2), 165.