JUSTINDO
Jurnal Sistem dan Teknologi Informasi
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO
E-ISSN: 25541-5735, P-ISSN: 2502-5724
Volume 6, No. 2, Agustus 2021

Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist

Muhammad Rizky Al-Fajri[1], Caruddin[2], Dadang Yusup[3]

Universitas Singaperbangsa Karawang
Email: rizki.fajri17021@student.unsika.ac.id

(Naskah masuk: 29 Mei 2021, diterima: 25 Juni 2021, diterbitkan: 30 Agustus 2021)

ABSTRAK

Berkembangnya teknologi menyebabkan sebuah informasi dapat dengan mudahnya menyebar secara luas dan juga cepat. Dampak negatif yang terjadi akibat mudahnya informasi menyebar salah satunya yaitu informasi dapat dengan mudahnya di manipulasi, salah satunya adalah informasi berbentuk foto yang telah di rekayasa atau edit. Untuk mencegah hal tersebut dapat dilakukan analisis ke foto tersebut dengan *image forensic*. Dengan bantuan *tools image forensic* seperti *Jpegsnoop* kita dapat melihat metadata dari foto tersebut sehingga kita dapat dengan mudah mencari tahu sumber foto tersebut, dan dengan *Forensically beta* dapat dilakukan *analysis* dengan metode *Error level analysis* untuk melihat objek yang direkayasa. Dengan menerapkan metode NIST (Nasional Institute of Standart and Technology) dalam tahapannya akan dilakukan simulasi dengan melakukan analysis perbandingan ke pada dua foto yang diantaranya terdapat foto asli dan yang sudah direkayasa. Dari perbandingan yang dilakukan akan diketahui bahwa terdapat perbedaan metadata dan juga error level analysis yang dihasilkan dapat membuktikan bahwa foto tersebut sudah di rekayasa. Hasil dari metadata dapat mengetahui bahwa foto palsu tersebut di rekayasa menggunakan *Photoshop* dan dari hasil error level analysis dapat mengetahui bahwa terdapat objek asing yang di sisipkan ke dalam foto tersebut.

Kata kunci: *Error level analysis, Foto, Image Forensic, Metadata, NIST*

ABSTRACT

The development of technology causes information to spread widely and quickly. The negative impacts that occur due to the ease with which information spreads, one of which is that information can be easily manipulated, one of which is information in the form of photos that have been engineered or edited. To prevent this, an image forensic analysis can be carried out. With the help of image forensic tools such as Jpegsnoop, we can see the metadata of the photo so that we can easily find out the source of the photo, and with Forensically beta analysis can be carried out using the Error level analysis method to see engineered objects. By applying the NIST (National Institute of Standard and Technology) methodology, a simulation will be carried out in stages by performing a comparative analysis of two photos, including original and engineered photos. From the comparisons made, it will be seen that there are differences in the metadata generated and the resulting error level analysis can prove that the photo has been engineered.

Keywords: *Error level analysis, Photos, Image Forensics, Metadata, NIST*

1. PENDAHULUAN

Perkembangan teknologi di era digital ini menyebar secara luas dengan cepat. Dengan perkembangan yang terjadi ini sangat membantu pekerjaan manusia menjadi lebih mudah. Dampak positif yang kita nikmati saat ini perkembangan teknologi juga memiliki dampak negatif, dimana teknologi dapat dimanfaatkan untuk melakukan tindak kejahatan yang disebut cyber crime. Kejahatan cyber crime ini sering sekali terjadi misalnya cracking, hacking, phising, penyebaran pornografi, pelanggaran hak cipta, penipuan online, dan masih banyak lagi kejahatan cyber crime ini.

Penyebaran berita palsu juga merupakan kejahatan cyber crime yang sering terjadi dan salah satunya caranya adalah dengan merekayasa sebuah file foto. Foto yang telah dirakayasa dapat dengan mudahnya tersebar di berbagai media sosial. Penyebaran foto hasil rekayasa yang terjadi dapat membuat kecemasan pada masyarakat dan membuat masyarakat bertanya-tanya tentang kebenaran dari berita tersebut, karena sebuah gambar ataupun video dapat direkayasa dengan mudah. Berbagai macam motif dapat menjadi alasan untuk seseorang melakukan rekayasa foto. Seperti untuk motif politik, agama dan juga motif pribadi untuk memfitnah seseorang, Contoh dalam kasus pornografi sebuah gambar atau video dapat direkayasa dan dimanipulasi menyerupai seseorang sehingga dapat merusak nama dan repustasi orang tersebut. Dan banyaknya software editing yang ada memungkinkan untuk merekayasa sebuah foto/gambar seperti Photoshop, corel draw bahkan paint juga dapat digunakan untuk merekayasa foto.

Sebuah foto dapat di analysis untuk mencari tahu apakah foto tersebut asli atau sudah di rekayasa dengan berbagai macam metode seperti melihat metadata, error level analysis, noise analysis dan lain lain. Dengan menggunakan tools-tools forensics seperti fotoforensic, forensically beta, jpegsnoop, Opanda iexif dan lain-lain dapat digunakan untuk mengidentifikasi keaslian foto. Dan hasil yang di dapat dari tools tersebut dapat dimanfaatkan menjadi barang bukti digital. Bukti digital atau digital evidence merupakan berharga yang dapat di gunakan dalam tahap penyelidikan dan di pengadilan. Berbagai kasus kerjahatan cyber crime dengan menggukanan file foto masih sering terjadi, sehingga forensik terhadap foto atau gambar sebagai kunci utama untuk membantu menangani kasus tersebut.

Forensik digital sendiri ada berbagai macam jenis nya, berdasarkan barang bukti digital forensic dapat dibagi sebagai berikut, mobile forensik, audio forensik, image forensik dan cyber forensik. Pada penelitian ini akan berfokus ke image forensik dimana penelitian ini akan menganalisis barang bukti berbentuk file foto. Dengan menggunakan tools Forensically Beta dan Jpegsnoop, dan sesuai dengan tahapan metodologi NIST, sehingga penelitian ini berjudul “Analisis Digital Image Forensic untuk Deteksi Rekayasa Kasus Pemalsuan File Image dengan Metode NIST”.

2. METODOLOGI PENELITIAN

2.1. Metode NIST

Pada Penelitian ini akan dilakukan simulasi Image Forensic terhadap barang bukti berupa foto yang telah di edit. Tahapan penelitian yang akan dilakukan sesuai dengan metodologi investigasi Digital Forensic National Institute of Standards and Technology (NIST) yang memiliki 4 tahapan, yaitu Collection (Pengumpulan data), Examination (Pemeriksaan), Analysis (analisis), Reporting (Pelaporan) (Isnaini, K. N., Ashari, H., & Kuncoro, A. P. 2020).

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Gambar 1. Tahapan NIST

2.2. Bukti Digital

Ansori Hasibuan menyebutkan bahwa barang bukti merupakan barang yang digunakan oleh pelaku dalam melakukan suatu tindak pidana atau merupakan hasil dari suatu tindakan pidana tersebut, yang akan disita oleh penyidik untuk diselidiki sebagai barang bukti di pengadilan. Sedangkan barang bukti digital dapat diartikan sebagai barang bukti yang di dapat atau diekstrak dari barang elektronik atau hardware seperti, image file, video file, komputer file log, *encrypted file*, *email* dan sebagainya yang didapatkan pada saati dilakukan investiogasi terhadap komputer. Barang bukti digital di dalam Undang-Undang No.11 Tahun 2008 menyebutkan bahwa barang bukti digital dikenal sebagai informasi elektronik dan dokumen elektronik.

2.3. *Digital Forensics*

Digital forensic memiliki cakupan yang cukup luas yang dapat dibagi lagi menjadi beberapa jenis, seperti *Mobile Forensic, System Forensic, Disk Forensic, Image Forensic, dan Network Forensic* (Ruci Meiyanti & Ismaniah, 2015). Menurut Febryanto dan Sembiring *Digital forensic* merupakan suatu keahlian khusus untuk mengumpulkan barang bukti secara digital untuk disampaikan dalam suatu pengadilan sesuai dengan hukum (Riadi, Yudhana & Sulistyo, 2019). *Digital Forensic* merupakan cabang ilmu di bidang komputer yang pembahasannya berpusat pada pengembangan barang bukti yang berbentuk file digital yang akan digunakan di dalam pengadilan perdata maupun pidana (Irwansyah, 2019).

2.4. Image Forensics

Image Forensic merupakan suatu metode ilmiah di bidang penelitian untuk memperoleh fakta-fakta yang menjadi barang bukti bahwa foto tersebut merupakan asli atau tidak (Sulistyo, Riadi, & Yudhana, 2018). Berbagai kasus kejahatan dengan memanfaatkan media foto ini masaih sering kali terjadi di kehidupan kita, maka dari itu image forensic berperan penting dalam membantu pengadilan dalam mengambil keputusan. Untuk menyelidiki keaslian file foto, merupakan bagian dari dalam teknik fotografi forensik, yang digunakan untuk menyelidiki suatu barang bukti, yang berbentuk file foto yang merupakan salah satu barang bukti yang dapat diajukan ke persidangan, apabila barang bukti file foto ini sesuai dengan standar ketentuan yang ditetapkan oleh hukum yang berlaku, dan juga bisa dimanfaatkan sebagai dokumentasi, analisis intelijen.

2.5. Metadata

Metadata dapat diartikan sebagai deskripsi mendasar tentang suatu data. metadata merupakan informasi yang dapat mendeskripsikan data yang tertanam dalam suatu data, seperti konten halaman website, dokumen, atau file. Pada file berbentuk foto terdapat EXIF metadata atau Exchangeable Image File merupakan data yang memiliki informasi penting pada sebuah foto (Apriliani, A., Hijjayanti, K., & Suhairoh. 2020). Metadata pada file foto biasanya berisi tentang

informasi tanggal dan jam diambilnya foto, kamera atau handphone yang digunakan untuk mengambil foto, dan informasi exposure lainnya.

2.6. *Error Level Analysis* (ELA)

Error Level Analysis (ELA) merupakan salah satu metode *Image forensic* untuk mengidentifikasi unsur-unsur dari file foto dengan tingkat yang berbeda dari kompresi (Djaksana, Y. M., & Rivai, A. K. 2018). Dengan menggunakan teknik ini kita dapat mengetahui bahwa gambar tersebut telah dimanipulasi secara digital dengan melihat objek yang memiliki tekstur, garis tepi, dan warna yang berbeda dari objek yang lain. Maka apabila terdapat objek tersebut maka dapat disimpulkan bahwa objek tersebut merupakan rekayasa. Error Level Analysis adalah teknik yang dapat membantu mengidentifikasi manipulasi ke gambar terkompresi (JPEG) dengan mendeteksi distribusi kesalahan yang diperkenalkan setelah mengembalikan gambar pada tingkat kompresi tertentu

3. HASIL DAN PEMBAHASAN

3.1. Collection

Pada tahapan ini akan dilakukan pengumpulan barang bukti yang merupakan foto hasil rekayasa dan juga foto asli tersebut. Barang bukti tersebut akan diperiksa agar dapat diketahui keasliannya.

Gambar 2. Foto Asli

Gambar 3. Foto Rekayasa

3.2. Examination

Pada tahapan Examination ini akan dilakukan pemeriksaan pada foto tersebut dengan melihat metadata dari kedua foto yang menjadi barang bukti pada penelitian kali ini. Dengan dibantu salah satu tools forensic yaitu Jpegsnoop akan dilakukan penyelidikan terkait metadata. Dari penyelidikan metadata yang dilakukan akan diketahui asal dari foto tersebut. Berikut ini merupakan Metadata dari kedua foto yang digunakan untuk simulasi.

```
EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000D
  [Make                          ] = "vivo"
  [Orientation                   ] = 0
  [DateTime                      ] = "2020:02:29 08:41:48"
  [GPSOffset                     ] = @ 0x0312
  [YResolution                   ] = 72/1
  [XResolution                   ] = 72/1
  [Model                         ] = "vivo 1807"
  [Software                      ] = "msm8937_64-user 8.1.0 OPM1.17
  [YCbCrPositioning              ] = Centered
  [ExifOffset                    ] = @ 0x012B
  [ResolutionUnit                ] = Inch
  Offset to Next IFD = 0x000003FD
```

Gambar 4. Hasil Jpegsnoop Foto Asli

```
*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000002
  Length          = 2384
  Identifier      = [http://ns.adobe.com/xap/1.0/]
    XMP =

*** Marker: APP13 (xFFED) ***
  OFFSET: 0x00000954
  Length          = 44
  Identifier      = [Photoshop 3.0]
      8BIM: [0x0425] Name="" Len=[0x0010] DefinedName="Caption digest"
        Caption digest                                =  | 0xD4 1
```

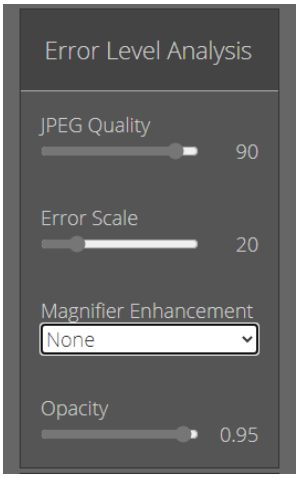
Gambar 5. Hasil Jpegsnoop Foto Rekayasa

Berdasarkan Metadata yang di dapat kita sudah dapat melihat asal dari kedua foto tersebut yang dimana pada foto asli di dapatkan dari *handphone* Vivo sedangkan pada foto hasil rekayasa telah di edit dengan menggunakan aplikasi editing photoshop.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

3.3. Analysis

Pada tahap *analysis* ini akan menggunakan metode *Error level analysis* (ELA) dengan menggunakan bantuan *tools Forensically beta.* pada *error level analysis* di *forensically beta* memiliki beberapa indicator untuk di atur yaitu kualitas Jpeg, *error scale, opacity,* dan *magnifier enchancement*.



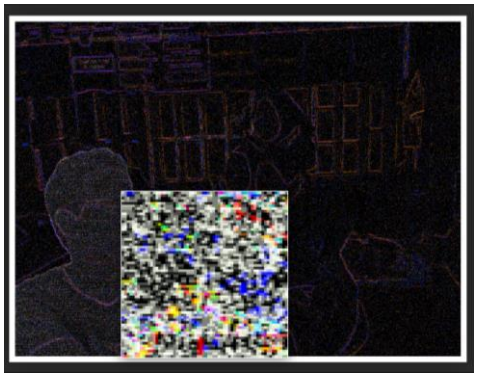
Gambar 6. Indikator *Error Level Analysis*

Indicator yang akan digunakan pada kali ini adalah 95 *jpeg quality,* 50 *error scale dan* 0.95 opacity pada kedua foto dan mendapatkan hasil seperti berikut.

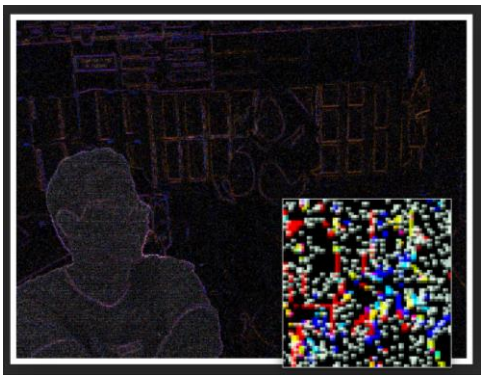
Gambar 7. Hasil ELA Foto Asli

Gambar 8. Hasil ELA Foto Rekayasa

Pada foto rekayasa ada objek yang memiliki tingkat error yang berbeda yaitu pada bagian kiri bawah. Pada objek tersebut memiliki warna, garis tepi dan tekstur yang berbeda dari pada yang lain nya. Untuk memperjelas teksturnya dapat dilakukan *zooming* pada bagian tersebut.



Gambar 9. Tekstur Pada Objek



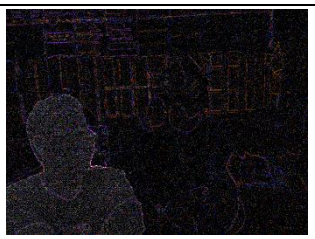
Gambar 10. Tekstur Pada Daerah Lainnya

Dengan melihat tiga aspek tadi yaitu warna, garis tepi dan tekstur pada objek yg direkayasa memiliki perbedaan pada daerah lainnya kita dapat mengetahui bahwa foto tersebut merupakan foto rekayasa.

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 *Jpegsnoop* dan *Forensically beta* ditampilkan dalam bentuk table sebagai berikut

Tabel 1. Hasil Report Simulasi

	Barang Bukti	Metadata	*Error Level Analysis*	status
Foto asli		Taken by Vivo		Asli
Foto rekayasa		Edited by Photoshop		Terbukti Rekayasa

Dari hasil *report* simulasi kita dapat mengetahui perbedaan antara foto asli dan foto palsu dengan melihat metadata dan juga perbedaan error level analysis. Pada foto asli metadata foto tersebut diambil dari kamera hp vivo dan pada foto palsu merupakan hasil rekayasa dari *Photoshop*. Dan dengan Error level analysis pada foto palsu terlihat adanya objek asing. Hasil tersebut dapat digunakan sebagai barang bukti digital.

Gambar 11. Hasil Error Level Analysis Foto Rekayasa

4. KESIMPULAN DAN SARAN

Dari dua foto yang dijadikan barang bukti ditemukan bahwa salah satu dari kedua foto tersebut merupakan hasil rekayasa. Dari kedua foto tersebut dilakukan scan dengan Jpegsnoop dan didapatkan metadata dari kedua foto tersebut. Setelah diketahui metadata dari kedua foto tersebut dilanjutkan dengan analisis tingkat error atau error level analysis dengan menggunakan tools bantuan yaitu Forensically beta. Dengan error level analysis dapat diketahui daerah mana yang di rekayasa atau diedit dari foto tersebut, karena pada error level analysis apabila ada daerah yang berbeda dari yang lain seperti tekstur, garis tepi, dan warnanya itu terjadi karena adanya level kompresi yang berbeda. Setelah dilakukan analisis pada foto kedua terdapat ketiga perbedaan tersebut pada bagian kiri bawah tepatnya di bagian wajah pria itu.

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Saran bagi penelitian selanjutnya yang berkaitan dengan image forensik ini dapat menggunakan metode analisis lainnya seperti noise analysis, clone detection dan masih banyak lagi. Dan juga tools atau aplikasi yang digunakan, dapat mencoba dengan tools lain selain Forensically beta dan Jpegsnoop yang dapat melakukan proses analisis lebih baik lagi untuk penelitian selanjutnya .

5. DAFTAR PUSTAKA

Apriliani, A., Hijjayanti, K., & Suhairoh. (2020). Analisis Keaslian Citra Dengan Menggunakan Exif Metadata. CESS (Journal of Computer Engineering System and Science), 84-88.

Djaksana, Y. M., & Rivai, A. K. (2018). Analisis Manipulasi Citra (Image Forgery) Menggunakan Integrasi Metode Error Level Analysis dan Block Matching. Jurnal Teknologi Informasi ESIT, 83-89.

Irwansyah; Yudiastuti, Helda. (2019). Analisis Digital Forensik Rekayasa Image Menggunakan Jpegsnoop dan Forensically beta . Jurnal Ilmiah MATRIK, 54-63.

Isnaini, K. N., Ashari, H., & Kuncoro, A. P. (2020). Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST. Jurnal Resistor, 72-81.

Riadi, Imam; Yudhana, Anton; Sulistyo; Wicaksono Yuli. (2019). Deteksi Pemalsuan Foto Digital Menggunakan Image Forensics. Jurnal Mobile and Forensics, 13-21.

Sari, T., Riadi, I., & Fadlil, A. (2016). Forensik Citra Untuk Deteksi Rekayasa File Menggunakan Error Level Analysis. Annual Research Seminar, 133-138.

Sulistyo, W. Y., & Riadi, I. Y. (2018). Analisis Deteksi Keaslian Citra Menggunakan Teknik Error Level Analysis Dengan Forensically beta. Seminar Nasional Informatika, 154-159.

Sulistyo, W. Y., Riadi, I., & Yudhana, A. (2020). Penerapan Teknik SURF pada Forensik Citra Untuk Analisis Rekayasa Foto Digital. Jurnal Informatika, 179-186.

Putra, A. I., Umar, R., & Fadlil, A. (2018). Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool. Seminar Nasional Informatika, 21-25.

Meiyanti, Ruci., Ismaniah. (2015) Perkembangan Digital Forensik Saat Ini dan Mendatang.Jurnal Kajian Ilmiah UBJ.