

PERBANDINGAN HASIL ANALISA FOTO HOAX MENGGUNAKAN METODE EXIF/METADATA, REVERSE IMAGE DAN FORENSICS

Moh. Subli*¹, Muhamad Masjun Efendi², Salman³

¹²³Universitas Teknologi Mataram; Jl. Kampus UTM Kekalik Mataram, 0370628418
e-mail: *¹subli.kerta@gmail.com, ²creativepio@gmail.com, ³asal.lombok@gmail.com

Abstrak

Informasi hoax yang tersebar selama ini banyak berupa foto-foto yang sudah diedit dan dimanipulasi dari foto-foto yang sebenarnya, kemudian foto-foto tersebut menyebar secara luas di internet. Perkembangan foto yang semakin maju membuatnya memiliki banyak keunggulan untuk dijadikan berita hoax seperti mudahnya dimanipulasi, mudahnya disebar secara massif dan luas serta mudah sekali membuat orang cepat percaya. Perubahan foto yang mudah dimanipulasi dapat merubah informasi yang disampaikan menjadi berbeda dan membuatnya rawan digunakan untuk tindak kejahatan. Dengan banyak foto-foto yang dijadikan sebagai sarana tindak kejahatan maka perlu dilakukan sebuah penelitian yang bisa dijadikan sebagai pedoman untuk bisa melihat foto mana yang asli dan yang palsu dengan menggunakan sebuah metode. Banyak sekali beredar sebuah metode yang bisa melihat keaslian dan kepalsuan foto tersebut. Namun dari banyak yang beredar, tidak jarang yang memiliki tingkat pengujian yang tidak mendekati kebenaran, karena kelayakan dan tingkat kebenaran dari metode tersebut masih belum bisa dipercaya. Untuk itu didalam penelitian ini dibandingkan hasil analisa foto hoax dengan menggunakan metode exif/metadata, reverse image dan image forensics. Ketiga metode ini akan dijadikan contoh mana yang lebih mendekati kebenaran yang kemudian bisa dijadikan pedoman atau rujukan oleh orang-orang untuk membuktikan keaslian sebuah foto atau informasi yang sedang menyebar luas ditengah-tengah masyarakat.

Kata kunci— Informasi/Foto Hoax, Exif/Metadata, Reverse Image, Image Forensics.

Abstract

The hoax information that has been spread so far is in the form of photos that have been edited and manipulated from actual photos, then the photos are spread widely on the internet. The development of increasingly advanced photos makes it have many advantages to be used as hoax news, such as easy to manipulate, easy to spread massively and widely and easy to make people believe quickly. Changes in photos that are easily manipulated can change the information submitted to be different and make them vulnerable to being used for crime. With many photos that are used as a means of crime, it is necessary to do a study that can be used as a guide to be able to see which photos are real and which are fake by using a method. There are so many circulating methods that can see the authenticity and fakeness of the photo. However, from many in circulation, it is not uncommon to have a level of testing that is not close to the truth, because the feasibility and level of truth of the method still cannot be trusted. For this reason, in this study, the results of the analysis of hoax photos are compared using the exif/metadata, reverse image and image forensics methods. These three methods will be used as examples of which one is closer to the truth which can then be used as a guide or reference by people to prove the authenticity of a photo or information that is being spread widely in the community.

Keywords— Hoax Information/Photos, Exif/Metadata, Reverse Image, Image Forensics.

1. PENDAHULUAN

Indonesia setiap lima tahun sekali selalu menyelenggarakan pesta demokrasi yaitu PEMILU, PILEG dan PILKADA. Pesta demokrasi yang diselenggarakan lima tahun sekali ini akan memilih wakil-wakil rakyat yang akan duduk di kursi parlemen mulai dari tingkat daerah sampai tingkat pusat. Pemilu tahun 2019 misalnya menghadapi permasalahan yaitu gelombang hoax. Hoax muncul bertubi-tubi dalam berbagai konteks persebaran informasi, tidak hanya politik saja, tetapi dibidang lain seperti agama, suku, ras, ekonomi, pendidikan, kesehatan, sampai dari urusan publik hingga privat seseorang [1].

Dunia internet kini dipenuhi banyak sekali informasi hoax, provokasi, fitnah, sikap intoleran dan anti agama. Kemajuan teknologi di era globalisasi membuat informasi begitu cepat beredar luas. Keberadaan internet sebagai media online membuat informasi yang belum terverifikasi benar dan tidaknya tersebar begitu cepat. Hanya dalam hitungan detik, suatu peristiwa sudah bisa langsung tersebar dan diakses oleh pengguna internet lainnya yang berada jauh. Melalui internet, ratusan bahkan ribuan informasi disebar setiap harinya. Bahkan orang kadang belum sempat memahami materi informasi, reaksi atas informasi tersebut sudah lebih dulu terlihat.

Berdasarkan hasil penelitian Mastel [2], jenis hoax yang paling sering diterima masyarakat adalah bidang sosial politik (Pilkada, pemerintah) dan masalah SARA. Kementerian Komunikasi dan Informatika (Kemenkominfo) mendata ada 1.000 berita hoax yang disebar dari awal masa kampanye sampai sekarang. Berita hoax itu menyerang kedua pasangan calon presiden dan calon wakil presiden. “Menurut mesin scrolling kami, ada 1.000 lebih konten hoax yang berkaitan dengan konten politik dan beberapa instrumen pendukungnya, terkait partai, kampanye menjelang pilpres dan pileg ini,” ucap Plt Kabiro Humas Kemenkominfo, Ferdinandus Setu, di Ibis Budget Hotel, Jalan Cikini Raya, Jakarta Pusat, Jumat (19/10/2018).

Diantara konten-konten penyebaran informasi hoax yang tersebar selama ini banyak berupa foto-foto yang sudah diedit dan dimanipulasi dari foto-foto yang sebenarnya, kemudian foto-foto tersebut menyebar secara berantai di dunia elektronik lewat situs-situs internet dan media sosial. Dengan banyak foto-foto yang dijadikan sebagai sarana tindak kejahatan maka perlu dilakukan sebuah penelitian yang bisa dijadikan sebagai pedoman untuk bisa melihat foto mana yang asli dan yang palsu dengan menggunakan sebuah metode. Banyak sekali beredar sebuah metode yang bisa melihat keaslian dan kepalsuan foto tersebut. Namun dari banyak yang beredar, tidak jarang yang memiliki tingkat pengujian yang tidak mendekati kebenaran, karena kelayakan dan tingkat kebenaran dari metode tersebut masih belum bisa dipercaya. Sehingga fokus dari pada penelitian ini, bagaimana ketepatan hasil analisa informasi hoax yang berupa foto tersebut dengan menggunakan metode exif/metadata, reverse image dan image forensics.

Penelitian yang dilakukan [3] bahwa kebhinnekaan sebagai pengikat sosial diuji karena kecenderungan praktik ujaran kebencian yang dipromosikan melalui media sosial. Kondisi itu diperparah oleh penyalahgunaan media sosial seperti persebaran berita bohong atau informasi palsu (hoax) yang dampaknya menimbulkan permusuhan dan tidak sesuai dengan budaya bangsa Indonesia yang mengutamakan toleransi.

Keberadaan internet sepaket dengan kebudayaan yang terbangun di dalam ruang publik baru membuat masyarakat sulit membedakan informasi faktual dan hoax. Jalan utama untuk mengantisipasi hoax adalah membangun kompetensi publik dalam menghadapi luapan banjir informasi. Upaya membangun kompetensi publik dilakukan melalui literasi media [4].

Dalam penelitiannya [5] mengatakan Media online/internet mempunyai peranan penting yang terletak pada kemampuannya untuk menyajikan berita-berita tentang perkembangan masyarakat yang bisa mempengaruhi kehidupan modern pada saat ini. Oleh karena individu diyakini sangat terpengaruh oleh pesan-pesan media mengingat media dianggap sangat kuat dalam membentuk opini masyarakat.

Saat ini penyebaran informasi/berita bohong (hoax) makin marak. Survei Mastel 2017 mengungkapkan bahwa masyarakat menerima hoax setiap hari lebih dari satu kali. Saluran yang paling banyak digunakan dalam penyebaran hoax adalah media sosial. Fenomena hoax di

Indonesia menimbulkan keraguan terhadap informasi yang diterima dan mebingungkan masyarakat. Hal ini dimanfaatkan pihak yang tidak bertanggung jawab untuk menanamkan fitnah dan kebencian. Karena itu, penelitian ini bertujuan untuk mendapatkan gambaran tentang interaksi komunikasi hoax di media sosial dan cara mengantisipasinya [6].

Bahkan didalam pengambilan keputusan untuk pengembangan jiwa kewirausahaan mensyaratkan adanya kemampuan untuk mengambil keputusan dalam menghadapi berbagai resiko. Dimana dalam mengambil keputusan sangat dibutuhkan informasi dan kemampuan mendapatkan informasi yang tepat. Salah satu sumber informasi adalah media social dan lagi trend saat ini. Namun persoalan adanya kecenderungan masih lemahnya kemampuan menyaring berita menyebabkan perlunya adanya solusi untuk mengatasi masalah tersebut. Menilai kemampuan menilai kebenaran sebuah berita dari mahasiswa sangat berguna dalam menilai jiwa kewirausahaan mahasiswa dalam mengambil keputusan berwirausaha bahwa kemampuan menilai sebuah berita dapat dilihat dari: penilaian judul, penilaian situs, kontens, foto dan sumber berita [7].

Perkembangan software pengolahan gambar sangat banyak dan bermacam-macam, dengan tersedianya beberapa program aplikasi yang ada mampu dapat merubah dan memodifikasi gambar asli menjadi gambar yang telah diubah bahkan gambar asli dan gambar termodifikasi nyaris tidak dapat dibedakan. Perubahan modifikasi tersebut dilakukan untuk tujuan mempercantik tampilan gambar, atau memperbaiki kualitas gambar agar lebih baik hasilnya. Pada kenyataannya memodifikasi gambar adapula dengan tujuan yang tidak baik. Memodifikasi dengan tujuan untuk menyamarkan data aslinya, atau membuat modifikasi gambar untuk kepentingan menyudutkan seseorang dengan gambar-gambar yang tidak layak, diubah bentuk dan terlebih-lebih banyak gambar artis yang dimodifikasi untuk kepentingan tertentu [8].

Pertumbuhan pesat manipulasi citra digital telah mendorong para penulis di forensik gambar untuk mengungkapkan keasliannya. Manipulasi adalah biasanya ditemukan dalam format gambar seperti Joint Photographic Kelompok Pakar (JPEG). JPEG adalah format yang paling umum didukung oleh perangkat dan aplikasi [9].

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 [10].

Ada 3 jenis tools atau metode yang digunakan: Exif/Metadata, Reverse Image dan Image Forensics.

1.1 Exif/Metadata

ExifTool adalah perpustakaan Perl platform-independen ditambah aplikasi baris perintah untuk membaca, menulis dan mengedit informasi meta dalam berbagai macam file. ExifTool mendukung banyak format metadata yang berbeda termasuk EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, Profil ICC, Photoshop IRB, FlashPix, ACP dan ID3, Lyrics3, serta catatan pembuat banyak kamera digital oleh Canon, Casio, DJI, FLIR, FujiFilm, GE, GoPro, HP, JVC/Victor, Kodak, Leaf, Minolta/Konica-Minolta, Motorola, Nikon, Nintendo, Olympus/Epson, Panasonic/Leica, Pentax/Asahi, Fase Satu, Reconyx, Ricoh, Samsung, Sanyo, Sigma/Foveon dan Sony.[11]

Exiftool ini sendiri bisa digunakan untuk membaca, menulis dan mengedit informasi metadata file, khususnya file foto. Untuk bisa menggunakan tools ini bisa akses dan download toolsnya secara free di website <https://exiftool.org/>.

Teknik pengamanan data dan informasi merupakan salah satu cara untuk menjaga kerahasiaan suatu obyek. eXchangable Image File Format (EXIF) Metadata adalah informasi data tentang citra digital. Dalam penyelidikan forensik digital, ini sangat berguna untuk keamanan hak cipta atau pengamanan bukti digital [12].

1.2 Reverse Image

Reverse image adalah salah satu teknik yang berhubungan dengan banyak teknik baru lainnya seperti menangani pengetahuan tersembunyi menggunakan ekstraksi, asosiasi data, menemukan pola tambahan [13].

Pengambilan foto pada internet/media sosial sangat menarik dan disebarluaskan lagi, sehingga banyak orang yang tidak mengetahui siapa pemilik asli dari foto tersebut. Seperti untuk apa foto itu dibuat dan digunakan untuk kebutuhan apa saja, orang-orang hanya menyebarkan tanpa punya kepentingan yang jelas dan tanpa mengetahui resiko dari penyebaran foto tersebut. Padahal kalau diselidiki lebih dalam lagi, foto itu sudah ada atau belum ada yang tersebar di dunia internet / media sosial dan informasi apa saja yang terkandung didalamnya, bisa menggunakan salah satu metode ini. Salah satu tools yang digunakan pada metode Reverse Image ini adalah menggunakan Google Images.

Google images adalah layanan pencarian yang dibuat oleh Google dan diperkenalkan pada bulan Juli 2001. Layanan ini memungkinkan pengguna mencari konten gambar di web. Kata kunci pencarian gambar didasarkan pada nama berkas gambar, teks tautan yang mengacu ke gambar, dan teks di dekat gambar. [13]

Untuk menggunakan tools ini silahkan akses websitenya di <https://images.google.com/> dan masuk pada menu upload gambar.

1.3 Image Forensics

Bidang ilmu forensik citra digital akan membantu para penegak hukum, intelijen, investigasi swasta 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 [14].

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 bisa 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. [15]

Salah satu cara yang valid digunakan untuk mengecek keaslian foto itu bisa digunakan dengan menggunakan image forensic. Metode image forensic merupakan salah satu cara dalam pemeriksaan bukti digital yang digunakan didalam sebuah persidangan. Pemeriksaan hasil image forensics bisa digunakan sebagai barang bukti yang berhubungan dengan bukti digital dan ini diakui oleh persidangan.

Meskipun ada banyak alat untuk melakukan investigasi forensik pada gambar, mereka tidak memiliki fitur dan umumnya bermasalah. Situs ini dimaksudkan untuk mengatasi masalah ini dan menawarkan layanan yang stabil dan andal untuk penyelidik forensik dan profesional keamanan. [16]

Untuk menggunakan tools ini silahkan akses websitenya di <https://www.imageforensic.org/> dan silahkan browse gambar yang ingin di analisa.

Beberapa penelitian yang pernah dilakukan sebelumnya yang berkaitan dengan hasil analisa foto hoax menjadi referensi dalam penulisan penelitian ini diantaranya;

Riadi, dkk [17] melakukan penelitian dengan judul “Image Forensic for detecting Splicing Image with Distance Function”. Mengungkapkan untuk menganalisis pengukuran kesamaan gambar forensik menggunakan metode distance function, sedangkan untuk manipulasi gambar digunakan specially on image splicing. Hasil penelitian ini menunjukkan distance function tersebut dapat berupa 2 gambar yang berbeda.

Ami D, dkk [18] melakukan penelitian dengan judul “Reverse Image Search Image retrieval using various techniques”. Teknik ini berhubungan dengan banyak teknik baru lainnya seperti menangani pengetahuan tersembunyi menggunakan ekstraksi, asosiasi data, menemukan

pola tambahan. Disini kita memberikan gambaran umum tentang teknik Image Mining yang muncul dengan berbagai teknik deteksi gambar.

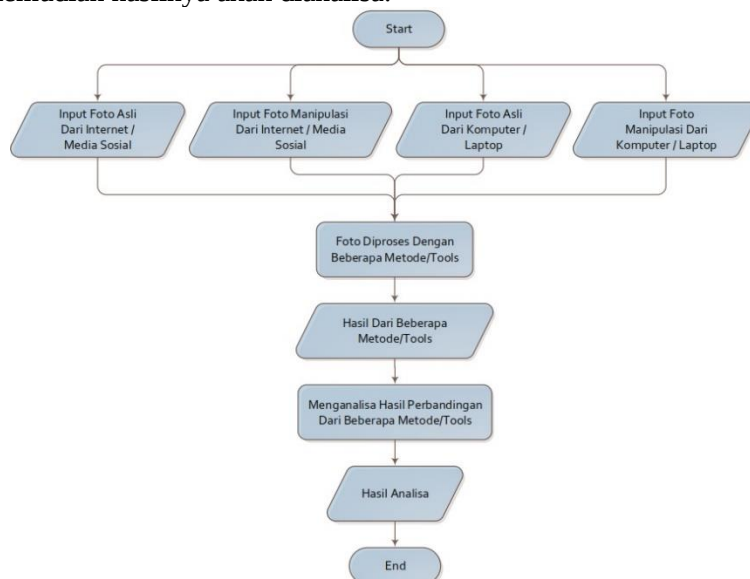
Imanda Putra, dkk [19] melakukan penelitian dengan judul “Analisis Forensik Deteksi Keaslian Metadata Video Menggunakan Exiftool”. Dalam penelitian ini penulis akan menguji menganalisa metadata pada keaslian video dengan menggunakan exiftool. Hasil dari penelitian ini diharapkan dapat menunjukkan informasi perbandingan metadata yang baik.

Riadi, dkk [20] melakukan penelitian dengan judul “Deteksi Pemalsuan Foto Digital Menggunakan Image Forensics”. 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 menunjukkan adanya perubahan pada foto tersebut.

Dari beberapa penelitian sebelumnya, pada penelitian ini akan mengusulkan inovasi dan solusi yang terbaru yaitu terletak pada penggunaan banyak metode untuk penentuan keaslian sebuah informasi yang berupa foto. Penelitian ini di fokuskan untuk mempermudah orang-orang dalam menganalisa sebuah informasi tersebar secara cepat dan tepat yang dapat membantu penekanan penyebaran sebuah informasi hoax.

2. METODE PENELITIAN

Adapun tahapan metode penelitian ini menggunakan sebuah pembuatan metode sendiri untuk melakukan pendeteksian yang digunakan untuk menganalisa foto hoax. Skenario yang dibuat yaitu dengan mengambil sebuah foto di internet atau media sosial dan menyiapkan dua buah foto yang asli dan yang sudah dirubah, setelah itu dimasukan kedalam metode/tools untuk diproses yang kemudian hasilnya akan dianalisa.



Gambar 1. *Flowchart* Menganalisa Hasil Foto

Berdasarkan gambar 1 *flowchart* alur proses menganalisa hasil foto diatas yang akan dibangun secara garis besar terbagi menjadi beberapa tahapan berikut:

2.1 File Foto

Beberapa file foto yang akan dijadikan sampel yaitu foto-foto yang tersebar di internet / media sosial dan file foto yang tersimpan pada computer / laptop. Foto yang diambil yang akan dibuat percobaan ini terdiri dari dua jenis yaitu foto asli dan foto yang sudah dimanipulasi

2.2 Metode/Tools

Jenis metode/tools yang akan digunakan ada tiga jenis yaitu exif/metadata, reverse image dan image forensics. Pertama menggunakan Metode Exif/Metadata yaitu melihat rekaman aktivitas foto. Jika foto itu asli, dari camera smartphone atau DSLR, maka akan ada informasi merk camera, pemakaian ISO, focal length, flash, dan lain-lainnya. Jika geotag diaktifkan, bisa diketahui juga di mana foto tersebut diambil, asalkan belum diedit. Kedua menggunakan Metode Reverse Image berarti melacak balik, mencocokkan sebuah foto dengan foto yang sudah ada di website dan media sosial. Mencocokkan sebuah foto dengan foto yang sudah ada dan pernah diunggah di internet, bisa dengan proses upload, bisa pula dari copy-paste URL yang langsung mengarah ke foto yang mau dibandingkan dengan foto yang sudah ada di internet. Selanjutnya yang ketiga menggunakan Metode Image Forensics yaitu merupakan salah satu metode ilmiah pada bidang penelitian yang bertujuan untuk mendapatkan fakta-fakta pembuktian dalam menentukan sebuah keaslian image.

2.3 Hasil

Dari beberapa metode/tools yang sudah di uji cobakan, maka akan muncul hasil prosesnya.

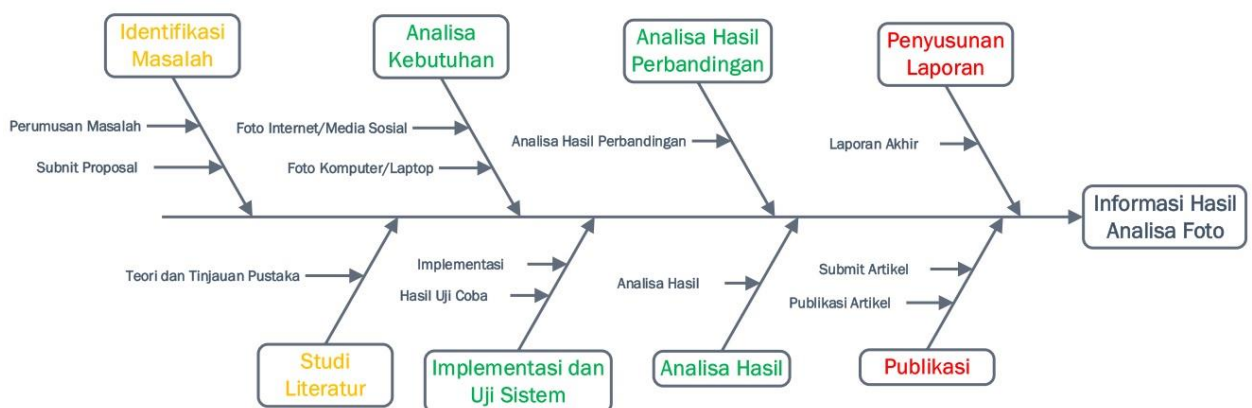
2.4 Analisa Hasil Perbandingan

Hasil-hasil tersebut di analisa untuk mendapatkan sebuah metode/tools yang tepat yang hasilnya mendekati kebenaran.

2.5 Hasil Analisa

Dari hasil analisa tersebut, maka bisa dipastikan sebuah metode/tools yang sudah bisa digunakan secara tepat dan cepat.

Fishbone Diagram Penelitian



Gambar 2. Fishbone Diagram Penelitian

Berikut langkah-langkah penelitian berdasarkan gambar 2 fishbone diagram penelitian diatas:

2.1 Identifikasi Permasalahan

Pada tahapan awal penelitian ini adalah bagaimana merumuskan masalah untuk dijadikan sebagai objek penelitian. Perumusan masalah dilakukan terlebih dahulu melihat situasi di lapangan. Setelah masalah dirumuskan selanjutnya menentukan tujuan penelitian. Tujuan penelitian merupakan sasaran yang ingin di wujudkan dari penyelesaian permasalahan yang diteliti.

2.2 Studi Literatur

Pada tahapan ini mencari sumber-sumber literatur yang berada di internet yang berhubungan dengan informasi hoax, buku-buku teori dan praktek serta tools yang digunakan

dalam penelitian ini, serta dijelaskan mengenai tools yang akan digunakan dalam mendeteksi sebuah informasi hoax yang berupa foto.

2.3 Analisis Kebutuhan

Analisis kebutuhan yaitu berupa bahan-bahan yang akan dibutuhkan untuk menganalisis sebuah *system/tools* yang akan di implementasi dan uji coba. Kebutuhan itu bisa berupa perangkat keras (komputer/laptop), perangkat lunak (aplikasi-aplikasi), file-file foto dan kebutuhan lainnya untuk mendukung penelitian ini.

2.4 Implementasi dan Uji Sistem

Implementasi sistem merupakan proses dimana memastikan sebuah sistem atau tools yang akan diuji bisa menghasilkan kesimpulan dengan baik dan benar. Terdapat banyak metode yang akan di uji cabakan pada tahapan ini.

2.5 Analisa Hasil Perbandingan

Beberapa metode/tools yang sudah di uji cobakan, maka akan muncul hasil prosesnya. Kemudian hasil-hasil tersebut di analisa untuk mendapatkan sebuah metode/tools yang tepat yang hasilnya mendekati kebenaran.

2.6 Analisa Hasil

Kesimpulan dari semua hasil yang sudah didapatkan.

2.7 Penyusunan Laporan

Pada tahapan ini terdapat penyusunan laporan yang memuat semua hasil dari penelitian. Mulai dari latar belakang, tinjauan pustaka, metode penelitian, hasil dan pembahasan sampai pada tahap kesimpulan.

2.8 Publikasi

Pengiriman artikel ilmiah yang akan di publikasi dalam bentuk jurnal.

3. HASIL DAN PEMBAHASAN

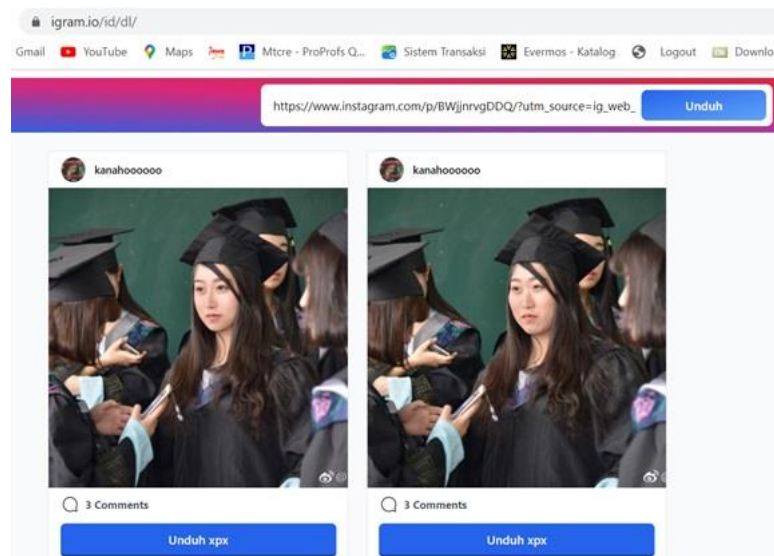
Hasil dan pembahasan dilakukan dalam bentuk implementasi dan uji sistem, dimana proses ini untuk memastikan sebuah sistem atau tools yang akan diuji bisa menghasilkan kesimpulan yang sesuai dengan apa yang akan diharapkan, terutama dalam penelitian ini.

Adapun tahapan implementasi dan uji sistem dilakukan dengan 2 jenis bukti foto yang sudah di persiapkan sebagai sampel dengan masing-masing menggunakan 3 metode yang telah dijelaskan pada pendahuluan dan metode penelitian diatas.

3.1 Bukti Foto dari Internet/Media Sosial

Sebelum melakukan implementasi dan uji sistem, terlebih dahulu mengambil sampel foto yang ada di Internet/Media Sosial. Foto yang diambil ada 2 jenis yaitu foto asli dan foto manipulasi. Kedua foto tersebut akan di uji coba pada tahap implementasi dan uji sistem ini.

Foto diambil dari akun instagram @kanahooooo dengan link url <https://www.instagram.com/p/BWjjnrvgDDQ/> dan di download dengan bantuan link url <https://igram.io/id/dl/> dengan tampilan fotonya seperti gambar berikut:



Gambar 3. Sampel Foto Asli dan Manipulasi

File foto yang sudah di download berikut tampilan *Name*, *Date Modified*, *Type* dan *Size* jika dibuka pada PC/Laptop OS Windows 10.

View			
PC > Downloads			
Name	Date modified	Type	Size
▼ Today (4)			
19985689_116897472268112_9054493905596186624_n.jpg	16/09/2021 13:01	JPG File	787 KB
19985654_489612018045740_4996359537318428672_n.jpg	16/09/2021 13:01	JPG File	797 KB

Gambar 4. Tampilan Informasi Foto dari Media Sosial

Berikut implementasi dan uji sistem bukti foto ini dilakukan dengan menggunakan 3 metode/tools:

1. Metode Tools Exif/Metadata

Tools exif/metadata ini ada yang bisa di implementasi dan ujitobakan secara *offline* dan *online*. Disini digunakan versi *online*, dimana untuk uji coba tools ini harus terkoneksi internet dan internet tidak boleh terputus selama melakukan proses uji coba. Caranya langsung saja akses link url <https://exifmeta.com/> kemudian upload file foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:

EXIF	IPTC	Composite
System.FileName	19985689_116897472268112_9054493905596186624_n.jpg	
System.FileSize	815218	
System.FileModifyDate	2021:09:16 09:03:47+00:00	
System.FileCreateDate	2021:09:16 09:03:47+00:00	
System.FileChangeDate	2021:09:16 09:03:47+00:00	
System.FilePermissions	100644	
FileFileType	JPG	
FileFileTypeExtension	.jpg	
FileMimeType	image/jpeg	
FileMimeTypeOriginal	image/jpeg	
FileImageWidth	1000	
FileImageHeight	1000	
FileImageProcess	2	
FileImageSample	8	
FileImageCompression	2	
FileImageSubsampling	1:1	
JPEGIFVersion	1.1	
JPEGResolutionUnit	0	
JPEGResolution	1	
JPEGResolution	1	
IPTCSystemFileName	19985689_116897472268112_9054493905596186624_n.jpg	
CompositeImageSize	1000 1000	
CompositeImageSize	1.1864	

Gambar 5. Hasil Proses EXIF & Metadata

EXIF	IPTC	Composite
System.FileName	19985689_116897472268112_9054493905596186624_n.jpg	
System.FileSize	815218	
System.FileModifyDate	2021:09:16 09:03:47+00:00	
System.FileCreateDate	2021:09:16 09:03:47+00:00	
System.FileChangeDate	2021:09:16 09:03:47+00:00	
System.FilePermissions	100644	
FileFileType	JPG	
FileFileTypeExtension	.jpg	
FileMimeType	image/jpeg	
FileMimeTypeOriginal	image/jpeg	
FileImageWidth	1000	
FileImageHeight	1000	
FileImageProcess	2	
FileImageSample	8	
FileImageCompression	2	
FileImageSubsampling	1:1	
JPEGIFVersion	1.1	
JPEGResolutionUnit	0	
JPEGResolution	1	
JPEGResolution	1	
IPTCSystemFileName	19985689_116897472268112_9054493905596186624_n.jpg	
CompositeImageSize	1000 1000	
CompositeImageSize	1.1864	

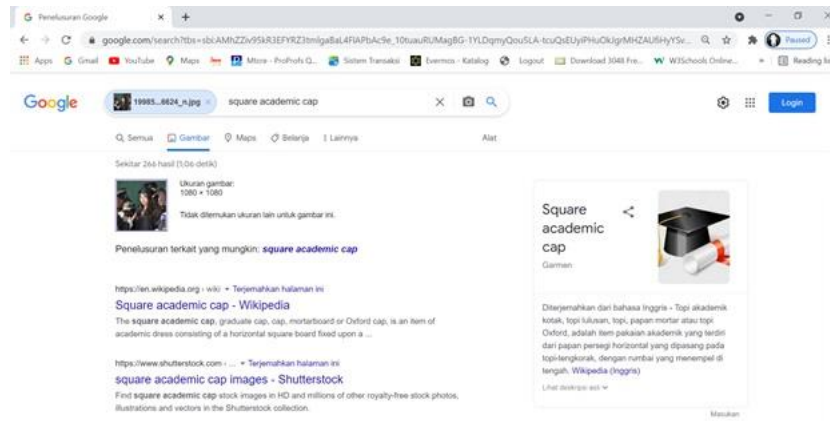
Gambar 6. Hasil Proses EXIF & Metadata

Viewer Foto Asli

Viewer Foto Manipulasi

2. Metode Reverse Image

Metode ini dilakukan dengan mencocokkan dan mencari foto yang sama dari berbagai sumber link/situs yang sudah mempunyai file foto tersebut. Langkah yang dilakukan sama seperti point diatas, untuk uji coba tools ini harus terkoneksi internet dan internet tidak boleh terputus selama melakukan poroses uji coba. Akses link url <https://images.google.com/> kemudian upload file foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:



Gambar 7. Hasil Proses Pengecekan

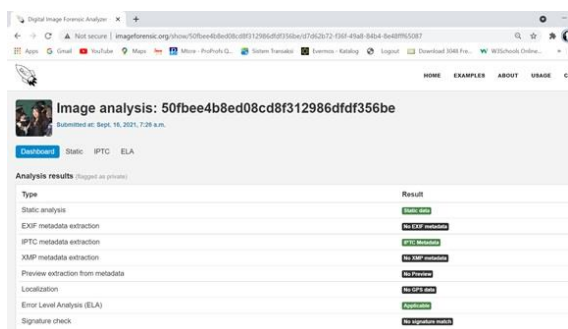
Tampilan yang serupa pada sebuah foto akan ditampilkan pada penulisan mesin pencari google, mulai dari foto-foto yang mempunyai kemiripan sampai situs-situs penyedia foto-foto tersebut. Berikut jika di buka salah satu penyedia situs foto tersebut pada gambar 8 dibawah ini:



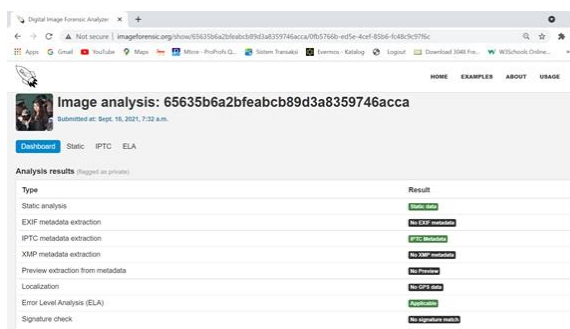
Gambar 8. Situs Penyedia Foto Serupa

3. Metode Image Forensic

Metode ini dilakukan dengan melihat semua informasi metada yang terkandung pada sebuah foto. Langkah yang dilakukan sama seperti point diatas, karena untuk melakukan uji coba metode ini sendiri harus terkoneksi internet dan internet tidak boleh terputus selama melakukan poroses uji coba ini. Langsung akses link url <https://www.imageforensic.org/> kemudian upload file foto yang akan dianalisa dengan tampilan hasil proses pengecekannya seperti gambar berikut:



Gambar 9. Hasil Pengecekan Foto Asli



Gambar 10. Hasil Pengecekan Foto Manipulasi

3.2 Bukti Foto dari Smartphone/Laptop

Sebelum melakukan implementasi dan uji sistem, terlebih dahulu mengambil sampel foto yang ada di Smartphone Infinix Hot 10 kemudian di masukkan kedalam PC/Laptop. Foto yang akan di uji coba pada implementasi ini ada 2 jenis yaitu foto asli dan foto manipulasi dengan menghilangkan salah satu objek (orang) pada foto asli yang sudah di edit dengan Photoshop CC 2017. Tampilan fotonya seperti gambar berikut:



Gambar 11. Foto Asli



Gambar 12. Foto Manipulasi

Implementasi dan uji sistem bukti foto ini dilakukan sama dengan menggunakan 3 metode/tools diatas dengan melakukan langkah-langkah yang sama. Berikut yang ditampilkan adalah hasil analisa pengecekan dari masing-masing metode dalam bentuk tabel dibawah ini:

1. Metode Tools Exif/Metadata

Analisa hasil perbandingan foto asli dan foto manipulasi dari *Metode Tools Exif/Metadata* ditampilkan dalam tabel 1 dan tabel 2 berikut:

Tabel 1. Hasil Foto Asli

No	Menu	Description
1	System	FileName, FileSize, FileModifyDate, FileAccessDate, FileInodeChangeDate, FilePermissions
2	File	FileType, FileTypeExtension, MIMEType, ExifByteOrder, ImageWidth, ImageHeight, EncodingProcess, BitsPerSample, ColorComponents, YCbCrSubSampling
3	IFD0	ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, ModifyDate, YCbCrPositioning
4	ExifIFD	ExposureProgram, ISO, ExifVersion, DateTimeOriginal, CreateDate,

		OffsetTime, OffsetTimeOriginal, OffsetTimeDigitized, ComponentsConfiguration, DigitalZoomRatio, FocalLengthin35mmFormat, SceneCaptureType
5	IFD1	Compression, Orientation, XResolution, YResolution, ResolutionUnit, ThumbnailOffset, ThumbnailLength, YCbCrPositioning, ThumbnailImage
6	Composite	Aperture, ImageSize, Megapixels, ShutterSpeed, SubSecCreateDate, SubSecDateTimeOriginal, SubSecModifyDate, FocalLength35efl, LightValue

Tabel 2. Hasil Foto Manipulasi

No	Menu	Description
1	System	FileName, FileSize, FileModifyDate, FileAccessDate, FileInodeChangeDate, FilePermissions
2	File	FileType, FileTypeExtension, MIMEType, ExifByteOrder, ImageWidth, ImageHeight, EncodingProcess, BitsPerSample, ColorComponents, YCbCrSubSampling
3	IFD0	ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, ModifyDate, YCbCrPositioning
4	ExifIFD	ExposureProgram, ISO, ExifVersion, DateTimeOriginal, CreateDate, OffsetTime, OffsetTimeOriginal, OffsetTimeDigitized, ComponentsConfiguration, DigitalZoomRatio, FocalLengthin35mmFormat, SceneCaptureType
5	IFD1	Compression, Orientation, XResolution, YResolution, ResolutionUnit, ThumbnailOffset, ThumbnailLength, YCbCrPositioning, ThumbnailImage
6	IPTC	CodedCharacterSet, ApplicationRecordVersion, DateCreated, TimeCreated
7	Photoshop	IPTCDigest, XResolution, DisplayedUnitsX, YResolution, DisplayedUnitsY, PrintStyle, PrintPosition, PrintScale, WriterName, ReaderName, PhotoshopQuality
8	XMP	Toolkit, CreatorTool, ModifyDate, CreateDate, MetadataDate, Format
9	ICC-header	ProfileCMType, ProfileVersion, ProfilClass, ColorSpaceData, ProfileDateTime, ProfilFileSignature, ProfilCreator, ProfileCopyright, ProfileDescription
10	Adobe	DCTEncodeVersion, APP14Flags0, APP14Flags1, ColorTransform, Aperture
11	Composite	Aperture, ImageSize, Megapixels, ShutterSpeed, SubSecCreateDate, SubSecDateTimeOriginal, SubSecModifyDate, FocalLength35efl, LightValue

Untuk analisa hasil perbandingan dari *Metode Tools Exif/Metadata* adalah bisa dilihat dengan jelas dari tabel 1 dan tabel 2, dimana tabel 2 lebih banyak memberikan informasi seperti IPTC, Photoshop, XMP, ICC-header. Sudah sangat jelas bahwa gambar 12 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu tools yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop.

2. Metode Reverse Image

Analisa hasil perbandingan dari *Metode Reverse Image* adalah menampilkan *OfficeEquipment* atau peralatan kantor yang sesuai dan berhubungan dengan apa yang ada di gambar, baik dari foto asli maupun yang sudah dimanipulasi, sehingga pada saat muncul banyak gambar-gambar yang berupa peralatan kantor dan link website yang ditampilkan juga berisi tentang peralatan kantor semua. Foto asli yang diambil dari Smartphone dan yang sudah di manipulasi dengan Photoshop ini juga tidak ditemukan gambar persis yang sama di internet, karena memang foto sampel ini belum pernah di upload di media sosial dan website. Berbeda dengan kasus sampel 3.1 Bukti Foto dari Internet/Media Sosial diatas, banyak yang tersebar di internet karena memang foto sampel tersebut diambil di Internet/Media Sosial.

3. Metode Image Forensics

Analisa hasil perbandingan foto asli dan foto manipulasi dari *Metode Image Forensics* ditampilkan dalam tabel 3 dan tabel 4 berikut:

Tabel 3. Hasil Foto Asli

No	Menu	Description
1	Dashboard	Static analysis, EXIF metadata extraction, Preview extraction from metadata, Localization, Error Level Analysis, Signature check
2	Static	Static info, FileType, Hashes
3	EXIF	Segment, PHOTO, IMAGE, THUMBNAIL, IOP
4	Thumb	Size, Mime type, Dimension
5	ELA	Black Striped Drawing
6	Signatures	Low, Medium

Tabel 4. Hasil Foto Manipulasi

No	Menu	Description
1	Dashboard	Static analysis, EXIF metadata extraction, IPTC extraction, XMP extraction, Preview extraction from metadata, Localization, Error Level Analysis, Signature check
2	Static	Static info, FileType, Hashes
3	EXIF	Segment, PHOTO, IMAGE, THUMBNAIL, IOP
4	IPTC	Segment, APPLICATION2, ENVELOPE
5	XMP	Segment, XMPMM, PHOTOSHOP, XMP, DC
6	Thumb	Size, Mime type, Dimension
7	ELA	Black Striped Drawing
8	Signatures	Low, Medium, High

Untuk analisa hasil perbandingan dari *Metode Image Forensics* adalah dengan membandingkan tabel 3 dan tabel 4, dimana tabel 4 lebih banyak memberikan informasi seperti IPTC, XMP. Sudah sangat jelas juga bahwa gambar 12 merupakan foto yang sudah di manipulasi, karena informasinya memunculkan salah satu *tools* yang digunakan untuk mengedit memanipulasi foto tersebut yaitu Photoshop sama seperti *metode tools exif/metadata*, bedanya *Metode Image Forensics* bisa memunculkan *Error Level Analysis (ELA)* untuk mendeteksi perbedaan *error* pada seluruh bagian foto yang disimpan dengan kompresi *lossy* seperti JPEG. Algoritma ELA mempermudah pengguna untuk mengetahui apakah sebuah foto sudah asli atau hasil dari manipulasi. Dari hasil analisis ELA sendiri bahwa gambar 12 memiliki daerah dan tepian yang berbeda pada bagian gambar 11 yang asli, sehingga bisa disimpulkan gambar 12 merupakan gambar hasil manipulasi.

4. KESIMPULAN

Kesimpulan yang bisa diambil dari penelitian ini adalah adanya sebuah pilihan metode yang bisa digunakan oleh para pengguna internet/media sosial dalam menyaring sebuah informasi yang berhubungan foto hoax, dimana para pengguna bisa melakukan analisa terlebih dahulu sebelum menyebarkan kembali informasi/foto tersebut. Dengan melihat hasil analisa foto asli dan foto manipulasi dari ketiga metode diatas bisa ditarik kelebihan dan kekurangan dari masing-masing metode tersebut. *Metode Tools Exif/Metadata* banyak menampilkan metadata file yang tersembunyi pada sebuah foto yang bisa di analisa informasi kebenaran apa saja yang terkandung didalamnya, *Metode Reverse Image* bisa menelusuri foto-foto serupa yang mirip atau yang aslinya sehingga akan muncul foto-foto yang pernah di upload dan dimiliki oleh siapa saja dan yang terakhir dengan *Metode Image Forensics* juga banyak menampilkan metadata file yang ada didalam foto sampai memunculkan *Error Level Analysis (ELA)* foto dimana daerah dan tepian yang mirip pada foto aslinya akan terlihat mirip pula, jika tidak mirip, besar kemungkinan foto tersebut hasil manipulasi.

5. SARAN

Pengembangan selanjutnya dalam penelitian ini bisa dengan menggunakan metode lain dari ketiga metode yang sudah di uji cobakan itu, dengan melihat kemudahan dan efektivitasnya dari sisi pengguna. Untuk foto juga bisa mengambil sampel yang ada di PC/Laptop untuk kemudian di upload terlebih dahulu di internet/media sosial. Bukti foto yang sudah di upload kemudian di download kembali lalu melakukan manipulasi, sehingga hasil analisisnya dengan menggunakan metode yang dilakukan diatas atau yang lainnya bisa dibandingkan dengan sampel foto yang ada di PC/Laptop yang belum pernah di upload.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak terkhusus Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi yang telah memberi dukungan financial terhadap penelitian ini dan ucapan terima kasih banyak juga kepada kampus Univeristas Teknologi Mataram yang telah memberi kesempatan dan dukungan kepada peneliti untuk melaksanakan proses penelitian sesuai dengan jadwal dan pembiayaan yang telah diberikan oleh pemerintah, sehingga proses penelitian dosen pemula ini dapat terlaksana dengan baik dan lancar sesuai dengan jadwal yang telah ditetapkan.

DAFTAR PUSTAKA

- [1] Kementerian Komunikasi dan Informatika. (2018, October 4). 1000 Berita Hoax Selama Masa Kampanye Pemilu 2019. Retrieved from detik.com: <https://news.detik.com/berita/4264513/kemenkominfo-ada-1000-berita-hoax-selama-masa-kampanye-pemilu>
 - [2] Mastel. (2017, February 13). Hasil Survey MASTEL Tentang Wabah HOAX Nasional. Retrieved from mastel.id: <https://mastel.id/infografis-hasil-survey-mastel-tentang-wabah-hoax-nasional>
 - [3] Juliswara, V. (2017). Mengembangkan Model Literasi Media yang Berkebhinnekaan dalam Menganalisis Informasi Berita Palsu (Hoax) di Media Sosial. *Jurnal Pemikiran Sosiologi* Volume 4 No. 2, 142-164.
 - [4] Gumilar, G., Adiprasetyo, J., & Maharani, N. (2017). Literasi Media: Cerdas Menggunakan Media Sosial Dalam Menanggulangi Berita Palsu (Hoax) Oleh Siswa SMA. *Jurnal Pengabdian Kepada Masyarakat* Vol. 1, No. 1 ISSN 1410 - 5675, 35-40.
 - [5] Adhianto, D. S., Utari, P., & Slamet, Y. (2017). Pemberitaan Hoax di Media Online Ditinjau dari Konstruksi Berita dan Respon Netizen. *Jurnal Ilmu Komunikasi*, Volume 15, Nomor 3, September - Desember, 215-225.
 - [6] Juditha, C. (2018). Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya. *Jurnal Pekommas*, Vol. 3 No. 1, April, 31-44.
 - [7] Fatkhurahman. (2018). Kemampuan Mahasiswa Tempatan Menilai Berita Palsu Atau "Hoax" Dalam Media Sosial Dalam Upaya Pengembangan Jiwa Kewirausahaan. *Jurnal Benefita* 3(3) Oktober, 417-426.
 - [8] Heriyanto. (2013). ANALISA GAMBAR BITMAP TERMODIFIKASI ATAU TIDAK TERMODIFIKASI DENGAN MEMADUKAN METODE DEVIASI PIXEL, RGB (RED GREEN BLUE) DAN HISTOGRAM. *Seminar Nasional Informatika 2013 (semnasIF 2013)*. ISSN: 1979-2328.
 - [9] Riadi, I., Fadlil, A., & Sari, T. (2017). Image Forensic for detecting Splicing Image with Distance Function. *International Journal of Computer Applications* (0975 – 8887). Volume 169 – No.5.
 - [10] Riadi, I., Yudhana, A., & Yuli Sulisty, W. (2019). DETEKSI PEMALSUAN FOTO DIGITAL MENGGUNAKAN IMAGE FORENSICS. *Jurnal Mobile and Forensics (MF)*. Vol. 1, No. 1, pp. 13-21. P-ISSN: 2656-6257, E-ISSN: 2714-6685.
-

- [11] Imanda Putra, A., Umar, R., & Fadlil, A. (2018). ANALISIS FORENSIK DETEKSI KEASLIAN METADATA VIDEO MENGGUNAKAN EXIFTOOL. Seminar Nasional Informatika 2018 (semnasIF 2018). ISSN: 1979-2328.
 - [12] Lad Ami D., Mori Shilpa I., Raulji Urvashi K., & Shaikh Saliha H. (2017). Reverse Image Search: Image retrieval using various techniques. Scientific Journal of Impact Factor (SJIF): 4.72. Volume 4, Issue 4, e-ISSN (O): 2348-4470.
 - [13] Wijayanto, H., Ady Prabowo, I., & Harsadi, P. (2018). OPTIMALISASI PENYUSUTAN EXIF METADATA DENGAN TEKNIK SUBSTITUSI NULL VALUE PADA KASUS KEAMANAN CITRA DIGITAL. Jurnal Ilmiah SINUS 16(1).
 - [14] Adrakatti, A .F., Wodeyar, R. S., & Mulla, K. R. (2016). Search by Image: A Novel Approach to Content Based Image Retrieval System. International Journal of Library Science™. Volume 14; Issue No. 3; ISSN 0975-7546.
 - [15] Yuli Sulisty, W., Riadi, I., & Yudhana, A. (2018). ANALISIS DETEKSI KEASLIAN CITRA MENGGUNAKAN TEKNIK ERROR LEVEL ANALYSIS DENGAN FORENSICALLYBETA. Seminar Nasional Informatika 2018 (semnasIF 2018). ISSN: 1979-2328.
 - [16] Wijayanto, H., Ady Prabowo, I., & Harsadi, P. (2018). OPTIMALISASI PENYUSUTAN EXIF METADATA DENGAN TEKNIK SUBSTITUSI NULL VALUE PADA KASUS KEAMANAN CITRA DIGITAL. Jurnal Ilmiah SINUS 16(1).
 - [17] Apriliani, A., Hijjayanti, K., & Suhairoh. (2020). Analisis Keaslian Citra Dengan Menggunakan Exif Metadata. CESS (Journal of Computer Engineering System and Science), 84-88
 - [18] P. N. Andono, T. Sutojo och M. , Pengolahan Citra Digital, Yogyakarta: ANDI, 2017.
 - [19] ExifTool by Phil Harvey (2021, July 30). Metode Tools Exif/Metadata. Retrieved from exiftool.org: <https://exiftool.org/>
 - [20] Jeffrey's Image Metadata Viewer (2021, July 30). Metode Tools Exif/Metadata. Retrieved from exif.regex.info: <http://exif.regex.info/exif.cgi>
 - [21] EXIF & Metadata Viewer (2021, July 30). Metode Tools Exif/Metadata. Retrieved from exifmeta.com: <https://exifmeta.com/>
 - [22] Adrakatti, A .F., Wodeyar, R. S., & Mulla, K. R. (2016). Search by Image: A Novel Approach to Content Based Image Retrieval System. International Journal of Library Science™. Volume 14; Issue No. 3; ISSN 0975-7546.
 - [23] Google Images (2021, July 30). Metode Reverse Image. Retrieved from images.google.com: <https://images.google.com/>
 - [24] Yuli Sulisty, W., Riadi, I., & Yudhana, A. (2018). ANALISIS DETEKSI KEASLIAN CITRA MENGGUNAKAN TEKNIK ERROR LEVEL ANALYSIS DENGAN FORENSICALLYBETA. Seminar Nasional Informatika 2018 (semnasIF 2018). ISSN: 1979-2328.
 - [24] Rizky Al-Fajri, M., Caruddin & Yusup, D. (2021). Analisis Image Forensic Dalam Mendeteksi Rekayasa File Image Dengan Metode Nist. Jurnal Sistem dan Teknologi Informasi (Justindo). Volume 6, No. 2; E-ISSN: 25541-5735, P-ISSN: 2502-5724.
 - [25] Image Forensic (2021, July 30). Metode Image Forensics. Retrieved from [imageforensic.com](https://www.imageforensic.org/): <https://www.imageforensic.org/>
-