JUSTISE
E-ISSN : XXXX-XXXX

Journal Data Science, Technology, Informatics and Security (JuSTISe)

Volume 2 No 2 Desember 2024

EFEKTIFITAS RANSAC DAN OUTLIER DETECTION DALAM MENDETEKSI KEASILIAN PADA GAMBAR FOTO PRODUK DIGITAL HAMAKO ECO BABYWEAR

Anhar Abul Gani[1], Deni Suprihadi[2]
Program Studi Teknik Informatika, Universitas Kebangsaan Republik Indonesia, Bandung
Email : anhargani95@gmail.com[1], dens.tesis99@gmail.com[2]

ABSTRAK

Penelitian ini membahas peningkatan risiko kejahatan digital, khususnya pemalsuan gambar, akibat perkembangan teknologi informasi dan komunikasi. Studi ini fokus membandingkan dua metode, yaitu RANSAC dan Outlier Detection, dalam menganalisis keaslian gambar digital terkait produk *fashion* Hamako Eco Baby Wear, yang berpotensi melanggar Hak Kekayaan Intelektual (HKI). Kasus yang diteliti melibatkan penyalahgunaan logo dan atribut produk. *Framework Integrated Digital Forensic Investigation Framework* (IDFIF) digunakan sebagai kerangka kerja, dilengkapi dengan alat bantu seperti Image Hash Generator dan RANSAC Detection. Penelitian ini juga menganalisis metadata dari gambar sampel dan gambar tersangka, yang memberikan informasi penting terkait waktu pengambilan serta alat yang digunakan untuk mengambil atau mengedit gambar. Hasil menunjukkan bahwa metode *Outlier Detection* efektif dalam mengidentifikasi anomali gambar secara cepat, sementara RANSAC mampu menghasilkan model matematis yang lebih tahan terhadap outlier, memungkinkan analisis yang lebih mendalam. Kedua metode ini saling melengkapi dalam membuktikan pemalsuan atau penyalahgunaan gambar produk. Penelitian ini memberikan kontribusi signifikan dalam pengembangan teknik forensik digital, khususnya dalam menganalisis keaslian gambar digital di era modern.

Kata Kunci : Pemalsuan Gambar Digital, Cybercrime, Digital Forensic, RANSAC, Outlier Detection

ABSTRACK

This study addresses the increasing risk of digital crimes, particularly image forgery, as a result of advancements in information and communication technology. The research focuses on comparing two methods, RANSAC and Outlier Detection, for analyzing the authenticity of digital images related to Hamako Eco Baby Wear products, which potentially violate Intellectual Property Rights (IPR). The case involves the misuse of product logos and attributes. The Integrated Digital Forensic Investigation Framework (IDFIF) is employed as the main framework, supplemented by tools such as the Image Hash Generator and RANSAC Detection. This study also examines metadata from sample and suspect images,

providing crucial information about the time and tools used for capturing or editing the images. The findings reveal that the Outlier Detection method is effective in quickly identifying image anomalies, while RANSAC generates a mathematical model that is robust against outliers, enabling deeper analysis. These two methods complement each other in proving image forgery or misuse. This research contributes significantly to the development of digital forensic techniques, particularly in analyzing the authenticity of digital images in the modern era.

Keywords : *Digital Image Forgery, Cybercrime, Digital Forensics, RANSAC, Outlier Detection*

1. PENDAHULUAN

Teknologi informasi dan komunikasi telah menjadi bagian integral dari kehidupan modern. Meski menawarkan berbagai kemudahan, perkembangan ini juga menghadirkan tantangan baru terkait keamanan digital, terutama kejahatan dunia maya atau cybercrime. Cybercrime sebagai kejahatan yang dilakukan melalui internet, dengan berbagai bentuk seperti penipuan online, perdagangan gelap, dan serangan siber[1]. Untuk mengatasi masalah ini, forensik digital atau digital forensik berkembang sebagai ilmu yang berkaitan dengan identifikasi, pengumpulan, pemeriksaan, dan analisis bukti digital untuk mendukung proses penyelidikan hukum[2].

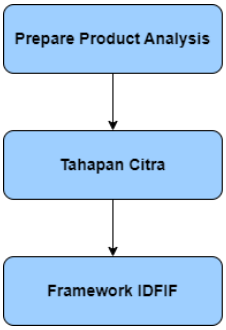
Laporan Patroli Siber tahun 2019 mencatat 4.586 kasus kejahatan siber, dengan penipuan online sebagai mayoritas kasus. Penipuan ini sering memanfaatkan gambar produk palsu atau informasi yang menyesatkan di media sosial seperti Instagram, WhatsApp, dan Facebook . Salah satu teknik manipulasi gambar yang umum digunakan adalah copy-move, sebagai teknik pemalsuan gambar di mana suatu bagian dari gambar disalin dan dipindahkan ke bagian lain dalam gambar yang sama[3].

Dalam hal ini, metode Random Sample Consensus (RANSAC) dan Outlier Detection dapat menjadi solusi efektif untuk mendeteksi pemalsuan gambar. RANSAC didefinisikan sebagai metode iteratif yang digunakan untuk memperkirakan parameter model dari kumpulan data yang mengandung outliers. Algoritma ini bekerja dengan memilih subset acak dari data untuk membangun model, lalu mengevaluasi seberapa baik model tersebut sesuai dengan seluruh dataset. [4]. Sementara itu, Deteksi Outlier didefinisikan sebagai proses identifikasi titik data yang berbeda secara signifikan dari mayoritas data dalam suatu kumpulan yang sedang dianalisis [5].

Penelitian ini membandingkan efektivitas RANSAC dan Deteksi Outlier dalam menganalisis keaslian gambar digital, terutama dalam kasus pemalsuan foto produk. Diharapkan hasil penelitian ini dapat memberikan panduan dalam penerapan teknik forensik digital untuk menangani kejahatan siber, terutama yang terkait dengan pemalsuan gambar produk.

2. METODE PENELITIAN

Penelitian ini terdiri dari tiga tahap Prepare Product Analysis, Tahapan Citra, dan Integrated Digital Forensic Investigation Framework (IDFIF).



Gambar 2.1 – Tahapan Penelitian

Data dikumpulkan dari gambar menggunakan tools SHA-256 Image untuk mendapatkan nilai hash, Algoritma SHA-256 adalah fungsi hash kriptografi dan digunakan dalam sertifikat digital serta integritas data. SHA-256 dikembangkan oleh N.I.S.T. Algoritma SHA256 mengambil pesan dengan panjang sembarang yang lebih kecil dari 264 bit sebagai masukan dan menghasilkan intisari pesan 256-bit sebagai keluaran[6], tools Image metadata generator bertujuan untuk mendeteksi metadata pada foto yang diambil dan pengaturan pada kamera, Metadata didefinisikan sebagai "data tentang data." bahwa metadata selalu merujuk pada data lain, menciptakan hubungan antara dua elemen[7]. Data yang diambil meliputi nomor hash dan metadata EXIF dari citra digital. Studi kasus yang digunakan adalah foto produk dari Hamako Eco Baby Wear merek tersebut telah terdaftar di Pangkalan Data kekayaan Intelektual (PDKI) dengan kode D002017057644 sebagai HKI Merek. Hak Kekayaan Intelektual mencakup hak-hak yang dimiliki oleh pencipta dan pemilik karya-karya intelektual, yang memberi mereka kekuasaan untuk melindungi karya mereka dari penggunaan tanpa izin[8].

Gambar 2.2 – Hak Kekayaan Intelektual Hamako

2.1 Prepare Product Analysis

Tahapan ini merupakan tahap pengumpulan data tentang suatu produk seperti kategori produk. Peneliti menggunakan foto produk fashion bayi dari Hamako Eco Baby Wear untuk dijadikan uji coba pada penelitian yang sedang diteliti.

2.1.1 Masalah Penelitian (Research Problem)

Pada tahap ini akan meneliti foto produk sebagai barang bukti digital forensik. Penelitian ini dilakukan sesuai dengan ciri-ciri produk yang ada, untuk melakukan investigasi digital forensik pada digital image dengan melihat ciri-ciri dari foto Produk Sample.

Ciri – ciri produk Hamako Eco Baby Wear :

1. Nametag 1 bertulisan Hamako Eco Baby Wear
2. Nametag 2 bertulisan Tencel
3. Size Label pada pakaian berlogo hamako
4. Logo Hamako dengan variasi huruf jepang yang memiliki HKI.
5. Setiap pakaian terdapat tulisan dan logo Hamako

2.1.4 Pengumpulan Data

Tahap berikutnya adalah mengakuisisi data yang telah teridentifikasi sebelumnya. Sumber data berasal dari Foto Produk Hamako Eco Baby Wear. Pengumpulan data dan informasi sebagai penunjang penelitian ini harus memiliki tujuan yang terarah. Tujuan yang jelas memungkinkan peneliti untuk menentukan data relevan yang diperlukan. Penting untuk tidak hanya fokus pada pengumpulan data, tetapi juga memperhatikan cara data tersebut diperoleh. Pada Tahap ini peneliti mengumpulkan bukti dari foto produk sample dari hamako dan pada foto produk yang disalahgunakan.

Gambar 2.3 – Foto Produk Sample

Pada foto produk sample terdapat ciri-ciri dari foto produk dari Hamako, untuk lebih jelasnya sebagai berikut:

1. Adanya logo tulisan Hamako di baju samping kiri bawah.
2. Nametag 1 adanya logo tulisan Hamako dan logo dengan tulisan Tencel.
3. Adanya logo dan tulisan Hamako jepang di bagian kaki

Gambar 2.4 – Foto Produk Suspect

Pada foto produk yang disalahgunakan terdapat penyalahgunaan dengan mengganti logo dan bebara unsur lainnya seperti :

1. Berubahnya logo tulisan hamako menjadi Solta pada bagian baju samping kiri bawah.
2. Nametag 1 dan 2 bertulisan diganti dengan merk lain yaitu Solta.

2.2 Tahapan Citra

Tahapan ini mencakup langkah-langkah untuk mengolah dan menganalisis citra dari akuisisi hingga interpretasi informasi. Tahapan Citra adalah Peningkatan citra didefinisikan sebagai proses memodifikasi citra agar lebih sesuai untuk aplikasi tertentu.

2.2.1 Akuisisi Citra

Pada tahap ini, citra diakuisisi menggunakan kamera digital sebagai bukti digital. Berikut adalah hasil akuisisi dan konversi citra produk pakaian dari Hamako Eco Baby Wear.

Tabel 1 Akuisisi Citra

No	Nama Produk	Format Foto	Pengambilan Citra	Resolusi
1	Produk Pakaian Bayi	JPG	Apple Iphone 11	3024x3024px
2	Produk Pakaian Balita	JPG	Apple Iphone 6	1000x1000px
3	Produk pakaian anak-anak	JPG	Apple Iphone 6	1000x1000px

2.2.2 Preprocessing

Pada tahap ini memastikan kualitas citra dari foto produk yang akan dijadikan sample penelitian. Minimal kualitas citra untuk diteliti adalah 512x412px dengan resolusi yang lebih tinggi memungkinkan machine learning untuk melihat lebih banyak detail dan menghasilkan analisis yang lebih akurat.

2.2.3 Segmentasi

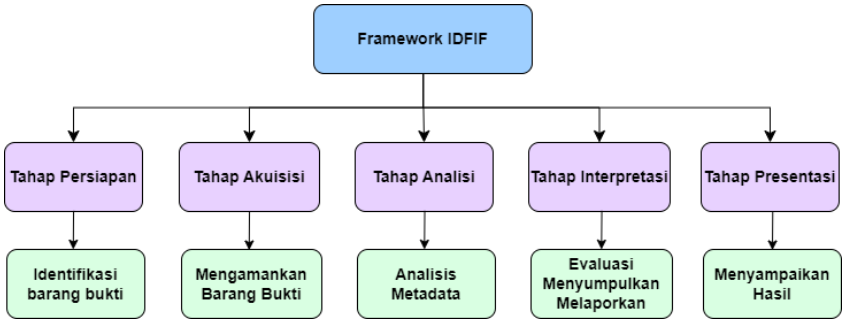
Pada tahap segmentasi mengumpulkan atribut citra yang sama seperti tekstur dan intensitas pixel, untuk lebih jelasnya sebagai berikut :

Tabel 2 Segmentasi Pixel

No	Camera Digital yang dipakai	Intensitas Pixel	Nama Produk
1	Apple Iphone 11	3024x4032px	Produk Bayi
2	Apple Iphone 6	1000x1000px	Produk Anak-anak dan Foto Produk Balita

2.3 Framework IDFIF *(Integrated Digital Forensic Framework).*

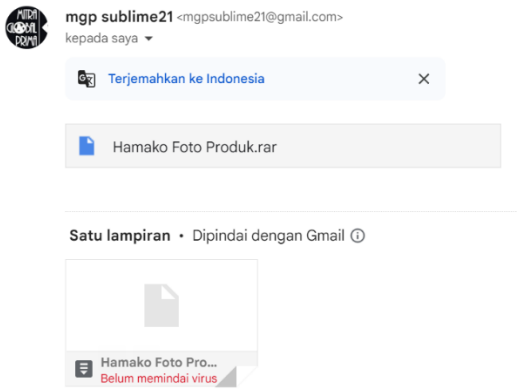
IDFIF (Integrated Digital Forensics Investigation Framework) adalah metodologi investigasi digital forensik yang komprehensif dan dapat diterapkan dalam kasus pemalsuan gambar. Berikut tahapan-tahapan IDFIF dalam kasus pemalsuan gambar digital[9].



Gambar 2.5 – Tahapan Framework IDFIF

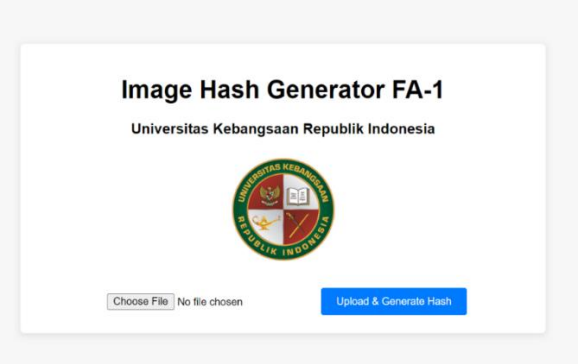
2.3.1 Persiapan

Pada tahap ini mempersiapkan gambar digital/foto produk yang disinyalir sebagai foto produk yang disalahgunakan atau dipalsukan. berikut penyerahan file foto Produk Hamako.



Gambar 2.6 – Persiapan Foto produk yang akan digunakan

Foto yang akan digunakan adalah foto produk pakaian bayi yang disalahgunakan untuk dijadikan sample penelitian yang akan dilakukan, dan untuk mengamankan barang bukti digital pada gambar citra maka dilakukan hashing dengan menggunakan tools Image Hash Generator FA-1.



Gambar 2.7 – Tampilan interfaces *Tools* Hash Generator FA-1

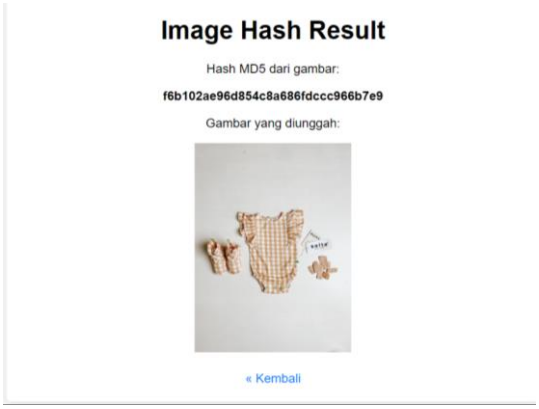
Berikut hasil hash pada gambar foto produk pakaian bayi sample :

Gambar 2.8 – Melacak Hash Foto Produk sample (Hash Generator FA-1)

Hasil perhitungan hash pada gambar foto produk pakaian bayi asli adalah 624ef53c3ac24b47609c5fe4920b9e66.

Gambar 2.9 – Foto Produk Sample

Berikut hasil hash pada gambar foto produk pakaian bayi suspect :



Gambar 2.10 – Melacak Hash Foto Produk Suspect (Hash Generator FA-1)

Hasil perhitungan hash pada gambar foto produk pakaian bayi suspect adalah f6b102ae96d854c8a686fdccc966b7e9.

Gambar 2.11 – Foto Produk Suspect

Pada foto produk sample terdapat ciri-ciri dari foto produk dari Hamako, untuk lebih jelasnya sebagai berikut:

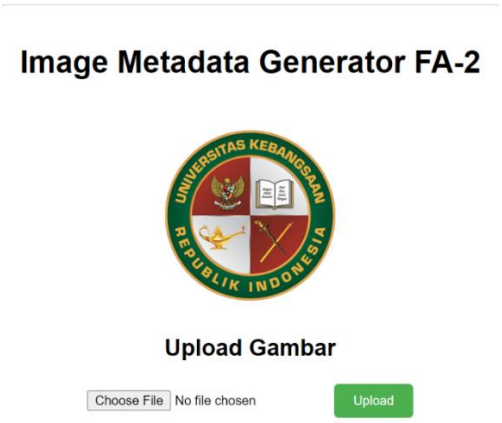
1. Adanya logo tulisan Hamako di baju samping kiri bawah.
2. Nametag 1 adanya logo tulisan Hamako dan logo dengan tulisan Tencel.
3. Adanya logo dan tulisan Hamako jepang di bagian kaki

Pada foto produk yang disalahgunakan terdapat penyalahgunaan dengan mengganti logo dan bebara unsur lainnya seperti :

1. Berubahnya logo tulisan hamako menjadi Solta pada bagian baju samping kiri bawah.
2. Nametag 1 dan 2 bertulisan diganti dengan merk lain yaitu Solta.

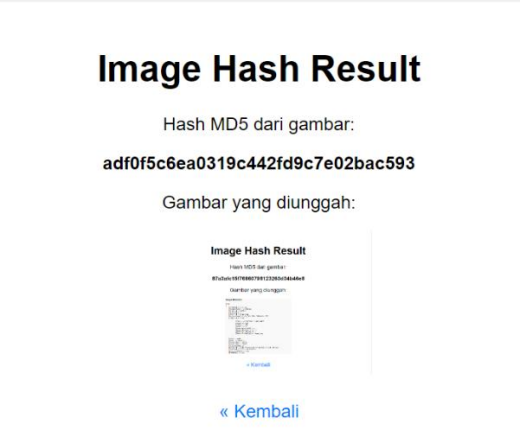
2.3.2 Akuisisi

Pada tahap ini peneliti mengakuisisi foto produk sample dan yang telah disalahgunakan menggunakan *tools Image Metadata Generator FA-2,* untuk memastikan dan mengamankan metadata untuk dijadikan bukti digital. Berikut tampilan interface pada *tools Image Metadata Generator FA-2*, seperti pada gambar 4.20.



Gambar 2.12 – Tampilan *tools* Image Metadata Generator

Berikut hasil Hash dari metadata foto produk pakaian bayi sample :



Gambar 2.13 – Melacak Hash Metadata sample

Hasil perhitungan hash pada gambar metadata foto produk pakaian bayi sample adalah adf0f5c6ea0319c442fd9c7e02bac593.

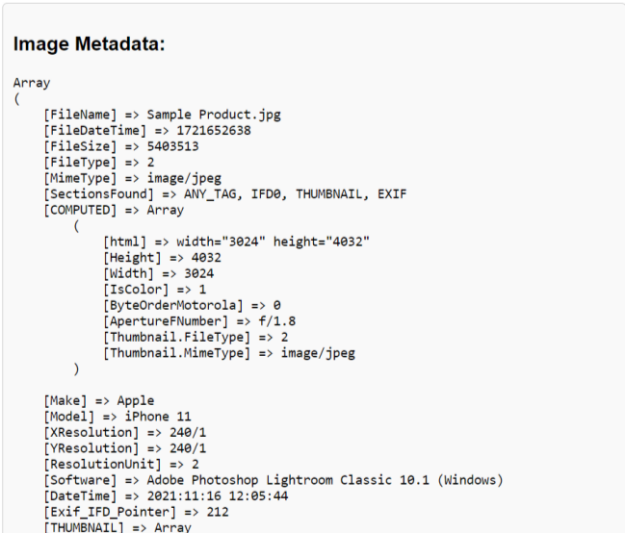


Image Metadata:

```
Array
(
    [FileName] => Sample Product.jpg
    [FileDateTime] => 1721652638
    [FileSize] => 5403513
    [FileType] => 2
    [MimeType] => image/jpeg
    [SectionsFound] => ANY_TAG, IFD0, THUMBNAIL, EXIF
    [COMPUTED] => Array
        (
            [html] => width="3024" height="4032"
            [Height] => 4032
            [Width] => 3024
            [IsColor] => 1
            [ByteOrderMotorola] => 0
            [ApertureFNumber] => f/1.8
            [Thumbnail.FileType] => 2
            [Thumbnail.MimeType] => image/jpeg
        )

    [Make] => Apple
    [Model] => iPhone 11
    [XResolution] => 240/1
    [YResolution] => 240/1
    [ResolutionUnit] => 2
    [Software] => Adobe Photoshop Lightroom Classic 10.1 (Windows)
    [DateTime] => 2021:11:16 12:05:44
    [Exif_IFD_Pointer] => 212
    [THUMBNAIL] => Array
```

Gambar 2.14 – Metadata foto produk sample

Berdasarkan gambar metadata foto produk sample pada gambar 4.22 terdapat beberapa data penting seperti berikut:

1. Diambil dengan camera digital Apple Iphone 11.
2. Software editing Adobe lightroom.
3. Format yang dipakai JPEG.
4. Dengan waktu pengambilan gambar 16 November 2021.

Berikut hasil hash pada foto produk pakaian bayi suspect:

Image Hash Result

Hash MD5 dari gambar:

df0f2a38781bb6dbbc4958445feff730

Gambar yang diunggah:

« Kembali

Gambar 2.15 – Melacak Metadata yang terdapat pada foto produk yang disalahgunakan

Hasil perhitungan hash pada gambar metadata foto produk pakaian bayi sample adalah df0f2a38781bb6dbbc4958445feff730.
Berikut hasil Hash dari metadata foto produk pakaian bayi suspect:

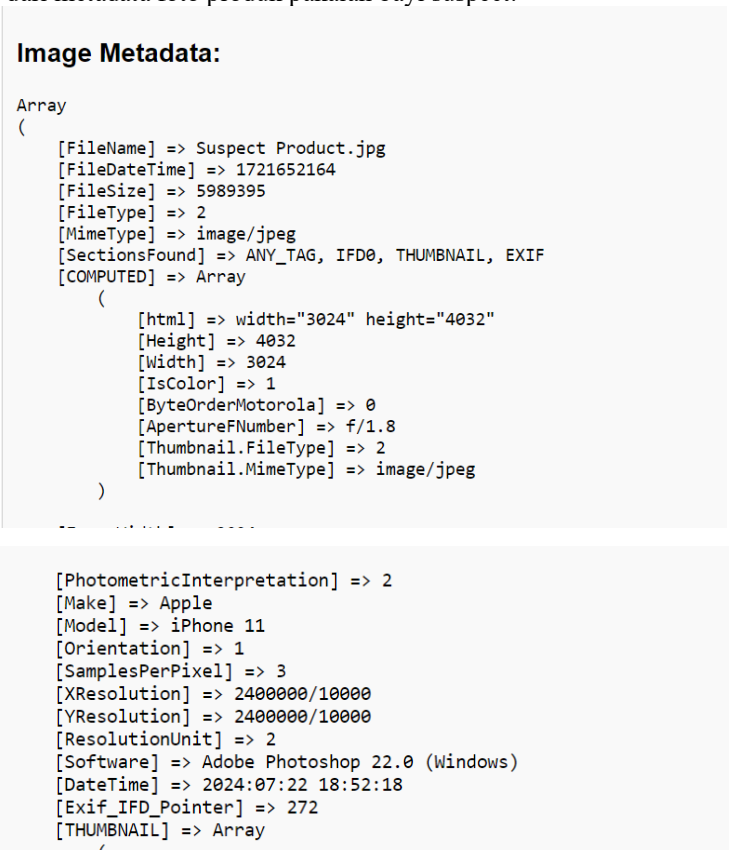


Image Metadata:

```
Array
(
    [FileName] => Suspect Product.jpg
    [FileDateTime] => 1721652164
    [FileSize] => 5989395
    [FileType] => 2
    [MimeType] => image/jpeg
    [SectionsFound] => ANY_TAG, IFD0, THUMBNAIL, EXIF
    [COMPUTED] => Array
        (
            [html] => width="3024" height="4032"
            [Height] => 4032
            [Width] => 3024
            [IsColor] => 1
            [ByteOrderMotorola] => 0
            [ApertureFNumber] => f/1.8
            [Thumbnail.FileType] => 2
            [Thumbnail.MimeType] => image/jpeg
        )

    [PhotometricInterpretation] => 2
    [Make] => Apple
    [Model] => iPhone 11
    [Orientation] => 1
    [SamplesPerPixel] => 3
    [XResolution] => 2400000/10000
    [YResolution] => 2400000/10000
    [ResolutionUnit] => 2
    [Software] => Adobe Photoshop 22.0 (Windows)
    [DateTime] => 2024:07:22 18:52:18
    [Exif_IFD_Pointer] => 272
    [THUMBNAIL] => Array
```

MD5 : df0f2a38781bb6dbbc4958445feff730

Gambar 2.16 – Metadata yang terdapat pada foto produk yang disalahgunakan

Berdasarkan gambar metadata foto produk suspect pada gambar 4.24 terdapat beberapa data penting seperti berikut:

1. Diambil dengan camera digital Apple Iphone 11.
2. Software editing Adobe Photoshop.
3. Format yang dipakai JPEG
4. Dengan waktu pengambilan gambar 22 Juli 2024.

2.3.3 Analisis

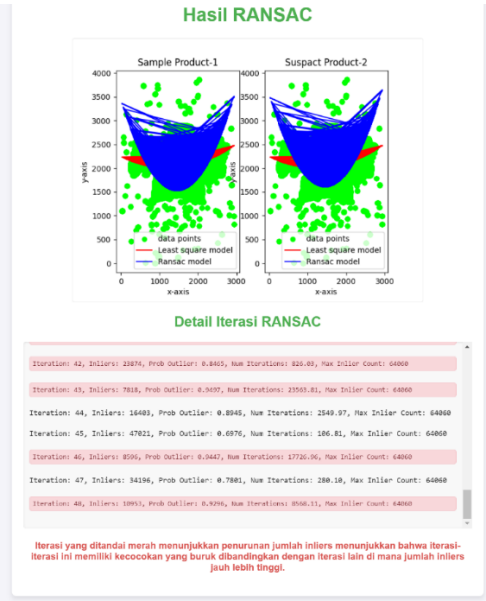
Pada tahap analisis ini, peneliti memanfaatkan metode deteksi metadata serta alat hash, yaitu SHA-256 dan MD5, untuk mendeteksi potensi pemalsuan atau penyalahgunaan foto produk. Setelah metadata diperiksa, peneliti menggunakan metode RANSAC dan deteksi outlier untuk menganalisis konsistensi foto produk. Metode RANSAC membantu menemukan model terbaik sambil mengabaikan outlier, dengan hasilnya berupa kurva visualisasi dan iterasi.

Langkah-langkah analisis mencakup:

1. Pengunggahan Gambar dan CSV: Gambar sampel dan suspect serta file CSV diunggah melalui tools "Image Detection using Outlier Detection and RANSAC". Hasilnya disimpan di direktori uploads.
2. Deteksi Outlier: Skrip `detect.py` menganalisis kesamaan gambar dengan hasil berupa tingkat kemiripan, status gambar (suspect atau tidak), dan perbedaan visual ditandai dalam kotak merah.

Gambar 2.17 – Hasil Outlier Detection

3. Iterasi RANSAC: Skrip `ransac_model.py` memproses data CSV dengan metode RANSAC, menampilkan iterasi dan visualisasi kurva. Beberapa iterasi menunjukkan anomali seperti penurunan drastis jumlah inliers (misalnya pada iterasi 2, 3, 4, dan 10), jumlah iterasi tinggi (contoh iterasi 4), serta probabilitas outlier mendekati 1 (seperti iterasi ke-25). Hasil menunjukkan iterasi ke-9 sebagai salah satu yang paling stabil, dengan jumlah inliers tinggi dan iterasi minimal.



Gambar 2.17 – Hasil Metode RANSAC

Anomali-anomali ini menunjukkan pola tidak konsisten akibat noise atau outlier dominan dalam dataset, memberikan indikasi potensi penyalahgunaan pada gambar produk. Setelah hasil diperoleh, hash dari hasil outlier detection dan RANSAC dihitung, menghasilkan nilai: f37e28046af21003de04e9a0fea9b3c6.

Gambar 2.18 – Melacak Hash hasil pengolahan tools Image Detection using Outlier Detection and RANSAC tools Deteksi Outlier

2.3.4 Interpretasi

Pada tahap ini akan mengevaluasi hasil analisis dan menginterpretasikan temuan yang telah dibuktikan, menyimpulkan tentang gambar yang telah dimanipulasi dan menyusun laporan investigasi yang berisi temuan, analisis, dan kesimpulan dalam bentuk COC (*Chain Of Custody*) sebagai standarisasi pelaporan forensik digital.

2.3.5 Presentasi

Pada tahap ini menyajikan hasil investigasi kepada pihak yang berkepentingan, seperti penyidik, hakim, atau klien. Presentasi ini juga bertujuan untuk menjelaskan temuan dan kesimpulan dengan cara yang mudah dipahami, serta menjawab pertanyaan dan memberikan klarifikasi.

3. Hasil Pembahasan

Penelitian ini menunjukkan bahwa metode digital forensik yang diterapkan efektif dalam mengidentifikasi manipulasi pada gambar produk. Pada tahap *Prepare Product Analysis*, hasil hash SHA-256 dan MD5 untuk produk asli dan tersangka memperlihatkan adanya perbedaan signifikan, yang menunjukkan bahwa gambar suspect telah mengalami modifikasi. Selanjutnya, proses pemrosesan citra dan segmentasi pada *Tahapan Citra* meningkatkan detail gambar yang memungkinkan identifikasi manipulasi seperti perubahan logo dan label. Framework *Integrated Digital Forensics Investigation Framework* (IDFIF) memfasilitasi alur kerja forensik menyeluruh, di mana analisis metadata dan hashing pada gambar menunjukkan perbedaan yang mendukung indikasi manipulasi. Analisis dengan metode RANSAC memperlihatkan pola anomali pada gambar suspect yang memperkuat indikasi ketidaksesuaian. Pada tahap interpretasi, perbedaan hash dan metadata menegaskan adanya perubahan pada gambar suspect, dan hasil analisis ini kemudian disajikan dalam bentuk *Chain of Custody* untuk memperkuat integritas bukti dalam proses investigasi forensik digital. Hasilnya, penelitian ini membuktikan bahwa kombinasi metode hashing dan framework IDFIF adalah pendekatan efektif untuk mendeteksi manipulasi pada gambar digital.

4. Kesimpulan

Penelitian ini menggunakan kamera digital untuk memastikan kualitas gambar produk Hamako Eco Baby Wear dengan standar minimal 512x412px. Berdasarkan Tabel 2 Segmentasi Pixel, gambar produk

memenuhi kriteria sampel, sementara segmentasi atribut citra seperti tekstur dan intensitas pixel juga telah dilakukan. Foto produk bayi diambil dengan iPhone 11 (3024x4032px) dan produk anak-anak serta balita dengan iPhone 6 (1000x1000px). Ciri-ciri khusus produk Hamako terlihat dari logo di bagian tertentu, yang pada produk yang disalahgunakan mengalami perubahan menjadi merek Solta, namun sebagian tulisan Jepang tetap ada, menunjukkan potensi pelanggaran Hak Kekayaan Intelektual (HKI). Metadata gambar sampel menunjukkan pengambilan menggunakan iPhone 11 dan pengeditan dengan Adobe Lightroom pada 2021, sementara metadata gambar suspect menunjukkan penggunaan Adobe Photoshop pada 2024. Analisis RANSAC dan Outlier Detection mendeteksi perbedaan signifikan, dengan ambang batas kesamaan 98,27%, yang mengindikasikan penyalahgunaan. Outlier Detection berfungsi untuk deteksi cepat anomali, sedangkan RANSAC memberikan model tahan terhadap outliers, memungkinkan analisis lebih dalam. Kombinasi kedua metode ini efektif untuk mendeteksi manipulasi dan anomali pada data gambar produk.

Referensi

[1]. Thomas J. Holt, A. M.-S. (2022). *Cybercrime and Digital Forensics: An Introduction VOL 3.* London: Routledge.

[2]. Ahmed A. Abd El-Latif, L. T. (2024). *Digital Forensics and Cyber Crime Investigation.* London: Routledge.

[3]. Anjali L. Jadhav, S. V. (2023). *A Review on Machine Learning-Based Approaches for Image Forgery Detection.* Heidelberg: Springer.

[4]. Umbaugh, S. E. (2023). *Digital Image Processing and Analysis.* Florida: CRC Press.

[5]. N. N. R. Ranga Suri, N. M. (2019). *Outlier Detection: Techniques and Applications.* Heidelberg: Springer.

[6] Rachmawati, D. (2017). *A comparative study of Message Digest 5(MD5). Journal of Physics: Conference*, 1.

[7] Gartner, R. (2021). *Metadata in the digital Library: Building an Integrated Strategy with XML.* Euston Road: Faced Publishing.

[8] Goodhart, P. (2023). *Intellectual Property Rights: A Global Perspective*. Heildelberg: Springer.

[9] Casey, E. (2020). *Digital Forensic and Incident Response (5th ed)*. Florida: CRC Press