



Penerapan Metode Localization Tampering dan Hashing untuk Deteksi Rekayasa Video Digital

Alfiansyah Imanda Putra¹, Rusydi Umar², Abdul Fadlil³^{1,2}Program Studi Teknik Informatika, Universitas Ahmad Dahlan³Program Studi Teknik Elektro, Universitas Ahmad Dahlan¹alfiansyah1807048011@webmail.uad.ac.id, ²rusydi@mti.uad.ac.id, ³fadlil@mti.uad.ac.id

Abstract

The development of digital video technology which is increasingly advanced makes digital video engineering crimes prone to occur. The change in digital video has changed information communication, and it is easy to use in digital crime. One way to solve this digital crime case is to use the NIST (National Institute of Standards and Technology) method for video forensics. The initial stage is carried out by collecting data and carrying out the process of extracting the collected results. A local hash and noise algorithm can then be used to analyze the resulting results, which will detect any digital video interference or manipulation at each video frame, and perform hash analysis to detect the authenticity of the video. In digital video engineering, histogram analysis can be performed by calculating the histogram value metric, which is used to compare the histogram values of the original video and video noise and make graphical comparisons. The results of the difference in frame analysis show that the results of the video show that the 2nd to 7th frames experience an attack while the histogram calculation of the original video centroid value and video tampering results in different values in the third frame, namely with a value of 124.318 and the 7th frame of the video experiencing a difference in the value of 105,966 videos. tampering and 107,456 in the original video. Hash analysis on video tampering results in an invalid SHA-1 hash, this can prove that the video has been manipulated.

Keywords: Forensics, Video, Localization tampering, Manipulation.

Abstrak

Perkembangan teknologi video digital yang semakin maju membuat kejahatan rekayasa video digital rawan terjadi. Perubahan video digital membuat informasi yang disampaikan menjadi berubah dan sangat rawan dimanfaatkan menjadi aksi kejahatan digital. Salah satu cara untuk mengatasi kasus kejahatan digital ini adalah dengan menggunakan digital forensik seperti metode NIST (National Institute of Standards and Technology). Tahapan awal yang dilakukan akuisisi data dan melakukan proses ekstraksi hasil akuisisi tersebut. Hasil yang sudah di dapat selanjutnya dianalisis menggunakan algoritma Localization Tampering dan Hashing, algoritma ini untuk mendeteksi adanya perusakan atau manipulasi video digital pada tiap frame dan analisis hash untuk mendeteksi keaslian video. Dalam rekayasa video digital, analisis histogram dapat dilakukan dengan menghitung metrik nilai histogram, yang digunakan untuk membandingkan nilai histogram pada video asli dan video *tampering* serta membuat perbandingan grafik. Hasil perbedaan analisis *frame* menunjukkan hasil video bahwa *frame ke 2* sampai *7* mengalami *attack* sedangkan pada perhitungan histogram nilai centroid video asli dan video *tampering* menghasilkan nilai yang berbeda pada *frame ke tiga* yaitu dengan nilai 124.318 dan *frame ke 7* video mengalami perbedaan nilai yaitu sebesar 105.966 video *tampering* dan 107.456 di video asli. Analisis *hash* pada video *tampering* menghasilkan hash SHA-1 tidak valid, hal ini dapat membuktikan bahwa video tersebut telah dimanipulasi.

Kata kunci: Forensik, Video, Localization Tampering, Rekayasa.

1. Pendahuluan

Perkembangan teknologi yang semakin maju membuat mudahnya merubah atau memodifikasi video sehingga pemalsuan semakin marak. Video digital merupakan media audiovisual yang menggambarkan proses benda bergerak dengan suara [1]. Teknik manipulasi video digital yang semakin berkembang membuat orang yang

melihat merasa kesulitan untuk membedakan antara video asli dan video *tampering* [2]. Video dapat dirusak atau di rubah dengan menggunakan beberapa *tools*, seperti Adobe Premier Pro, Vegas Pro, Corel Video Studio [3]. Kemajuan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban secara global [4]. Hal ini

menyebabkan terjadinya perubahan social, budaya, ekonomi secara signifikan dan berlangsung sangat pesat serta menyebabkan hubungan dunia menjadi tanpa batas. Berbagai aksi kejahatan yang menggunakan teknologi informasi dan internet sebagai medianya disebut dengan istilah *cybercrime* (kejahatan dunia maya) [5]. *Cybercrime* dapat didefinisikan juga sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer yang memiliki kecanggihan teknologi internet [6].

Peningkatan kasus *cybercrime* seperti ujaran kebencian atau *cyberbullying* sangat tinggi di Indonesia, [7]. Pada tahun 2017 sebanyak 3.325 kasus ujaran kebencian yang di tangani oleh Polri. Sementara pada tahun 2016, kasus *cyberbully* yang di tangani Polri sebanyak 1.829 kasus [8][9]. Dari data tersebut membuktikan bahwa kejahatan *cybercrime* dari tahun ke tahun semakin meningkat, untuk menangani hal-hal tersebut diperlukan suatu langkah untuk dapat memberikan kepastian dan penanganan terhadap kasus *cybercrime* [10]. Hal inilah yang menyebabkan munculnya forensik digital yang bertujuan untuk melakukan analisis barang bukti yang akan diproses di persidangan. [11]. Terjadinya kasus *cybercrime* akan meninggalkan jejak aktivitas kriminal [12]. Jejak kriminal ini dapat digunakan sebagai alat bukti elektronik, misalnya *smartphone* dan alat bukti digital berupa video digital [13]. Ada dua metode untuk pengangkatan barang bukti digital pada forensik digital yaitu Teknik *static forensic* dan *live forensic* [14]. Proses akuisisi pada *smartphone* yang tidak aktif atau dalam keadaan mati disebut *static forensic* sedangkan akuisisi *smartphone* secara langsung pada system yang sedang berjalan disebut *live forensic* [15].

Penelitian dengan tema sejenis pernah dilakukan oleh Amirul Putra Justicia. Penelitian ini membahas tentang Analisis Video Forensik dalam Data Penyimpanan. Metode yang digunakan adalah zooming, Lplacian, Sharpening, Contrast brightnes, optical deblurring, exposure, turbulence deblurring, Wiener filter, bilateral filter, unsharp masking dan homomorphic filter. Hasil penelitian tersebut menunjukkan bahwa video asli dan video perusakan membuktikan kebenaran melalui berbagai pengujian antara lain Optical Deblurring, Turbulence Deblurring, Contrast Brightness, Exposure, Laplacian Sharpening, Unsharp Masking, Wiener Filter, Bilateral Filter, Homomorphic Filter dan Temperature Tint dengan *software* AMPED FIVE Ultimate 9010 [16]. Penelitian kedua dengan tema sejenis pernah dilakukan oleh Titi Sari, Imam Riadi. Penelitian yang dilakukan adalah Forensik citra untuk deteksi rekayasa *file* menggunakan teknik *error Level Analysis*. Peneliti menganalisis tingkat kesalahan menggunakan teknik ELA untuk otentikasi pasif dalam forensik citra dengan menggunakan kompresi dan teknik *resize*. Hasil dari penelitian ini adalah metode ELA dapat mendeteksi

manipulasi sebuah citra JPEG dengan kualitas menghasilkan ELA yang jelas dan metode ELA mampu mengevaluasi citra melalui tepi dan variasi halus. Tingkat keputihan dan kecerahan antar tepi harus identik untuk citra asli [17].

Penelitian ketiga dengan tema sejenis pernah dilakukan oleh Jamimamul Bakas, Ruchira Naskar. Penelitian yang dilakukan adalah mengusulkan teknik forensik digital untuk mendeteksi pemalsuan video antar *frame* berdasarkan 3D Convolutional Neural Network (3D-CNN). Hasil dari penelitian ini dengan menerapkan metode 3D CNN mampu mendeteksi penyisipan *frame* penghapusan *frame* dan jenis duplikasi pemalsuan pada video[18]. Penelitian ke empat dengan tema sejenis pernah dilakukan dengan judul *A Video Forensic Famework for the unsupervised analysis of MP\$-like file Container*. Penelitian ini penulis mengusulkan algoritma yang efektif berdasarkan *exponential-Fourier moments* (EFMs) untuk mendeteksi duplikasi video. Metode yang diusulkan dalam penelitian ini mampu secara otomatis mendeteksi manipulasi yang pernah terjadi pada video [19]. Penelitian ke lima dengan tema sejenis lainnya pernah dilakukan dengan judul mendeteksi orisinalitas file video menerapkan metode MD5. Penelitian ini melakukan mendeteksi orisinalitas file video berdasarkan cara kerja algoritma *message Digest* (MD5) dengan menggunakan *hasher pro*. Penelitian ini berhasil malakukan proses deteksi orisinalitas file video dengan format MP4 [20].

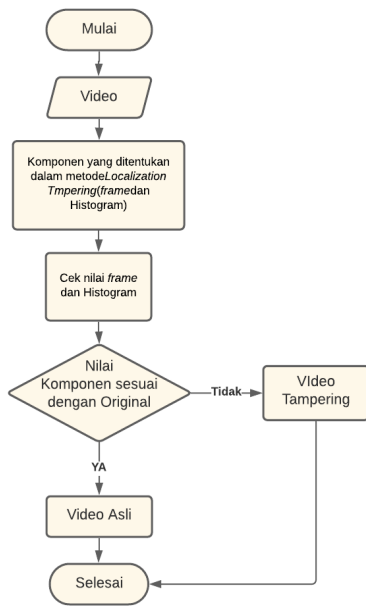
Novelty pada penelitian ini adalah menggunakan proses forensik yang berjalan pada suatu kasus video dengan analisa *frame* menggunakan metode *localization tampering* dan analisa hash menggunakan metode *hashing*. Analisis tampering digunakan untuk mendeteksi adanya perusakan video dan mengetahui keaslian nya. Analisis hash digunakan untuk mendeteksi orisinalitas *file* video dengan menganalisa nilai hash SHA-1 dari video dalam kasus *cybercrime* [21]. Kedua metode tersebut digunakan untuk saling melengkapi dan memperkuat hasil analisis dari temuan barang bukti video.

2. Metode Penelitian

2.1 Alur Penelitian

Tahapan penelitian ini adalah membuat *scene* menggunakan video yang telah disiapkan yang diperoleh dari bukti *smartphone* yang diindikasikan sebagai bukti elektronik dalam kasus *cybercrime*. Video tersebut dilakukan pengecekan nilai *frame* dan histogram, dari hasil pengecekan jika terjadi perbedaan pada nilai maka video tersebut telah mengalami *tampering* dan jika nilai komponennya sama maka video tersebut adalah video asli. Selanjutnya dilakukan analisa *hash* dengan menggunakan *tools* Forevid. Gambar 1

merupakan diagram alir langkah-langkah analisis untuk deteksi keaslian video.

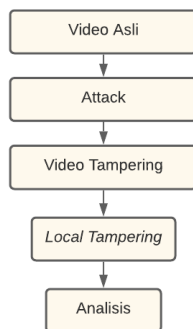


Gambar 1. Diagram alir deteksi *tampering* video

Gambar 1 menunjukkan diagram alir dalam langkah-langkah dalam analisis untuk mendeteksi keaslian video. Proses pertama adalah proses pengecekan nilai *frame* dan histogram dengan menggunakan MATLAB r2017, hasil dari pengecekan jika terjadi perbedaan nilai maka video tersebut mengalami *tampering* dan jika nilai pada komponen sama maka video tersebut merupakan video asli. Hasil dari analisis tersebut maka akan diketahui letak perbedaan *frame* yang telah mengalami *tampering*.

2.2 Proses Simulasi Video

Proses simulasi dimulai dari menyiapkan video sebagai media untuk analisis *tampering*. Biasanya pelaku menghilangkan jejak barang bukti dengan cara memanipulasi video yang bertujuan untuk menghilangkan barang bukti. Proses simulasi video digambarkan pada diagram alir pada Gambar 2.



Gambar 2. Diagram alir proses simulasi video

Gambar 2. Menunjukkan proses simulasi video *tampering* menggunakan *attack zooming, cropping, grayscale, dan*

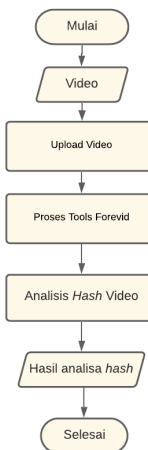
rotation. Video asli dilakukan manipulasi *attack* menjadi video *tampering* dengan cara *zooming, cropping, grayscale, dan rotation* yang selanjutnya akan dilakukan analisis dengan metode *localization tampering* pada video asli dan video *tampering*.

Analisis pada video dengan menggunakan algoritma K-Means ini menggunakan nilai pixel pada tiap *frame* video dalam perhitungan *clustering*. Rumus algoritma K-Means adalah:

$$D_{L1}(x_2, x_1) = |x_2 - x_1|_1$$

$$= \sqrt{\sum_{j=1}^p (X_{2j} - X_{1j})^2} \quad (1)$$

Analisis *frame* video asli dan video manipulasi menggunakan *tools* Matlab r2017a untuk menentukan nilai RGB pada tiap *frame*, dan untuk menentukan centroid awal dengan cara mengambil nilai pixel dari RGB, jarak antar cluster atau kelompok. Proses analisis *hash* video digambarkan pada Gambar 3.



Gambar 3. Diagram Alir Analisis *hash*

Gambar 3 menunjukkan diagram alir dalam proses analisis *hash* SHA-1 dengan menggunakan *tools* Forevid. Fungsi hash adalah metode untuk mengakses record secara langsung dalam sebuah tabel dengan melakukan konversi aritmatika pada sebuah *key*, *key* tersebut muncul pada tabel dalam bentuk nilai atau string, dan nilai atau string tersebut menjadi alamat pada tabel [22]. *Secure hash Algorithm -1* (SHA-1) merupakan fungsi hash satu arah yang dianggap aman oleh National Institute of Standards and Technology (NIST), dikarenakan secara pengolahan komputasi pesan yang dihasilkan SHA-1 tidak dapat menghasilkan hasil yang sama. SHA dapat dianggap sebagai kelanjutan pendahulunya MD5 dan dapat dikatakan aman karena dirancang sedemikian rupa sehingga secara komputasi tidak mungkin menemukan string yang berkoresponden dengan *message Digest* yang diberikan [3]. *Hashing* tersebut bertujuan untuk menjaga integritas data yang berhubungan dengan penjagaan dari

perubahan data secara tidak sah. Untuk menjaga integritas data dari gangguan-gangguan seperti penyisipan, penghapusan, dan pensubstitusian data lain kedalam data yang sebenarnya, sedikit saja file tersebut di rumah maka nilai *hash* akan berubah [23].

3. Hasil dan Pembahasan

3.1 Akuisisi Barang Bukti Digital

Penelitian ini menggunakan *Software* dan *Hardware* untuk mendukung proses forensic. Tahapan ini merupakan proses perencanaan perangkat lunak dan perangkat keras yang akan digunakan serta langkah-langkah yang akan diambil dalam proses penelitian. Agar proses penelitian dapat berjalan dengan lancar maka harus dibuat perencanaan, termasuk menentukan alat-alat yang akan digunakan dalam proses penelitian agar diperoleh hasil yang efektif. *Software* dan *hardware* yang digunakan adalah sebagai berikut.

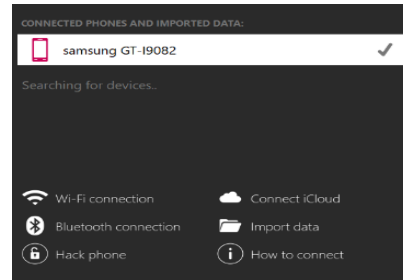
- 1) *Software*
 MOBILedit Forensic Express
 HashMyFiles
 Matlab r2017a
- 2) *Hardware*
 Intel® Core™ i3-234M CPU @2.30Hz
 RAM 8 GB
 NVIDIA GeForce 710m
 SSD 120 GB
 Samsung Galaxy Grand Duos

Pada proses pertama yaitu *Collection* dengan menggunakan barang bukti yang sudah disiapkan yaitu 1 buah video asli dan 1 buah video yang telah dimanipulasi. *Smartphone* yang digunakan adalah Samsung Galaxy Grand Duos dengan system android 4.4.4 KitKat. Bahan yang digunakan seperti gambar 4.



Gambar 4. *Smartphone* yang digunakan

Gambar 4 menunjukkan *smartphone* yang digunakan dalam penelitian ini. Setelah mendapatkan barang bukti tersebut maka selanjutnya dilakukan tahap *Examination*. Tahap *examination* meruakan tahap pemeriksaan pengambilan data dan *backup* untuk menjaga keaslian barang bukti dari unit *smartphone* dengan menggunakan *tools* forensic yaitu menggunakan *software* MOBILedit Forensic Express. Proses akuisisi data seperti pada gambar 5.



(a)

| Case Label: Forensic-ACTOFORMS | Case Evidence Number | Device Label |
|--------------------------------|----------------------|--------------|
| Table of Contents | | |
| Screenshots of Report Settings | | 4 |
| List of Selected Applications | | 4 |
| Summary | | 5 |
| Deleted Data | | 6 |
| Applications | | 7 |
| WhatsApp | | 7 |
| Contacts | | 7 |
| Groups | | 9 |
| Conversations | | 10 |
| Messages | | 42 |
| Web Sessions | | 120 |
| Stored Media Files | | 121 |
| Stored Images | | 121 |
| Stored Video | | 130 |
| List of unopened files | | 130 |
| Application List | | 131 |
| Applications Filesystem | | 132 |
| Data Extraction Log | | 138 |

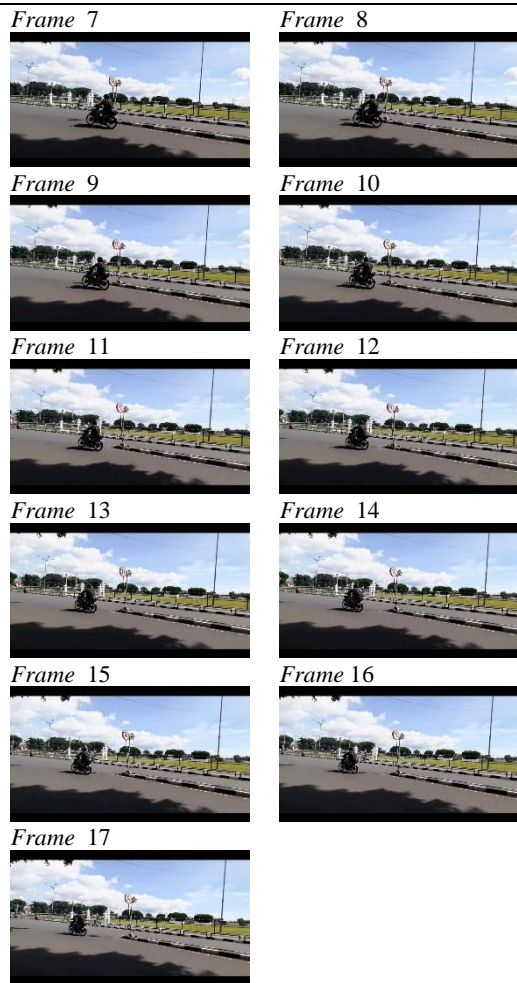
(b)

Gambar 5. Proses ekstraksi pada MOBILedit Forensic

Gambar 5 menampilkan alat forensic yang digunakan untuk proses ekstraksi dan *backup* menggunakan MOBILedit Forensic Express. Proses ini memakan waktu lama, tergantung dari kapasitas penyimpanan *smartphone* yang digunakan, serta hasil yang diperoleh dari proses akuisisi data *smartphone* ditampilkan dalam bentuk file jenis *disc image* dan folder yang berisi data hasil ekstraksi dari *smartphone*. Proses selanjutnya adalah analisis *frame-by-frame*. Menggunakan algoritma K-means yaitu dengan menampilkan cluster atau data RGB, melakukan analisis nilai piksel pada hasil ekstraksi video asli dan video olahan K-means, yaitu dengan menampilkan *clustering* atau data RGB. Hasil video yang di dapat dari proses ekstraksi seperti pada Tabel 1

Tabel 1. Video yang di dapat dari hasil ekstraksi

| Bahan Video (Perframe) | |
|------------------------|---------|
| Frame 1 | Frame 2 |
| | |
| Frame 3 | Frame 4 |
| | |
| Frame 5 | Frame 6 |
| | |



Tabel 1 adalah video yang di dapat dari hasil ekstraksi menggunakan MOBILEdit Forensic Express, yaitu sebuah video MP4 yang terdiri dari 17 *frame*.

3.2 Analisis Pendeteksian

Tahap awal dilakukan analisis Nilai pixel warna pada video asli dan video *tampering*. Hasil analisis dapat dilihat pada table 2.

Tabel 2. Nilai Pixel Warna

| Frame | Video Asli | | | video manipulasi | | |
|-------|------------|-------|------|------------------|-------|------|
| | red | green | blue | red | green | blue |
| 1 | 117 | 122 | 131 | 116 | 121 | 130 |
| 2 | 117 | 123 | 131 | 117 | 121 | 130 |
| 3 | 118 | 123 | 131 | 138 | 143 | 149 |
| 4 | 118 | 123 | 131 | 117 | 122 | 130 |
| 5 | 119 | 123 | 131 | 118 | 122 | 130 |
| 6 | 118 | 123 | 131 | 117 | 122 | 130 |
| 7 | 118 | 122 | 130 | 117 | 121 | 129 |
| 8 | 118 | 123 | 130 | 117 | 121 | 129 |
| 9 | 118 | 122 | 130 | 117 | 121 | 129 |
| 10 | 118 | 123 | 130 | 118 | 122 | 129 |
| 11 | 119 | 124 | 130 | 118 | 122 | 130 |
| 12 | 120 | 124 | 130 | 119 | 122 | 130 |
| 13 | 120 | 124 | 130 | 119 | 122 | 129 |
| 14 | 120 | 124 | 130 | 120 | 123 | 130 |

| | | | | | | |
|----|-----|-----|-----|-----|-----|-----|
| 15 | 121 | 125 | 131 | 120 | 124 | 131 |
| 16 | 121 | 125 | 131 | 120 | 123 | 130 |
| 17 | 121 | 125 | 131 | 120 | 123 | 130 |

Tabel 2 merupakan nilai hasil analisis nilai pixel pada setiap *frame* video asli dan video manipulasi menggunakan *tools* Matlab r2017a. Untuk menentukan centroid awal dengan cara mengambil nilai pixel dari RGB, jarak antar cluster atau kelompok data–data dihitung menggunakan cara nilai pixel1 data 1 atribut warna R dikurangi nilai centroid awal cluster 1 atribut warna R dan kemudian dipangkat 2, ditambah nilai pixel data 1 warna G dan dipangkatkan 2, nilai pixel pada data 1 atribut B dikurang dengan nilai centroid awal cluster 1 atribut B selanjutnya di pangkatkan 2. Hasil dari perhitungan tersebut di akarkan.

Video Asli

$$D1 = \sqrt{(117 - 58)^2 + (122 - 61)^2 + (131 - 65)^2} = 107.033$$

$$D2 = \sqrt{(117 - 58)^2 + (122 - 61)^2 + (131 - 65)^2} = 107.033$$

$$D3 = \sqrt{(118 - 59)^2 + (122 - 61)^2 + (131 - 65)^2} = 107.033$$

$$D7 = \sqrt{(117 - 58)^2 + (122 - 62)^2 + (130 - 66)^2} = 107.456$$

$$D15 = \sqrt{(117 - 58)^2 + (112 - 61)^2 + (131 - 65)^2} = 149.125$$

$$D16 = \sqrt{(117 - 58)^2 + (112 - 61)^2 + (131 - 65)^2} = 149.125$$

Video *Tampering*

$$D1 = \sqrt{(116 - 58)^2 + (121 - 61)^2 + (130 - 65)^2} = 106.131$$

$$D2 = \sqrt{(117 - 58)^2 + (121 - 61)^2 + (130 - 65)^2} = 106.480$$

$$D3 = \sqrt{(138 - 69)^2 + (143 - 71)^2 + (149 - 75)^2} = 124.318$$

$$D7 = \sqrt{(117 - 58)^2 + (121 - 60)^2 + (129 - 65)^2} = 105.966$$







$$D15 = \sqrt{(119 - 60)^2 + (122 - 62)^2 + (130 - 65)^2} = 108.138$$

$$D16 = \sqrt{(120 - 60)^2 + (123 - 62)^2 + (130 - 65)^2} = 107.976$$

Hasil diatas merupakan nilai pixel pada video asli dan video *tampering* yang mengalami perbedaan yang sangat signifikan pada nilai pixel RGB. Deteksi frame dapat dilihat dari perbedaan nilai pada pixel, pada D3 video tampering menunjukkan perbedaan nilai yang sangat signifikan yaitu 124.318, nilai tersebut

menunjukkan frame video mengalami *attack zooming*. Pada D7 video mengalami perbedaan nilai yaitu sebesar 105.966 video *tampering* dan 107.456 di video asli, nilai tersebut menunjukkan *frame* pada video mengalami *attack rotation*. analisis deteksi *frame* dapat dilihat pada Tabel 3

Tabel 3. Deteksi *frame* video

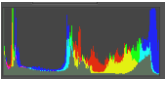
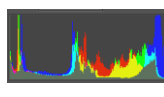
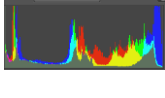
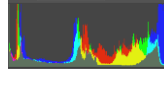
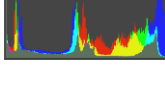
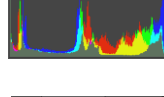
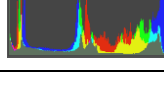
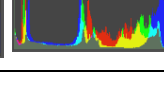
| Attack | Analisis | | Keterangan |
|----------|---|---|--|
| | Asli | Tampering | |
| Cropping |  |  | Frame 2 mengalami <i>crooping</i> karena antar <i>frame</i> tidak sama |
| Zooming |  |  | Terjadi <i>zooming</i> pada <i>frame</i> 3 pada video <i>tampering</i> |
| Rotation |  |  | Terjadi rotasi 180° pada video <i>tampering</i> pada <i>frame</i> ke 7 |

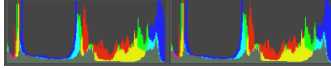
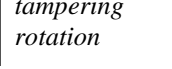
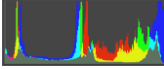
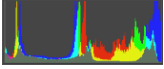
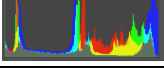
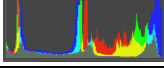
Tabel 3 merupakan hasil deteksi *frame* video *tampering* dan video asli. Terlihat pada *frame* 2 video mengalami *crooping*, karena antar *frame* tidak sama. Pada *frame* ke tiga video mengalami *zooming* karena tampilan *frame* berbeda, dan pada *frame* ke tujuh mengalami *tampering rotation* 180°.

3.3 Analisis perbandingan Histogram

Tujuan dari menganalisa hasil menggunakan histogram ini adalah untuk melihat perubahan citra dilihat dari grafik pada histogram sebelum dan sesudah proses *tampering* sehingga dapat melihat perubahan *frame* secara rinci. Tabel 4 menunjukkan hasil perbandingan histogram R, G dan B pada setiap *frame* video.

Tabel 4 Grafik Histogram

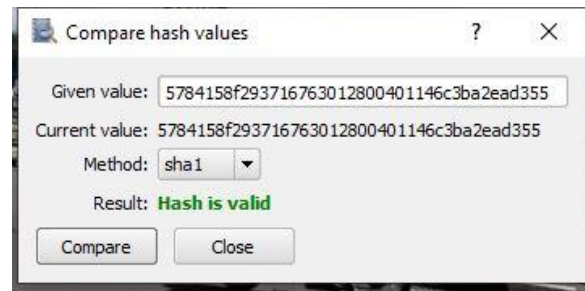
| Frame/ Durasi | Video Asli | Video Tampering | Keterangan |
|------------------|---|---|---|
| 2 |  |  | Frame mengalami <i>tampering cropping</i> |
| 3 |  |  | Terjadi <i>tampering Zooming</i> |
| 4 |  |  | Non <i>Tampering</i> |
| 7 |  |  | Frame mengalami |

| | | | |
|----|--|---|---------------------------|
| 8 |  |  | <i>tampering rotation</i> |
| 12 |  |  | Non <i>tampering</i> |
| 14 |  |  | Non <i>tampering</i> |

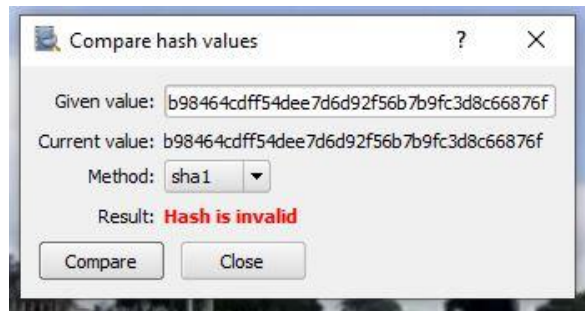
Tabel 4 menunjukkan perbandingan histogram video asli dan video *tampering* pada tiap *frame*. Pada histogram tersebut, jika dilihat secara detail terdapat sedikit perubahan bentuk grafik yang sangat tipis, hal tersebut dikarenakan video mengalami *tampering*. Semakin banyak *tampering* pada *frame*, grafik pada histogram akan semakin banyak berubahannya. Perubahan ekstensi file juga akan berpengaruh terhadap perubahan histogram.

3.4 Analisa Hash

Analisis hash dilakukan dengan menggunakan *tools* forensik Forevid. Gambar 6 dan gambar 7 merupakan hasil Analisa Hash video asli dan video *tampering*.



Gambar 6. Hash video asli



Gambar 7. Hash video *tampering*

Gambar 6 dan gambar 7 merupakan hasil Hash SHA-1 video asli dan video *tampering*. Analisa hash menggunakan *tools* forensik Forevid. Hash SHA-1 merupakan algoritma yang dipakai untuk mengenkripsi data yang terdiri dari 40 bit karakter yang terenkripsi. Fungsi ini digunakan sebagai standar untuk proses identifikasi dan verifikasi bukti digital untuk menjaga

integritas data. Hasil hash SHA-1 pada video asli tanpa pengeditan akan menghasilkan hash yang valid, yang berarti file video belum mengalami *tampering*, sedangkan video *tampering* tidak akan menghasilkan hash yang valid.

4. Kesimpulan

Kesimpulan yang didapat setelah melakukan beberapa tahapan penelitian dengan menggunakan skenario kasus berupa *smartphone*, didapat barang bukti digital berupa video. Dalam rekayasa video digital, analisis histogram dilakukan dengan menghitung metrik nilai histogram, yang digunakan untuk membandingkan nilai-nilai pada video asli dan perusakan video serta membuat perbandingan grafik. Hasil analisis *frame* menunjukkan hasil video bahwa *frame ke 2* sampai *7* mengalami *attack cropping, zooming, dan rotation 180°*. sedangkan pada perhitungan histogram nilai centroid video asli dan video *tampering* menghasilkan nilai yang berbeda pada *frame ke tiga* yaitu dengan nilai 124.318 video *tampering* dan video asli menghasilkan nilai sebesar 107.456. *Frame ke tujuh* mendapatkan nilai yang berbeda yaitu sebesar 105.966 video *tampering* dan 107.456 video asli. Analisis hash pada video *tampering* menghasilkan hash SHA-1 tidak valid, hal tersebut dapat membuktikan bahwa video sudah mengalami *tampering*.

Daftar Rujukan

- [1] J. Xiao, S. Li, and Q. Xu, "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation," *IEEE Access*, vol. 7, pp. 55432–55442, 2019, doi: 10.1109/ACCESS.2019.2913648.
- [2] I. Riadi, A. Yudhana, and W. Y. Sulisty, "Analisis Perbandingan Nilai Kualitas Citra pada Metode Deteksi Tepi," *Rekayasa Sist. dan Teknol.*, vol. 4, no. 2, pp. 345–351, 2020.
- [3] K. D. Wandani and S. Sinurat, "Implementasi Secure Hash Algoritma Untuk Pengamanan Pada File Video," *Maj. Ilm. INTI*, vol. 5, no. 3, pp. 165–168, 2018.
- [4] N. F. Hasan, C. N. Dengen, and D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 1, pp. 20–29, 2020, doi: 10.31849/digitalzone.v11i1.3413.
- [5] Y. Fernando, "Identifikasi Ancaman PCI (Positif Clandestine Intelligence) Berbentuk Cyber Terrorism Terhadap Keamanan Nasional," no. 1, pp. 31–40, 2019.
- [6] M. Rifauddin and A. N. Halida, "Waspada Cybercrime dan Informasi Hoax pada Media Sosial Facebook," *Khazanah al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 6, no. 2, p. 98, 2018, doi: 10.24252/kah.v6i2a2.
- [7] F. P. Ambarita, "Penanggulangan Tindak Pidana Terorisme," *Binamulia Huk.*, vol. 7, no. 2, pp. 141–156, 2018, doi: 10.37893/jbh.v7i2.29.
- [8] E. Chintia, R. Nadiyah, H. N. Ramadhani, Z. F. Haedar, A. Febriansyah, and N. A. Rakhmawati S.Kom., M.Sc.Eng, "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *J. Inf. Eng. Educ. Technol.*, vol. 2, no. 2, p. 65, 2019, doi: 10.26740/jieet.v2n2.p65-69.
- [9] T. Yuridis, T. Penerapan, D. A. N. Transaksi, E. Bagi, and P. Tindak, "Juridic Review Of The Application Of Law Number 11 Of 2008 Concerning Information And Electronic Transactions For Criminal Actions Of Hate Achievements (Case Study Perkara Number : 370 / PID . SUS / 2018 / PN . JKT.," pp. 245–262, 2020.
- [10] H. A. Gani and A. W. Gani, "Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No . 11 TAHUN 2008 dan UU No . 19 Tahun 2016," *Pros. Semin. Nas. LP2M UNM - 2019*, no. 11, pp. 121–129, 2019.
- [11] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.
- [12] W. Y. Sulisty, I. Riadi, and A. Yudhana, "Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital," *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.
- [13] J. P. Soepomo, "Analisis Forensik Bukti Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Standards and Technology (Nist)," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.
- [14] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.
- [15] I. Riadi and I. M. Nasrulloh, "Analisis Forensik Solid State Drive (Ssd) Menggunakan Framework Grr Rapid Response Forensic Analysis of Solid State Drives (Ssd) Using the Grr Rapid Response Framework," vol. 6, no. 5, pp. 509–518, 2019, doi: 10.25126/jtiik.201961516.
- [16] A. Putra Justicia, "Analysis of Forensic Video in Storage Data Using Tampering Method," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 328–335, 2018, doi: 10.17781/p002471.
- [17] G. Hendita, A. Kusuma, and I. N. Prawiranegara, "Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash," *Pros. Semin. Nas. Sist. Inf. dan Teknol.*, vol. 3, no. 1, pp. 223–227, 2019.
- [18] J. Bakas and R. Naskar, "A Digital Forensic Technique for Inter-Frame Video Forgery Detection Based on 3D CNN," *Int. Conf. Inf. Syst. Secur.*, pp. 304–317, 2018, [Online]. Available: https://doi.org/10.1007/978-3-030-05171-6_16.
- [19] M. Iuliani, D. Shullani, M. Fontani, S. Meucci, and A. Piva, "A Video Forensic Framework for the Unsupervised Analysis of MP4-Like File Container," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 635–645, 2019, doi: 10.1109/TIFS.2018.2859760.
- [20] E. S. Nasution, "Mendeteksi Orisinalitas File Video Menerapkan Metode Md5," vol. 3, pp. 156–163, 2019, doi: 10.30865/komik.v3i1.1583.
- [21] W. Zhang, X. Tang, Z. Yang, and S. Niu, "Multi-scale segmentation strategies in PRNU-based image tampering localization," *Multimed. Tools Appl.*, vol. 78, no. 14, pp. 20113–20132, 2019, doi: 10.1007/s11042-019-7288-y.
- [22] H. Sembiring, S. Utara, F. Y. Manik, S. Utara, and S. Utara, "Penerapan Algoritma Secure Hash Algorithm (SHA) Keamanan Pada Citra," vol. 4, no. 1, pp. 33–36, 2019.
- [23] D. García-Retuerta, A. Bartolomé, P. Chamoso, and J. M. Corchado, "Counter-terrorism video analysis using hash-based algorithms," *Algorithms*, vol. 12, no. 5, pp. 1–9, 2019, doi: 10.3390/a12050110.