Vol. 3, No. 1, Juni 2022, hal. 43-51

p-ISSN: 2723-567X
e-ISSN: 2723-5661

Jurnal Computer Science and Information Technology (CoSciTech)

http://ejurnal.umri.ac.id/index.php/coscitech/index

Analisis digital forensik keaslian video rekaman CCTV menggunakan metode *localization tampering*

Desti Mualfah[*1], Yoze Rizki[2], Meiriladiwis Gea[3]
Email: [1]destimualfah@umri.ac.id, , [2]yozerizki@umri.acid, [3]150401096@student.umri.acid

[123]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau

Diterima: 05 April 2020 | Direvisi: 05 Mei 2020 | Disetujui: 27 Mei 2020

Abstrak

Video merupakan salah satu barang bukti yang sah apabila proses penanganan sesuai dengan prosedur digital forensik. *Closed Circuit Television* merupakan salah satu sumber video yang sering dijadikan sebagai barang bukti otentik di persidangan. Keaslian video menjadi hal yang sering diragukan oleh pihak tertentu. Untuk itu, penelitian ini membahas tentang cara mendeteksi keaslian video sebagai barang bukti digital dengan cara membandingkan file video asli dan file video tampering hasil *attack frame addition*, dan *attack frame delection*. *Tools* mediainfo digunakan untuk menganalisis metadata dan metode *localization tampering* digunakan untuk mendeteksi *frame* keberapa terjadi manipulasi. *Localization tampering* yaitu menganalisis *frame by frame*, menghitung histogram dan menampilkan grafik histogram. Berdasarkan hasil analisis metadata file video asli dan file video *tampering* menampilkan informasi yang berbeda yang artinya video tersebut telah dimanipulasi. Selanjutnya, menganalisis video dengan metode *localization tampering* untuk mengetahui lokasi pada *frame* video yang telah terjadi manipulasi. Dari hasil analisis memberikan informasi yang berbeda baik dari perhitungan nilai RGB maupun grafik histogram.

Kata kunci: Bukti Digital, Video CCTV, Tampering, Frame, Histogram

Digital forensic analysis of CCTV video authenticity using tampering localization method

Abstract

Video is one the valid evidence if the handling process is in accordance with digital forensic procedures. Closed circuit television is a video sourse that is often used as authentic evidence in court. The authenticity of the video is something that is often doubted by certain parties. For this reason, this discusses how to detect the authenticity of video as digital evidence by comparing the original video files and tampering video files resulting from attack frame addition and attack frame delection. The media info tool is used to analyze the metadata and the localization tampering method is used to detect the frame where manipulation occurs. Localization tampering analyzes frame by frame, calculates as histogram and displays a histogram graph. Based on the results of the metadata analysis of the original video file and the video file tampering, it displays different information, which means that the video has been manipulated. Next, analyze the video with the localization tampering method to display the location on the video frame where manipulation has occurred. From the analysis results provide different information both from the calculation of the RGB value and the histogram graph.

Keywords: *Digital Evidence, Video CCTV, Tampering, Frame, Histogram*

1. PENDAHULUAN

Teknologi informasi telah mengubah perilaku dan peradaban manusia secara global yang mengharuskan setiap individu memasuki era baru. Kejahatan dan kriminalitas semakin meningkat dengan memanfaatkan alat elektronik dan digital, seperti alat keamanan CCTV (*closed circuit television)* [1], *handycam, handphone* dan *smartphone*, dan alat elektronik lain yang memiliki fitur video, merekam, dan menyimpan data pelaku.

Contoh kasus tindak kejahatan yang menggunakan rekaman CCTV sebagai barang bukti digital yaitu meninggalnya Wayan Mirna salihin pada 6 januari 2016 silam yang melibatkan Jessicca kumala wongso sebagai tersangka utama. Pada kasus tersebut barang bukti berupa USB flashdisk yang berisi rekaman video CCTV hasil ekstrasi dari CCTV pada cafe olivier. Pada sidang kasus Wayan mirna salihin yang paling disoroti adalah keaslian rekaman video CCTV tersebut. AKBP Muhammad Nuh Al-Alzahar adalah ahli forensik mabes polri mengatakan, rekaman tersebut telah melalui prosedur penanganan barang bukti digital forensik dan dianalisis dengan empat metode analisis yaitu analisis Hash, metadata, Frame, dan bit rate histogram sehingga keasliannya telah teruji. Dari hasil rekaman video CCTV itu Jessica kumala wongso ditetapkan sebagai tersangka dan dinyatakan bersalah. [2]

Fakta masalah yang sering dipertanyakan dalam lingkup keamanan CCTV ialah keaslian video yang didapatkan, maka dari itu diperlukan proses autentifikasi video sebelum dijadikan barang bukti digital [3]. Selain itu, banyak video *software editing* video yang dapat digunakan setiap orang untuk mengedit video dengan maksud dan tujuan yang berbeda, sehingga menyulitkan investigasi dalam membedakan video asli dan video yang telah dimanipulasi. Seseorang biasanya merusak serta mengubah *frame* video dengan berbagai cara untuk kepentingan tertentu. Penjahat sering dibebaskan karena barang bukti video yang menunjukkan kejahatan mereka, tidak bisa dijadikan barang bukti atau telah dimanipulasi.

Salah satu editing video berupa *tampering* yang menyisipkan objek tertentu ke dalam sebuah video, objek yang disisipkan dapat berupa rangkaian *frame* dari video yang sama atau berbeda, atau rangkaian potongan *frame* lain dari video yang sama atau berbeda, atau sebuah gambar disisipkan ke dalam beberapa rangkaian frame [4][5]. Untuk mendeteksi keaslian sebuah video diklasifikasi menjadi dua yaitu *tampering detection* dan *localization tampering*. Tampering detection adalah metode mendeteksi integritas suatu video tanpa menunjukan bagian yang telah dimanipulasi, sedangkan localization tampering adalah metode yang menunjukan bagian video yang telah dimanipulasi [6].

Kasus video CCTV yang diragukan keasliannya dapat merugikan orang lain maka diperlukan sebuah cara yang diharapakan untuk dapat membedakan video asli dan video manipulasi menggunakan metode *localization tampering* dengan teknik *frame by frame* dan perhitungan nilai *histogram* serta menampilkan grafik histogramnya untuk mengetahui *frame* yang telah terjadi perubahan pada video untuk mengetahui metadata autentikasinya.

2. METODE PENELITIAN

Adapun alur penelitian yang direncanakan dalam penelitian ini seperti pada ilustrasi berikut:

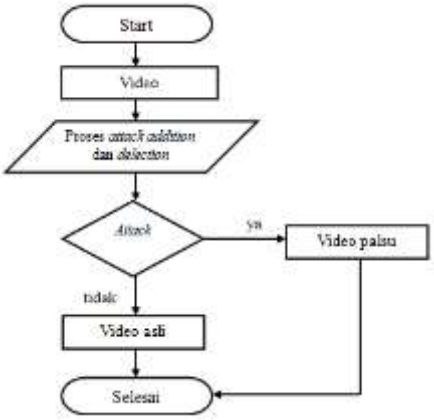
Gambar 1. Alur Penelitian

Untuk membantu proses investigasi forensik, maka membutuhkan suatu metode agar pada saat melakukan penyelidikan, proses investigasi menjadi lebih terstruktur.

3. HASIL DAN PEMBAHASAN

3.1. Simulasi Video

Pembuatan skenario dan implementasi skenario dijalankan untuk mendapatkan barang bukti digital. Pada tahap ini CCTV digunakan sebagai alat perekam dalam mendapatkan video, hasil rekaman video CCTV dipindahkan dari DVR ke flashdisk, kemudian dipindahkan dari flashdisk ke laptop. Langkah selanjutnya adalah menggandakan video tersebut menjadi dua, video pertama merupakan video asli dan video kedua merupakan video hasil *copy* yang digunakan sebagai bahan simulasi. Video hasil *copy* dilakukan *attack addition* dan *attack delection* yang bertujuan untuk mendapatkan video manipulasi [7]. Proses simulasi dapat dilihat pada gambar 2 berikut ini :



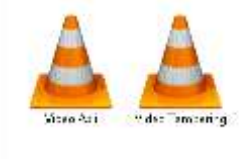
Gambar 2: Simulasi Video

Pada tahap ini hanya *attack addition* dan *attack delection* yang digunakan agar fokus pada letak titik terjadinya manipulasi pada setiap *frame* video berdasarkan nilai pixel RGB. *Attack frame shuffling* adalah kejahatan merubah urutan *frame* pada video, frame rate adalah kejahatan mempercepat laju setiap *frame* dan *attack transcoding* adalah mengubah kode video ke kode video lain. *Frame shuffling*, *transcoding* dan *frame rate* merupakan *attack* yang tidak berhubungan nilai RGB. Selanjutnya adalah *attack* spacial merupakan kejahatan merubah isi video seperti mengubah warna, memperbesar area tertentu dan lain-lain, telah gunakan pada penelitian sebelumnya.

3.2. Investigasi Digital Forensik

3.2.1 *Identification*

Pada tahap ini peneliti mengidentifikasi dua file video yang telah diberi nama video asli dan video tampering. Kedua video tersebut diambil dan dijadikan barang bukti. Pada gambar 3 terlihat dua video pertama dinamakan video asli merupakan video yang belum dimanipulasi, sedangkan video kedua dinamakan video tampering merupakan video yang telah dimanipulasi. File video asli dengan format file MPEG-4, kode file isom(isom/iso2/avc1/mp41), size file 44,4 MB, durasi 1 menit 0 detik, bit rate 6203 kb/s, *encoder bit rate* Lavf58.12.100, *frame rate* 30 fps, resolusi 1920x1080 *pixels*, *display aspect ratio* 16:9, dan seterusnya, sedangkan file video *tampering* dengan format file MPEG-4, kode file isom(isom/iso2/avc1/mp41), size file 44,8 MB, durasi 1 menit 0 detik, *bit rate* 6253 kb/s, *encoder bit rate* Lavf58.12.100, *frame rate* 30.032 fps, resolusi 1920x1080 *pixels*, *display aspect ratio* 16:9, dan seterusnya. Kedua video tersebut akan dijadikan bahan analisis untuk mengetahui letak terjadi tampering pada video tersebut.



Gambar 3: Barang Bukti Video

3.2.2 *Collection*

Pada tahap ini digunakan untuk mengumpulkan semua barang bukti yang berhubungan dengan investigasi. Peneliti telah mengambil dua video yang dijadikan sebagai barang bukti.

3.2.3 *Examination*

Tahap memeriksa (*examination*) merupakan proses memeriksa semua barang bukti yang telah dikumpulkan dari tempat kejadian perkara. Untuk memastikan barang bukti yang didapatkan asli dilakukan teknik hashing menggunakan hash MD5 dengan tujuan mengetahui derajat kesamaan pada sumber asli dan hasil duplikat.

Gambar 4: Hasil Nilai Hash MD5 file video asli

Gambar 4 merupakan nilai *hashing* pada file video asli yang dijadikan barang bukti sebagai bahan penelitian. selanjutnya adalah pengecekan nilai *hashing* pada file video *tampering* seperti pada gambar 5 dibawah ini.

Gambar 5: Hasil Nilai Hash MD5 file video *tampering*

Gambar 5 merupakan nilai *hashing* pada file video tampering yang dijadikan barang bukti sebagai bahan penelitian. Pada gambar 4 diatas menunjukan nilai *hash* pada file video asli adalah 6f3d46b53edea5c32adb43ad889d8ac3 dan pada gambar 5 diatas hasil *hash* MD5 file video *tampering* adalah 7770a1a226d249b1afd00519ab5d7ccb. Dari hasil tersebut dapat dilihat perbedaan sehingga dapat disimpulkan terjadi *tampering* pada file video tersebut.

3.4 Analysis

Pada tahap ini, peneliti menggunakan metode *Localization Tampering*. *Localization tampering* merupakan metode mendeteksi bagian video yang telah diganti, ditambah, dan dihapus oleh seseorang untuk kepentingan tertentu. Tujuan utama metode *lozalization tampering* adalah untuk mengetahui *frame* keberapa yang telah dimanipulasi. Langkah-langkah menganalisis video menggunakan metode *localization tampering* adalah seperti yang peneliti uraikan di bawah ini.

3.4.1 Analisis Metadata

Analisis metadata berguna untuk mengetahui informasi terkait dengan video seperti format, durasi, *size*, *frame* dan sebagainya. Hasil metadata video asli dan video *tampering* dibandingkan, jika ada perbedaan maka bisa dipastikan salah satunya video *tampering*. Pada penelitian ini, peneliti menggunakan *tools* Mediainfo untuk mengetahui metadata video asli dan video manipulasi. Berikut merupakan gambar hasil metadata video asli dan video tampering yang dihasilkan melalui *tools* Mediainfo.

Gambar 6: Metadata Bukti Digital Video Asli

Gambar 7: Metadata Bukti Digital Video Tampering

3.4.1 Analisis Metadata

Pada analisis frame, masing-masing video diesktrak menjadi bagian-bagian frame berupa file gambar dengan format jpg. Pada analisis ini peneliti menggunakan bantuan tools VLC media player. Video asli dan tampering masing-masing diekstrak menjadi 33 frame seperti terlihat pada gambar 8 frame asli dan gambar 9 frame tampering di bawah ini :

Gambar 8: *Frame* Asli

Gambar 9: *Frame Tampering*

Pada gambar 9 merupakan salah satu *frame* barang bukti file video *tampering*. Setiap *frame* akan dianalisis nilai RGB nya. Untuk mengetahui nilai RGB, peneliti menggunakan *tools* JPEGSnoop dimana *tools* ini dapat menampilkan info nilai RGB dari suatu gambar atau citra. Nilai RGB didapatkan berdasarkan nilai rata-rata *brightes pixel* dalam satu *frame* terlihat seperti pada tabel 1 di bawah ini.

Tabel 1: Nilai RGB Frame Bukti Digital

No.	Frame	Video Asli			Video Tampering		
		R	G	B	R	G	B
1	00001	234	233	199	234	233	199
2	00051	231	230	190	231	230	190
3	00101	246	231	178	246	231	178
4	00151	241	231	191	241	231	191
5	00201	239	223	189	239	223	189
6	00251	234	233	175	255	238	188
7	00301	233	227	191	207	228	233
8	00351	237	231	191	207	228	233
9	00401	237	231	191	254	233	173
10	00451	233	227	189	253	227	191
11	00501	241	225	164	237	231	191
12	00551	225	224	220	234	226	189
13	00601	240	226	167	241	227	178
14	00651	244	225	170	231	220	171
15	00701	244	223	171	231	227	168
16	00751	229	227	227	238	226	162
17	00801	244	231	178	233	226	188
18	00851	241	225	167	249	222	166
19	00901	239	229	180	255	224	167
20	00951	243	222	169	228	226	225
21	01001	239	231	181	228	226	225
22	01051	239	231	181	239	223	188
23	01101	235	228	188	239	233	237
24	01151	231	227	168	238	226	184
25	01201	237	228	168	240	226	188
26	01251	233	224	167	248	230	182
27	01301	245	222	168	227	224	178
28	01351	235	224	167	238	225	168
29	01401	235	234	167	209	230	245
30	01451	228	228	235	252	228	189
31	01501	239	231	188	238	227	189
32	01551	238	242	199	255	231	172
33	01601	237	229	168	250	238	190

Setelah mengetahui nilai RGB masing-masing frame, akan dilakukan analisis nilai RGB menggunakan algoritma K-means dengan cara menampilkan clustering atau data RGB. Analisis frame dengan cara frame by frame menggunakan rumus di bawah ini. Untuk menentukan nilai tengah (centroid) menggunakan rumus di bawah ini.

$$V = \sum_{\frac{i=1}{n}}^{n} xi \qquad (1)$$

Keterangan :

V : nilai tengah
N : jumlah cluster
I : jumlah data (1,2,3, dst)
Xi : data ke i

Agar mudah dipahami dari rumus di atas untuk menentukan titik pusat (centroid) masing-masing frame dapat disederhanakan dengan cara membagi dua tiap nilai R, G, dan B. Misalnya pada frame 1 file video asli nilai R=234, G=233, dan B=199, nilai tersebut dibagi dua untuk mendapatkan titik pusat tiap cluster sehingga titik pusat R=117, G=116.5, dan B=99.5. Begitu juga untuk mencari titik pusat frame 1 file video tampering. Untuk hasil perhitungan titik pusat cluster frame-frame file video asli dan file video tampering dapat dilihat pada tabel 2 di bawah ini.

Tabel 2: Nilai *Centroid Cluster* RGB Bukti Digital

No.	Frame	Video Asli			Video Tampering		
		R	G	B	R	G	B
1	00001	117	116.5	99.5	117	116.5	99.5
2	00051	115.5	115	95	115.5	115	95
3	00101	123	115.5	89	125	115.5	89
4	00151	120.5	115.5	95.5	120.5	115.5	95.5
5	00201	119.5	111.5	74.5	119.5	111.5	74.5
6	00251	117	116.5	87.5	117.5	114	94
7	00301	116.5	113.5	95.5	103.5	114	117.5
8	00351	118.5	115.5	95.5	103.5	114	117.5
9	00401	118.5	115.5	95.5	117	116.5	86.5
10	00451	116.5	113.5	94.5	116.5	113.5	95.5
11	00501	120.5	112.5	82	118.5	115.5	95.5
12	00551	112.5	112	114	117	113	94.5
13	00601	120	113	83.5	120.5	113.5	89
14	00651	122	112.5	85	113.5	114	85.5
15	00701	122	112.5	85.5	115.5	113.5	84
16	00751	114.5	113.5	118.5	119	113	81
17	00801	117	115.5	89	116.5	113	94
18	00851	121.5	112.5	83.5	122.5	111	83
19	00901	119.5	114.5	90	117.5	112	83.5
20	00951	121.5	111	81.5	114	113	112.5
21	01001	119.5	115.5	90.5	114	113	112.5
22	01051	119.5	113.5	90.5	119.5	111.5	93
23	01101	117.5	114	94	119.5	116.5	98.5
24	01151	115.5	113.5	84	119	113	82
25	01201	118.5	113	84	120	113	84.5
26	01251	116.5	112	83.5	123	115	91
27	01301	122.5	111	84	118.5	112	88
28	01351	117.5	112	83.5	119	112.5	84.5
29	01401	117.5	112	83.5	104.5	115	117.5
30	01451	114	113	112.5	116	114	94.5
31	01501	119.5	111.5	94	116.5	113.5	94.5
32	01551	119.5	116	99.5	117.5	116.5	86
33	01601	118.5	112.5	81.5	117.5	114	85

Langkah selanjutnya adalah menentukan jarak antara cluster dengan rumus seperti di bawah ini :

$$D_{L1}(x_2, x_1) = \|x_{2-} x_1\| = \sqrt{\sum_{j=1}^{p} (x_{2j} - x_{1j})^2} \qquad (2)$$

Keterangan :

DL1 : jarak *cluster*

X2 : data ke 1

X1 : titik pusat data

$\|x_{2-} x_1\|$: nilai mutlak dikurang nilai titik pusat

$\sqrt{\sum_{j=1}^{p} (x_{2j} - x_{1j})^2}$: akar dari penjumlahan hasil pengurangan antara data dengan titik pusat data ke j dimana j dimulai dari 1.

Dari rumus di atas dapat disederhanakan untuk menghitung jarak anggota cluster atau kelompok data dengan cara nilai pixel data 1 atribut warna R dikurangi nilai centroid awal cluster 1 atribut warna R kemudian dipangkatkan 2, ditambah nilai pixel data 1 atribut warna G dikurangi dengan nilai centroid awal cluster 1 atribut warna G kemudian di pangkatkan 2, nilai pixel data 1 atribut warna B dikurangi dengan nilai centroid awal cluster 1 atribut warna B kemudian dipangkatkan 2, kemudian hasil jumlah tersebut di akarkan. Hasil perhitungan nilai pixel RGB video asli dibandingkan nilai pixel RGB video manipulasi setiap frame, jika mengalami perbedaan maka salah satunya adalah video hasil manipulasi. Nilai pixel RGB yang paling besar merupakan video manipulasi. Analisis frame bertujuan untuk mengetahui frame keberapa terjadi tampering. Di bawah ini merupakan contoh perhitungan jarak antar titik pusat:

$$\text{D1A}=\sqrt{(234 - 117)^2 + (233 - 116.5)^2 + (199 - 99.5)^2}=192.8. \qquad (3)$$

Nilai 192.8 merupakan jarak titik pusat cluster RGB frame 1 video asli. Selanjutnya menghitung nilai jarak titik pusat cluster RGB frame 1 video tampering.

$$\text{D1T}=\sqrt{(234 - 117)^2 + (233 - 116.5)^2 + (199 - 99.5)^2}=192.8. \qquad (4)$$

Dari hasil perhitungan jarak titik pusat cluster frame 1 video asli dan video tampering sama maka dapat disimpulkan frame 1 tidak terjadi tampering. Hasil jarak antar titik pusat lengkap dapat dilihat pada tabel 3 dibawah ini.

No.	Frame	Video Asli	Video Tampering
		Jarak Centroid	Jarak Centroid
1	00001	192.8	192.8
2	00051	188.7	188.7
3	00101	190.8	190.8
4	00151	192.3	192.3
5	00201	179.6	179.6
6	00251	186.9	188.8
7	00301	188.6	193.7
8	00351	191.1	193.7
9	00401	191.1	186.4
10	00451	188.1	188.6
11	00501	184.1	191.1
12	00551	195.4	188.1
13	00601	184.8	187.9
14	00651	186.5	183.4
15	00701	186.7	182.4
16	00751	200.1	183.0
17	00801	186.9	182.7
18	00851	185.4	185.0
19	00901	188.4	182.5
20	00951	183.6	196.0
21	01001	189.2	196.0
22	01051	189.2	188.0
23	01101	188.8	193.8
24	01151	182.4	183.5
25	01201	184.0	185.2
26	01251	181.9	191.4
27	01301	185.4	185.3
28	01351	182.5	184.3
29	01401	182.5	194.8
30	01451	196.0	188.1
31	01501	188.5	188.1
32	01551	194.0	186.5
33	01601	182.6	184.5

Tabel 3 : Jarak titik pusat *cluster* RGB Bukti Digital

Pada tabel 3 diatas jarak titik pusat cluster dari frame ke 1 sampai dengan frame ke 5 memiliki nilai jarak titik pusat yang sama sehingga bisa disimpulkan bahwa pada frame tersebut belum terjadi tampering. Selanjutnya pada frame 6 sampai dengan frame 33 memiliki nilai jarak titik pusat yang berbeda sehingga bisa disimpulkan bahwa pada frame-frame tersebut telah terjadi *tampering*.

3.4.2 Analisis Histogram

Analisis histogram [9][10] dilakukan dengan cara menghitung matrik pada nilai histogram yang digunakan untuk membandingkan nilai histogram pada video asli dan video tampering berdasarkan nilai pixel setiap frame serta untuk membuat perbandingan grafik.

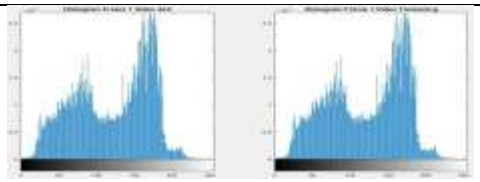
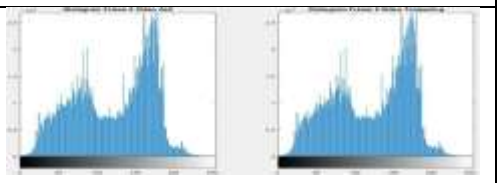
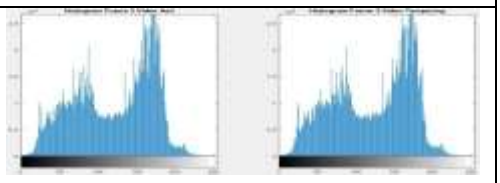
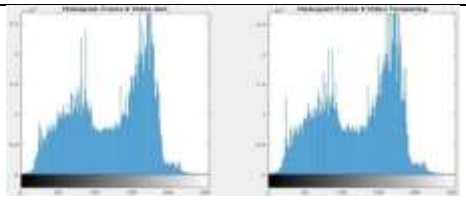
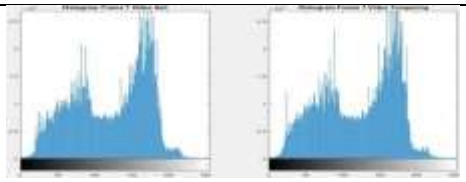
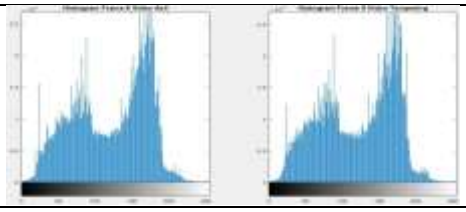
Dalam penelitian ini, frame yang ada memiliki resolusi pixel tinggi yaitu 1920x1080 pixel sehingga untuk perhitungan manualnya tidak bisa dilakukan karena jumlah total keseluruhan pixel yaitu 2.073.600 pixel. Oleh karena itu, peneliti membuat grafik histogram menggunakan bantuan tools pemograman Matlab, dimana Matlab digunakan untuk membuat grafik histogram citra secara langsung. Berikut source code program Matlab untuk menampilkan grafik histogram citra video asli dan video tampering frame 1.

citra 1=imread('frame00001a.jpg'); => kode untuk membaca gambar frame 1 video asli
figure, imshow(citra 1); => kode untuk menampilkan gambar frame 1 video asli
title('Frame 1 Video Asli'); => kode untuk menampilkan judul gambar frame video asli
citra 2=imread('frame00001b.jpg'); => kode untuk membaca gambar frame 1 video tampering
figure, imshow(citra 2); => kode untuk menampilkan gambar frame 1 video tampering
title('Frame 1 Video Tampering'); => kode untuk menampilkan judul gambar frame 1 video tampering
gs1=rgb2gray(citra 1); => kode untuk mengubah gambar RGB menjadi Gray frame 1 video asli
figure, imshow(gs1); => kode untuk menampilkan gambar Gray frame 1 video asli
title('Frame 1 Grayscale Video Asli'); => kode untuk menampilkan judul gambar Gray frame 1 video asli
gs2=rgb2gray(citra 2); => kode untuk mengubah gambar RGB menjadi Gray frame 1 video tampering
figure, imshow(gs2); => kode untuk menampilkan gambar Gray frame 1 video tampering
title('Frame 1 Grayscale Video Tampering'); => kode untuk menampilkan judul gambar Gray frame 1 video Tampering
subplot(1,2,1), imhist(gs1), title('Histogram Frame 1 Video Asli'); => kode untuk menampilkan histogram gambar Gray frame 1 video asli
subplot(1,2,2), imhist(gs2), title('Histogram Frame 1 Video Tampering'); => kode untuk menampilkan histogram gambar Gray frame 1 video asli

Dibawah ini merupakan hasil perbandingan frame bukti digital dari hasil video asli dan video *tampering* yang telah diimplementasikan dapat dilihat pada tabel 4 berikut ini :

Tabel 4: Hasil Perbandingan Frame Bukti Digital

No	*Frame*	Perbandingan *Frame* Bukti Digital	Keterangan

1	*Frame* 1		*Frame* 1 sampai *frame* 3 memiliki grafik yang sama sehingga bisa disimpulkan bahwa pada *frame* tersebut belum terjadi tampering. Seperti terlihat pada gambar disamping.
2	*Frame* 2		
3	*Frame* 3		
4	*Frame 6*		*Frame* 6 sampai dengan *frame* 8 memiliki grafik yang berbeda sehingga bisa disimpulkan bahwa pada *frame* tersebut telah terjadi tampering.
5	*Frame 7*		
6	*Frame 8*		

3.5 Laporan

Penelitian ini menggunakan metode *localization tampering*. Metode ini bisa diterapkan untuk menentukan bagian video yang telah diubah/manipulasi untuk kegiatan forensik. Selain metode *localization tampering* tersebut juga mengggunakan metode *clustering K-Means* [8] untuk mencari nilai jarak antar *cluster pixel* RGB masing-masing frame yang ada. Dan analisis histogram juga memperkuat metode yang digunakan dalam menentukan bagian video yang telah terjadi tampering. Pada penelitian ini, video yang digunakan berasal dari CCTV hasil *simulasi attack addition* dan *delection* yang kemudian dianalisis dengan metode *localization tampering*. Video yang digunakan masing-masing berdurasi 1 menit, dan masing-masing video tersebut memiliki 33 frame. Dari hasil analisis *frame* yang telah dilakukan, frame 1 sampai frame 5 antara *file* video asli dan file tampering memiliki nilai sama sedangkan pada frame 6 sampai frame 33 memiliki nilai yang berbeda antara file video asli dan file video tampering berdasarkan perhitungan algoritma K-means.

Selanjutnya, diperkuat dengan hasil grafik histogram setiap *frame*, dimana pada frame 1 sampai frame 3 antara file video asli dan file tampering memiliki grafik yang sama sedangkan pada *frame* 6 sampai *frame* 8 memiliki grafik yang berbeda antara file video asli dan file video *tampering*. Sehingga bisa disimpulkan pada frame 1 sampai frame 4 antara file video asli dan file tampering belum terjadi tampering sedangkan pada *frame* 5 sampai frame 8 lokasi/*frame* terjadinya *tampering*.

Penelitian ini menggunakan bantuan tools VLC media player yang mengubah video menjadi *frame-frame*, tools MediaInfo yang digunakan untuk mengetahui informasi metadata video, tools MD5 and SHA *checksum* digunakan untuk mengetahui nilai

hashing, tools JPEGSnoop yang digunakan untuk menentukan nilai pixel RGB masing-masing frame, dan tools Matlab yang digunakan untuk membuat grafik perbandingan *histogram* antara frame file video asli dan file video *tampering*.

4. KESIMPULAN

Berdasarkan hasil analisis yang dilakukan peneliti tentang analisis digital forensik keaslian video rekaman CCTV menggunakan metode *Localization Tampering* dapat disimpulkan beberapa hal yaitu: Video yang digunakan masing-masing berdurasi 1 menit, dan masing-masing video tersebut total memiliki 33 *frame*. Dari hasil analisis *frame* yang telah dilakukan, frame 1 sampai frame 3 antara file video asli dan file tampering memiliki nilai sama sedangkan pada frame 6 sampai frame 8 memiliki nilai yang berbeda antara file video asli dan file video tampering berdasarkan perhitungan algoritma K-means. Selanjutnya, diperkuat dengan hasil grafik histogram setiap *frame*, dimana pada *frame* 1 sampai *frame* 3 antara file video asli dan file *tampering* memiliki grafik yang sama sedangkan pada frame 6 sampai frame 8 memiliki grafik yang berbeda antara file video asli dan file video *tampering*. Sehingga bisa disimpulkan pada frame 1 sampai frame 3 antara file video asli dan file *tampering* belum terjadi tampering sedangkan pada frame 6 sampai frame 8 lokasi/*frame* terjadinya tampering.

DAFTAR PUSTAKA

[1] D. Mualfah and R. A. Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 2, pp. 257–267, 2020, doi: 10.31849/digitalzone.v11i2.5174.

[2] N. Irman, "Tinjauan Yuridis Terhadap Putusan Perkara Nomor: 85/PID.B/2012/PN.PWT)," *Pembuktian Alat Bukti Inf. Dan Transaksi Elektron. Dalam Pembobolan Atm*, p. 105, 2013.

[3] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[4] 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.

[5] M. N. O. Sadiku, A. E. Shadare, and S. M. Musa, "Digital Chain of Custody," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 7, p. 117, 2017, doi: 10.23956/ijarcsse.v7i7.109.

[6] D. Y. Sari, "Deteksi Keaslian Video Pada Handycam Dengan Metode Localization Tampering," *J. Online Inform.*, vol. 2, no. 1, p. 10, 2017, doi: 10.15575/join.v2i1.85.

[7] D. M. Suratno, I. Riadi, and Y. Prayudi, "First Respond Framework Untuk Forensik CCTV," *Hacking Digit. Forensics Expo.*, pp. 13–20, 2018.

[8] Sari, D. Y. (2020). Algoritma K-Means Untuk Mendeteksi Frame Pada Video Alsi dan Video Tampering. Teknokom, 3(1), 17-21.

[9] Sholihin, R. A., & Purwoto, B. H. (2015). Perbaikan Citra Dengan Menggunakan Median Filter Dan Metode Histogram Equalization. *Jurnal Emitor*, *14*(2), 1411–8890.

[10] Sinambela, J. M. (2016). Digital Forensik Dan Barang Bukti Rekaman CCTV Kasus Jessica. Retrieved August 9, 2020, from infosec.id website: https://infosec.id/2016/10/digital-forensik-dan-barang-bukti-rekaman-cctv-ka sus-jessica/