Deteksi Keaslian Video Pada Handycam Dengan Metode *Localization Tampering*

Dewi Yunita Sari [1], Yudi Prayudi [2], Bambang Sugiantoro[3]
[1,2] Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia
[3] Teknik Informatika UIN Sunan Kalijaga Yogyakarta
[1]14917116@students.uii.ac.id, [2] prayudi@*uii.ac.id*, [3] bambang.sugiantoro@uinsuka.ac.id

***Abstrak*—Video merupakan barang bukti digital yang salah satunya berasal dari handycam, dalam hal kejahatan video biasanya dimanipulasi untuk menghilangkan bukti-bukti yang ada di dalamnya, oleh sebab itu diperlukan analisis forensik untuk dapat mendeteksi keaslian video tersebut. Dalam penelitian ini di lakukan manipulasi video dengan *attack cropping, zooming, rotation, dan grayscale*, hal ini bertujuan untuk membandingkan antara rekaman video asli dan rekaman video tampering, dari rekaman video tersebut dianalisis dengan menggunakann metode *localization tampering*, yaitu metode deteksi yang menunjukkan bagian pada video yang telah dimanipulasi, dengan menganalisis frame, perhitungan histogram, dan grafik histogram. Dengan *localization tampering* tersebut maka dapat diketahui letak frame dan durasi pada video yang telah mengalami *tampering*.**

Kata kunci*—*Handycam, Histogram, Frame, Tampering, Video

I. PENDAHULUAN

Keberadaan barang bukti sangat penting dalam investigasi kasus-kasus *computer crime* maupun *computer related crime*, karena dengan barang bukti inilah investigator dan analisis forensik dapat mengungkap kasus-kasus yang terjadi dengan kronologis yang lengkap untuk kemudian melacak keberadaan pelaku dan menangkapnya [1].

Salah satu jenis barang bukti yang sering diterima untuk dianalisis lebih lanjut secara digital forensik adalah barang bukti berupa rekaman video, rekaman video tersebut salah satunya berasal dari handycam, handycam merupakan salah satu alat teknologi perekam suara dan gambar yang digunakan masyarakat untuk membuat video dengan mengabadikan momen-momen yang dianggap berharga atau menyenangkan dan digunakan untuk merekam suatu kejadian atau peristiwa-peristiwa penting [1].

Setiap kali video disajikan sebagai barang bukti dalam persidangan pengadilan, diperlukan proses autentifikasi video sebelum dijadikan sebagai barang bukti [2], karena itu video sangat penting untuk dijadikan sebagai sumber utama informasi. Berbagai software *editing* video menyulitkan seseorang untuk membedakan antara video otentik atau video *tampering*.

Berikut ini adalah beberapa contoh peristiwa mengapa mendeteksi pemalsuan video diperlukan: Sebuah frame video dapat dirusak atau dirubah dengan berbagai cara, hal itu digunakan untuk mencemarkan nama baik seseorang. Penjahat sering dibebaskan karena video (yang digunakan sebagai barang bukti), yang menunjukkan kejahatan mereka tidak bisa digunakan karena video tersebut telah dimanipulasi [3].

Untuk membedakan video asli atau video *tampering* maka diperlukan pendeteksian terhadap video tersebut. Metode yang digunakan untuk mendeteksi video secara umum dibedakan menjadi dua kategori: kategori pertama adalah *tampering detection*, yaitu metode deteksi yang hanya mengecek integritas dari video tanpa menunjukkan bagian mana pada video yang telah dimanipulasi. Namun tidak dapat memberikan informasi lokasi mana yang telah dimanipulasi pada video. Kategori kedua adalah *tampering localization*, yaitu metode deteksi yang menunjukkan bagian pada video yang telah dimanipulasi. Berbeda dengan *tampering detection* yang hanya mengecek validasi dari sebuah video, pada metode *tampering localization* ini kita dapat menunjukkan bagian pada video yang telah dimanipulasi. Lokasi manipulasi berupa posisi spasial dalam bentuk koordinat *pixel* dan posisi temporal dalam bentuk urutan frame yang telah dimanipulasi [4].

Penelitian tentang mendeteksi video *tampering* telah banyak dilakukan oleh peneliti sebelumnya, seperti yang dilakukan oleh penelitian [4] menggunakan *localization tampering* untuk mendeteksi video yang telah dimanipulasi, yaitu dengan menyisipkan potongan sejumlah frame tertentu pada sejumlah frame yang lain. Penelitian lain juga dilakukan oleh [3] mendeteksi video dengan dua jenis tampering, yang pertama adalah mendeteksi adanya spatial *copy-move* (duplikasi objek yang sama pada scene yang sama) menggunakan *Histogram Of Gradients* (HOG), yang kedua adalah mendeteksi adanya temporal *copy-move* (menyisipkan objek dari sebuah frame ke frame lain) menggunakan eksploitasi struktur MPEG-2 *Group Of Pictures* (GOP).

Peneliti [5] juga mengungkapkan ada dua pendekatan yang digunakan untuk mendeteksi video, yang pertama mendeteksi otentikasi video dan yang kedua mendeteksi video tampering. Dengan adanya gangguan yang berbeda maka telah dilakukan deteksi pada setiap piksel dari frame video tertentu dan gambar yang menyimpan nilai-nilai data frame. Jadi untuk melakukan distorsi pada video itu

Makalah dikirim: 22 Mei 2017; Revisi: 6 Juni 2017; Diterima: 22 Juni 2017; Publish : 30 Juni 2017

dapat dilakukan dengan penambahan objek dan penghapusan objek pada frame tertentu.

Banyaknya penelitian yang membahas tentang mendeteksi keaslian video, oleh karena itu tema yang di jadikan dalam penelitian ini adalah deteksi keaslian video pada handycam dengan metode *localization tampering*. Video yang digunakan dalam penelitian ini adalah video yang ada didalam handycam dengan format MPG.

Tujuan dalam penelitian ini adalah untuk mendeteksi adanya tampering pada video dengan menggunakan metode *localization tampering* karena untuk menunjukkan frame dan durasi keberapa pada video yang telah mengalami manipulasi dengan cara menganalisis frame dan histogramnya.

II. TINJAUAN PUSTAKA

A. Video

Video adalah teknologi pemrosesan sinyal elektronik mewakilkan gambar yang bergerak. Aplikasi umum dari teknologi video adalah televisi, tetapi dapat juga digunakan dalam aplikasi teknik, saintifik, produksi dan keamanan. Rekaman video bersifat *volatile* artinya rekaman tersebut dapat dengan mudah diubah dan direkayasa, mulai dari yang mudah untuk dikenali hingga yang sulit diketahui. Pertanyaan-pertanyaan dalam persidangan yang berkaitan dengan barang bukti rekaman video adalah tentang keaslian video tersebut oleh dari itu maka dilakukan analisis metadata dan *frame* untuk memastikan keaslian video hingga hal-hal yang berkaitan dengan teknik pembesaran objek pada rekaman video tersebut [1].

Video digital merupakan bagian terpenting multimedia yang paling menarik, dan merupakan peranti powerfull yang membawa pengguna komputer lebih dekat kedunia nyata. Video digital juga merupakan metode yang tepat dan cerdas untuk mengirimkan multimedia kepada audiens yang melihatnya.

B. Handycam

Salah satu alat yang dapat digunakan untuk menghasilkan video digital adalah camcorder, yang digunakan untuk merekam gambar-gambar video dan audio, sehingga sebuah camcorder akan terdiri dari camera dan recorder.

Camcorder terdiri dari 3 komponen:

- Lensa : untuk mengatur banyak cahaya, zoom, dan kecepatan shutter.
- Image : untuk melakukan konversi cahaya ke sinyal electronik video.
- Recorder : untuk menulis sinyal video ke media penyimpanan (seperti magnetic videotape).

C. *Localization Tampering*

Localization tampering yaitu metode deteksi yang menunjukkan bagian pada video yang telah dimanipulasi. Lokasi manipulasi berupa posisi spasial dalam bentuk koordinat pixel dan posisi temporal dalam bentuk urutan frame yang telah dimanipulasi [4].

Video *tampering* adalah proses untuk menyisipkan obyek tertentu ke dalam sebuah video [6]. Obyek yang disisipkan dapat berupa rangkaian *frame* lain 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*.

Tampering digital yang mengalami perubahan dari bentuk aslinya adalah berupa gambar, audio, video, teks, dll. Perubahan tersebut dapat diklasifikasikan sebagai tindakan sengaja atau tidak sengaja. *Tampering* yang disengaja memiliki tujuan yang jahat dengan memodifikasikan konten atau menghapus hak cipta. Disamping itu, tampering yang tidak disengaja merupakan konsekuensi dari dari proses operasional digital, seperti memperbaiki kecerahan, perubahan format, pengurangan ukuran, dan lainnya. Pada signal video teknik *tampering* dapat diklasifikasikan sebagai perubahan spasial dan temporal. Teknik *tampering* spasial disesuaikan dengan perubahan yang dibuat berdasarkan pixel pada *frame*.

Tampering spasial dapat lebih diklasifikasikan sebagai *tampering* lokal atau global. *Tampering* lokal sesuai dengan perubahan yang dibuat untuk satu set *pixel*. Contoh dari tampering lokal adalah mengubah warna suatu daerah, menghapus blok pixel, menyisipkan satu set *pixel*, dan lainnya. Gangguan global yang terjadi adalah dengan memodifikasi seluruh frame pada video. Contohnya perubahan kecerahan, konversi format, *zooming*, dan sebagainya.

Pada *attack* temporal dilakukan dengan memodifikasi informasi tentang posisi frame. Hal tersebut merupakan *attack* seperti memasukkan beberapa *frame* atau mengubah *frame rate* (menghapus atau duplikasi *frame*) [7].

Untuk menentukan keaslian video juga dapat dilakukan dengan mendeteksi beberapa video, baik itu video yang asli maupun video *tampering*. Video yang *tampering* biasanya telah di memanipulasi, beberapa yang dimanipulasi adalah:

a. Menghapusan frame, misalnya menghapus adegan tertentu (yang terdiri dari serangkaian frame) yang mungkin berisi bukti penting.
b. Menambahan frame, misalnya menambah adegan tertentu yang tidak terjadi untuk membuktikan bukti sebaliknya.
c. Duplikasi frame, misalnya menambah adegan yang terjadi dalam video untuk menambah atau mengganti adegan lain.
d. Memodifikasi bagian dari frame misalnya menambah atau menghapus objek dalam frame.
e. Ukuran frame, misalnya dengan menambah atau mengurangi ukuran frame.

Selain mendeteksi frame maka yang perlu dilakukan adalah mendeteksi histogram secara matematika dengan perhitungan matrik dengan rumus sebagai berikut:

$$hi = \frac{ni}{n} \qquad i = 0,1,2 \dots, L-1 \quad \text{..... (1)}$$

dalam hal ini L adalah nilai *gray-level* terbesar dalam citra, *hi* adalah histogram, *ni* adalah jumlah *pixel* yang memiliki derajat keabuan *i* dan *n* adalah jumlah seluruh *pixel* di dalam citra.

III. METODE PENELITIAN

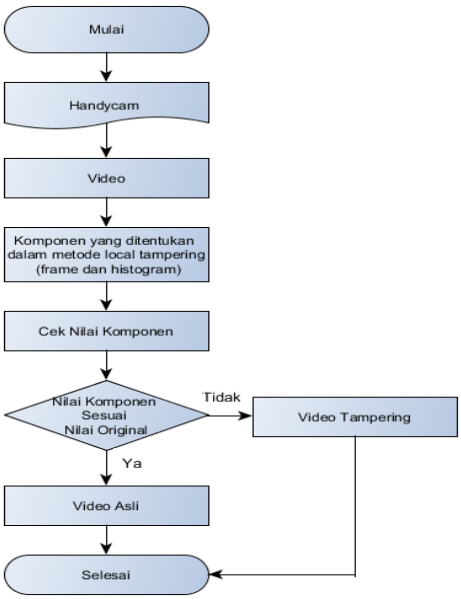
Tampering video yang mengalami perubahan dari bentuk aslinya adalah berupa gambar dan video.

Perubahan tersebut dapat diklasifikasikan sebagai tindakan sengaja atau tidak sengaja. *Tampering* yang disengaja memiliki tujuan yang jahat dengan memodifikasikan konten atau menghapus hak cipta. Disamping itu, *tampering* yang tidak disengaja merupakan konsekuensi dari proses operasional digital, seperti memperbaiki kecerahan, perubahan format, pengurangan ukuran, dll. Pada signal video teknik *tampering* dapat diklasifikasikan sebagai perubahan spasial dan temporal. Teknik *tampering* spasial disesuaikan dengan perubahan yang dibuat berdasarkan pixel pada frame [8].

Peneliti [5] mengungkapkan ada dua pendekatan yang digunakan untuk mendeteksi video, yang pertama mendeteksi otentika video dan yang kedua mendeteksi video *tampering*. Dengan adanya gangguan yang berbeda maka telah dilakukan deteksi pada setiap piksel dari frame video tertentu dan gambar yang menyimpan nilai-nilai data frame.

Metode *localization tampering* adalah metode yang menunjukan lokasi terjadinya *tampering* pada video, dimana video asli dilakukan attack dengan *zooming, rotation, cropping, grayscale.* Dari hasil *attack* tersebut kemudian dibandingkan dengan video asli, dilakukan dengan ekstraksi menjadi beberapa frame kemudian dilakukan percocokkan antar frame, perhitungan histogram secara matematika dan grafik histogram. Dari percocokan antara *frame by frame* itu maka akan diketahui frame yang mengalami perbedaan dan dari hasil perhitungan histogram, grafik histogram maka juga dapat diketahui perbedaan serta dapat menentukan lokasi mana yang terjadi *tampering* dan durasi keberadaan terjadi *tampering*. Dimana nilai yang terkandung dalam komponen tersebut akan dibuat sebuah *rule* yang nantinya akan menghasilkan *output* berupa deteksi keaslian video.

A. FLOWCHART DETEKSI VIDEO *TAMPERING*

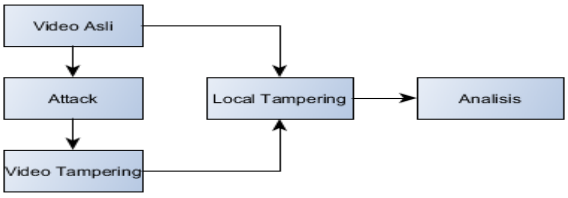


Gambar 1. Flowchart Deteksi Video *Tampering*

Gambar 1 merupakan proses atau langkah-langkah analisis untuk deteksi keaslian video. Dari proses pertama yaitu mendapati video yang ada pada *handycam*, kemudian dari video tersebut maka dilakukan pengecekan nilai pada frame dan histogram, dari hasil pengecekan jika terjadi perbedaan nilai maka video tersebut mengalami tampering dan jika nilai komponennya sama maka video tersebut merupakan video asli. Hasil dari analisis tersebut maka akan diketahui letak perbedaan frame yang telah mengalami *tampering*.

B. Proses Simulasi Video

Tahapan simulasi dimulai dari mempersiapkan video sebagai media untuk analisis *tampering*. Biasanya seseorang menghilangkan barang bukti dengan cara memanipulasi video hal tersebut bertujuan untuk menghilangkan barang bukti.



Gambar 2. Proses Simulasi Video

Gambar 2. merupakan proses simulasi video tampering menggunakan *attack cropping, zooming, rotation, dan grayscale*. Pada video asli dilakukan attack menjadi video *tampering* dengan cara *cropping, zooming, rotation, dan grayscale*. Setelah video di *tampering* maka akan dilakukan analisis dengan metode *local tampering* antara video asli dan *video tampering*.

IV. HASIL DAN PEMBAHASAN

Video yang digunakan dalam analisis ini adalah video yang ada didalam handycam dengan format MPG ukuran 79,5 MB dengan durasi 100 detik. Analisis ini dilakukan *frame by frame* hasil dari ekstraksi video.

Hasil ekstraksi pada video asli dan video tampering dilakukan analisis pada nilai pixel warna dengan menggunakan algoritma K-means, yaitu dengan menampilkan *clustering* atau kelompok data RGB.

Tabel 1. Analisis Nilai Pixel Warna

Frame	Video Asli			Video Tampering		
	R	G	B	R	G	B
1	198	186	212	227	221	245
2	198	186	210	227	221	245
3	199	187	211	228	220	245
4	200	193	212	192	192	192
5	203	192	210	196	196	196
6	216	206	221	199	199	199
7	204	199	217	198	198	198
8	225	211	233	212	212	212
9	224	213	234	207	207	207
10	224	210	231	220	220	220

Untuk menentukan centroid awal digunakan cara yaitu diambil nilai pixel dari RGB. Kemudian dari setiap nilai pixel diambil nilai tengahnya.

Jarak anggota cluster atau kelompok data dapat dihitung 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. Hasil jumlah tersebut di akarkan.

Video asli

$$d11 = \sqrt{(198-99)^2 + (186-93)^2 + (212-106)^2} = 172{,}3$$

$$d12 = \sqrt{(198-99)^2 + (186-93)^2 + (210-105)^2} = 171{,}7$$

$$d13 = \sqrt{(199-99{,}5)^2 + (187-93{,}5)^2 + (211-105{,}5)^2} = 172{,}5$$

Video tampering

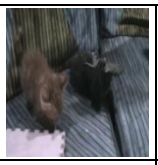
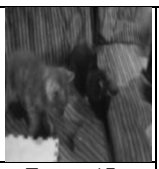
$$d11 = \sqrt{(227-113{,}5)^2 + (221-110{,}5)^2 + (245-122{,}5)^2} = 200{,}2$$

$$d12 = \sqrt{(227-113{,}5)^2 + (221-110{,}5)^2 + (245-122{,}5)^2} = 200{,}2$$

$$d13 = \sqrt{(228-114)^2 + (220-110)^2 + (245-122{,}5)^2} = 200{,}2$$

Dari hasil diatas maka dapat dilihat bahwa antara pixel pada video tampering dan video asli mengalami perbedaan yang sangat besar, pada nilai pixel RGB yang mempunyai nilai sama maka framenya mengalami attack yang berupa grayscale.

Tabel 2. Deteksi Frame Pada Video

Attack	**Analisis**		**Kesimpulan**
	Video Asli	**Video *Tampering***	
Cropping			Terjadi *cropping* pada frame 1 karena antar frame tidak sama
	Frame 1	Frame 1	
Rotation			Terjadi *rotasi* 180º frame 5 pada video *tampering*
	Frame 5	Frame 5	
Zooming			Terjadi *zooming* pada frame 10 pada video tampering
	Frame 10	Frame 10	
Grayscale			Terjadi *grayscale* pada frame 15 pada video *tampering*
	Frame 15	Frame 15	

A. Analisis Histogram

Analisis histogram dilakukan dengan cara menghitung matrik pada nilai histogram yang digunakan untuk membandingkan nilai histogram pada video asli dan video tampering serta untuk membuat perbandingan grafik. Secara matematika histogram citra dihitung dengan rumus sebagai mana yang terdapat pada rumus 1:

$$hi = \frac{ni}{n} \quad i = 0{,}1{,}2 \ldots, L-1 \quad \ldots\ldots\ldots\ldots \quad (1)$$

Berikut ini perhitungan histogram dari video asli dan video tampering, untuk mendapatkan histogram dari citra diatas pertama-tama kita harus menghitung jumlah kemunculan masing-masing dari *grey-level*, *ni*, dimana *i* adalah nilai *grey-level*

Tabel 3. Nilai Histogram Pada Video Asli

i	*hi*	*i*	*hi*
4	0.078	10	0.047
5	0.094	11	0.031
6	0.234	12	0.031
7	0.125	14	0.047
8	0.187	17	0.031
9	0.078	20	0.016

Tabel 3. merupakan tabel hasil perhitungan histogram dari salah satu frame pada video asli. Hasil perhitungan matrik histogam selanjunya dibandingkan dengan perhitungan matrik pada salah satu frame video *tampering*. Berikut ini perhitungan histogram yang terdapat pada video *tampering.*

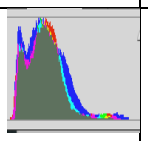
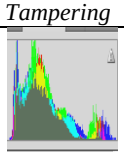
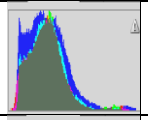
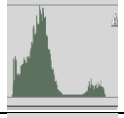
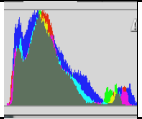
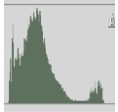
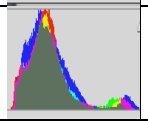
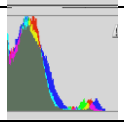
Tabel 4. Nilai Histogram Pada Video *tampering*

i	*hi*	*i*	*hi*	*i*	*hi*	*i*	*hi*
4	0.031	14	0.016	26	0.031	38	0.016
5	0.047	15	0.016	27	0.016	39	0.016
6	0.094	16	0.031	28	0.016	40	0.047
7	0.031	20	0.047	29	0.016	41	0.047
8	0.016	22	0.047	31	0.031	42	0.016
9	0.031	23	0.047	32	0.031	44	0.016
10	0.062	24	0.031	35	0.031	45	0.031
12	0.016	25	0.016	37	0.031	48	0.031

Tabulasi perhitungan histogram diatas dapat dilihat bahwa semakin besar nilai *ni* maka semakin besar pula nilai *hi*. Dari hasil perhitungan histogram secara matematika antara frame video asli dan frame video *tampering* mempunyai nilai yang berbeda. Hal tersebut maka akan diketahui bahwa frame mana yang terjadi *tampering*.

B. Analisis Grafik Histogram

Tabel 5. Grafik Histogram

Frame	Video Asli	Video *Tampering*	Durasi (s)	Keterangan
1			1 s	Terjadi *tampering* yaitu sisipan gambar
10			5 s	Terjadi tampering yaitu sisipan video dan *Attack grayscale*
20			9 s	
30			13 s	Non-tampering

Tabel 6 dilakukan analisis setiap frame pertama pada beberapa detik sekali karena untuk menunjukkan terjadinya attack. Hasil analisis grafik histogram pada frame video asli dan frame video *tampering* adalah sebagai berikut:

a. Pada frame 1 menunjukkan grafik histogram yang berbeda, hal tersebut menandakan bahwa frame 1 pada video *tampering* telah terjadi penyisipan gambar.
b. Pada frame 5 sampai frame 25 menunjukkan grafik histogram yang berbeda, hal tersebut menandakan bahwa pada video *tampering* terjadi *attack* yaitu *grayscale*.
c. Pada frame 30 menunjukkan grafik histogram yang sama, maka frame tersebut adalah frame asli.

Dari analisis frame diatas menunjukkan bahwa frame 1 sampai frame ke 29 pada detik ke 1 sampai detik ke 10 menunjukkan *tampering*, yaitu berupa *cropping, grayscale, zoom, dan rotasi*.

Dari analisis diatas memberikan informasi bahwa video terjadi *tampering* dengan durasi 10 detik pada awal video, yang terletak pada frame ke 1 sampai frame ke 29. Dalam analisis tersebut terdeteksi bahwa video mengalami *attack* berupa *cropping, zooming, rotation*, dan *grayscale.* Manipulasi video tersebut bertujuan untuk menyembunyikan kejadian atau bukti otentik dalam video.

Analisis di atas juga terdapat kelemahan yaitu hanya menganalisis video pada handycam dan tidak pada CCTV, smartphone dan dari media lainnya karena dibanding dengan alat perekam lainnya handycam sering digunakan oleh lembaga, instansi atau masyarakat dalam acara penting karena jangkauan yang luas. Pada penelitian ini juga masih menggunakan metode *local tampering* yaitu hanya menganalisis video dengan *frame by frame*, histogram dan *number of unique color*.

V. KESIMPULAN

Setelah melakukan beberapa hal terkait dengan perancangan, deteksi dan analisis dari penelitian deteksi keaslian video pada handycam dengan metode *localization tampering* maka diperoleh beberapa kesimpulan sebagai berikut:

1. Konsep dasar dalam mendeteksi video pada handycam ini yang pertama yang dilakukan adalah dengan membuat simulasi video tampering dengan attack dimana video asli dilakukan *cropping, zooming, rotation, dan grayscale*. Dari hasil attack tersebut terbentuk sebuah video tampering. Video asli dan video tampering kemudian dianalisis dengan menggunakan metode *localization tampering* dengan menganalisis frame by frame, dan grafik histogram.
2. Hal yang harus dilakukan untuk mengidentifikasi terjadinya *tampering* adalah dengan pembuatan sampel Video, dimana sampel video tersebut digunakan untuk membandingkan antara rekaman video asli dan rekaman video tampering. Selanjutnya adalah tahap Pre-processing, tahap ini dilakukan dengan ekstraksi *frame* pada file rekaman video, yaitu dengan mengubah file rekaman video ke dalam bentuk *frame-frame* agar dapat disusun sebagai citra digital yang berurutan kemudian dianalisis *frame* dan histogramnya dan yang terakhir proses simulasi video dengan *attack***.** Yang mana video asli di buat menjadi video tampering dengan cara *cropping cropping, zooming, rotation, dan grayscale*. Setelah video di tampering maka akan dilakukan analisis dengan metode *localization tampering* antara video asli dan video tampering.

Saran peneliti selanjutnya diharapkan dapat melakukan beberapa hal untuk peningkatan terhadap analisis video yang bukan hanya berasal dari handycam tapi juga ada di CCTV, smartphone, atau dari media sosial. Mengembangkan metode *localization tampering* dalam analisis video lebih lanjut atau perlu dilakukan gabungan metode untuk meningkatkan akurasi dalam mendeteksi dugaan manipulasi terhadap video.

VI. REFERENSI

[1] muhammad nuh Al-azhar, *digital forensic: Panduan Praktis Investigasi Komputer*. jakarta, 2012.
[2] M. K. Thakur dan V. Saxena, "Data-parallel full reference algorithm for dropped frame identification in uncompressed video using genetic algorithm," hal. 467–471, 2013.
[3] R. C. Pandey, S. K. Singh, dan K. K. Shukla, "Passive Copy- Move Forgery Detection in Videos," hal. 301–306, 2014.
[4] P. Bestagini, S. Milani, M. Tagliasacchi, dan S. Tubaro, "Local tampering detection in video sequences," *2013 IEEE Int. Work. Multimed. Signal Process. MMSP 2013*, hal. 488–493, 2013.

[5] A. Gupta, S. Gupta, dan A. Mehra, "Video authentication in digital forensic," *2015 1st Int. Conf. Futur. Trends Comput. Anal. Knowl. Manag. ABLAZE 2015*, no. Ablaze, hal. 659–663, 2015.

[6] P. Bestagini, K. M. Fontani, S. Milani, M. Barni, A. Piva, M. Tagliasacchi, dan K. S. Tubaro, "An overview on video forensics," *Eur. Signal Process. Conf.*, hal. 1229–1233, 2012.

[7] R. Rigoni, P. G. Freitas, dan M. C. Q. Farias, "Tampering detection of audio-visual content using encrypted watermarks," in *Brazilian Symposium of Computer Graphic and Image Processing*, 2014.

[8] Y. Su, W. Nie, dan C. Zhang, "A frame tampering detection algorithm for MPEG videos," in *Proceedings - 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, ITAIC 2011*, 2011.