DETEKSI LOCAL TAMPERING PADA VIDEO MENGGUNAKAN ALGORITMA LBP-TOP

Febryanti Sthevanie
Program Studi S1 Teknik Informatika, Fakultas Informatika
Universitas Telkom, Jl. Telekomunikasi Nomor 1 Bandung
sthevanie@telkomuniversity.ac.id

ABSTRAK

Video sering dijadikan sebagai bukti otentik dalam sebuah kasus persidangan. Hal ini menimbulkan permasalahan bagaimana memastikan sebuah video asli atau hasil rekayasa. Kegiatan untuk menganalisis keaslian sebuah video adalah salah satu fungsi dari video forensic. Salah satu bentuk rekayasa yang dapat dilakukan pada video adalah local tampering. Metode yang pernah digunakan untuk mendeteksi local tampering adalah cross correlation. Metode ini melakukan proses pengecekan per pixel, sehingga kurang efisien dari sisi kompleksitas waktu. Dalam penelitian ini, diusulkan sebuah metode LBP-TOP untuk melakukan proses deteksi local tampering pada video. Metode ini dipilih karena dapat melakukan ekstraksi ciri pada domain spasial dan domain temporal secara sekaligus sehingga lebih efisien dibandingkan metode cross correlation. Metode LBP-TOP ini akan digunakan untuk melakukan ekstraksi ciri pada macroblock sebuah video lalu membandingkannya pada macroblock lain dalam video yang sama. Berdasarkan hasil pengujian yang dilakukan menunjukkan bahwa kinerja LBP-TOP dalam mendeteksi local tampering lebih efisien dibandingkan metode cross correlation. Hal ini dapat terlihat dari kompleksitas waktu yang disajikan pada data video yang sama menggunakan kedua metode tersebut.

Kata Kunci :Local tampering, LBP-TOP, Cross Correlation, Video Forensic

1. PENDAHULUAN

Pada masa sekarang, aplikasi web telah menjadi media untuk berbagi informasi dalam bentuk apapun. Sudah banyak aplikasi web yang menyediakan fasilitas untuk unggah dan unduh content berupa gambar, suara dan juga video. Hal ini menimbulkan peningkatan yang luar biasa terhadap ketersediaan content multimedia yang dapat diakses oleh siapapun. Namun, hal ini tidak diimbangi dengan adanya sistem yang dapat memverifikasi apakah content multimedia yang diunggah autentik atau tidak. Karena hal ini, pada saat seseorang menjelajah dalam dunia maya, akan sangat mungkin untuk mendapatkan content multimedia yang dimanipulasi. Dalam banyak kasus, hasil manipulasi terhadap content multimedia tersebut bisa terlihat sangat nyata. Bahkan saat ini, di media sosial banyak beredar informasi berupa gambar dan video yang merupakan hasil manipulasi dan menipu banyak pengguna media sosial. Hal ini tentu saja dapat mengakibatkan masalah yang serius.

Untuk mengatasi masalah tersebut, penelitian terkait multimedia forensic banyak dilakukan [1]. Banyak teknik yang dibuat untuk mendeteksi apakah suatu content multimedia dimanipulasi atau tidak. Penelitian multimedia forensic banyak berkembang pada kasus berkas gambar, sedangkan pada berkas video masih sedikit [2]. Padahal, tingkat kepercayaan publik terhadap video lebih tinggi dibandingkan tingkat kepercayaan terhadap gambar. Dalam dunia hukum misalnya, bukti berupa rekaman video memiliki tingkat kepercayaan yang cukup tinggi dan sering menjadi bukti kunci untuk mengungkap kasus karena proses manipulasi video dianggap lebih sulit dibandingkan proses manipulasi gambar. Namun saat ini proses manipulasi video dipermudah dengan ketersediaan aplikasi-aplikasi video editing, baik yang open source maupun berbayar. Aplikasi-aplikasi tersebut memudahkan seseorang untuk memanipulasi video dan hasil manipulasinya dapat terlihat sangat nyata sehingga dapat dipercaya. Walaupun secara waktu, proses manipulasi video memakan waktu lebih lama dibandingkan proses manipulasi gambar. Hal ini menuntut adanya penelitian yang fokus untuk mencari solusi bagaimana mendeteksi adanya proses manipulasi terhadap sebuah video atau tidak.

Secara umum, metode deteksi manipulasi pada video terbagi ke dalam dua kategori [2]. Kategori pertama adalah tampering detection, yaitu metode deteksi yang hanya mengecek integritas dari video tanpa menunjukkan bagian mana pada video tersebut yang dimanipulasi.

Kategori kedua adalah tampering localization, yaitu metode deteksi yang menunjukkan bagian pada video yang dimanipulasi.

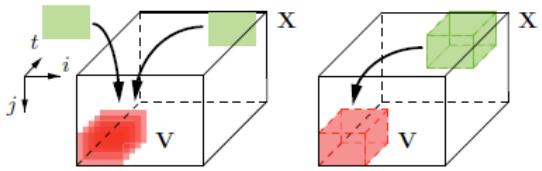
Algoritma pada kategori pertama mendeteksi proses manipulasi secara global. Contoh algoritma pada kategori ini adalah algoritma yang mendeteksi adanya kompresi ganda yang dilakukan pada sebuah berkas video [3]. Contoh lainnya adalah algoritma yang mendeteksi apakah sebuah video merupakan hasil rekam ulang dari sebuah berkas video yang lain [4]. Kemudian, pada penelitian lain dikembangkan algoritma untuk mendeteksi adanya proses interpolasi pada sebuah video [5]. Metode-metode tersebut dapat digunakan untuk mengecek validitas dari sebuah video. Namun, metode-metode tersebut tidak dapat memberikan informasi lokasi manipulasi pada video tersebut.

Algoritma pada kategori kedua dapat mendeteksi lokasi manipulasi dari video. Lokasi manipulasi berupa posisi spasial dalam bentuk koordinat pixel dan posisi temporal dalam bentuk urutan frame yang dimanipulasi. Pada penelitian [6] dikembangkan algoritma untuk mendeteksi manipulasi video tampering, yakni menyisipkan potongan sejumlah frame tertentu pada sejumlah frame yang lain. Algoritma yang dikembangkan bekerja dengan membentuk 3D block pada video dan dilakukan proses cross-corelation pada 3D block tersebut dengan seluruh bagian video secara non-overlapped. Algoritma tersebut bekerja pada level pixel. Hal ini mengakibatkan algoritma yang digunakan menjadi sangat kompleks. Karena itu pada penelitian ini diusulkan metode LBP-TOP untuk mengurangi kompleksitas algoritma deteksi video tampering tersebut. Diharapkan dengan menggunakan LBP-TOP, proses komputasi menjadi lebih sederhana dengan range nilai akurasi yang tidak terlalu jauh dengan metode sebelumnya pada [6].

2. VIDEO TAMPERING

Video tampering adalah proses untuk menyisipkan obyek tertentu ke dalam sebuah video [2]. 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.

Ilustrasi proses video tampering dapat dilihat pada gambar berikut.



Gambar 1 Ilustrasi Video tampering [6]

Dapat dilihat pada gambar terdapat dua jenis manipulasi tampering. Pada gambar yang sebelah kiri adalah proses tampering dengan menyelipkan sebuah gambar pada beberapa frame di video. Pada gambar yang sebelah kanan adalah proses tampering dengan menyisipkan potongan beberapa frame dari satu video ke beberapa frame lain yang berbeda dalam video yang sama.

Banyak metode yang telah dibangun untuk mendeteksi adanya tampering yang dilakukan terhadap video. Penelitian yang dilakukan pada [8] mendeteksi dua jenis tampering. Yang pertama adalah mendeteksi adanya spatial copy-move (duplikasi obyek yang sama pada scene yang sama) menggunakan Histogram of Gradients (HOG) matching. Yang kedua adalah mendeteksi adanya temporal copy-move (menyisipkan obyek dari sebuah frame ke frame lain) menggunakan eksploitasi struktur MPEG-2 GOP.

Penelitian yang dilakukan oleh [9] mendeteksi adanya tampering pada video menggunakan karakteristik derau. Karakteristik derau yang dimiliki oleh frame asli dengan potongan frame yang disisipkan memiliki perbedaan dan sangat sensitif terhadap proses kompresi. Pada penelitian [6] dikembangkan algoritma untuk mendeteksi manipulasi video tampering, yakni menyisipkan potongan sejumlah frame tertentu pada sejumlah frame yang lain. Algoritma yang dikembangkan bekerja dengan membentuk 3D block pada video dan dilakukan proses cross-corelation pada 3D block tersebut dengan seluruh bagian video secara non-overlapped.

3. LOCAL BINARY PATTERN-THREE ORTHOGONAL PLANES (LBP-TOP)

LBP-TOP adalah modifikasi dari metode LBP yang dapat digunakan untuk mendeskripsikan bukan hanya ciri spasial dari sebuah video, tapi juga ciri temporal. Local Binary Pattern (LBP) adalah metode untuk mendeskripsikan tekstur pada citra. LBP didefinisikan sebagai perbandingan nilai biner pixel pada pusat citra dengan nilai-nilai pixel di sekelilingnya [10]. Misalkan pada sebuah citra

berukuran 3x3, nilai biner pada pusat citra dibandingkan dengan nilai-nilai di sekelilingnya. Dengan cara mengurangkan nilai pixel pada pusat citra dengan nilai-nilai pixel di sekelilingnya. Jika hasilnya lebih atau sama dengan 0 maka diberi nilai 1 dan jika hasilnya kurang dari 0 diberi nilai 0. Setelah itu, menyusun 8 nilai biner searah jarum jam atau sebaliknya dan mengubah 8 bit biner ke dalam nilai desimal untuk menggantikan nilai pixel pada pusat citra. Ilustrasi lengkap dari proses LBP adalah sebagai berikut.

g_3	g_2	g_1
g_4	g_c	g_0
g_5	g_6	g_7

Gambar 2 Ilustrasi Matriks LBP

Misalkan:
$g_c = 20$ $g_4 = 17$
$g_0 = 18$ $g_5 = 11$
$g_1 = 23$ $g_6 = 121$
$g_2 = 27$ $g_7 = 9$
$g_3 = 31$

Maka matriks LBP yang dihasilkan adalah sebagai berikut

1	1	1
0		0
0	1	0

Dan nilai biner dari LBP tersebut adalah 01110010.

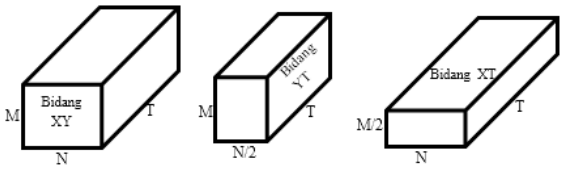
Secara umum persamaan dari LBP dapat dituliskan sebagai berikut:

$$\mathrm{LBP}(x_c, y_c) = \sum_{p=0}^{N-1} s(g_p - g_c)2^p \quad (1)$$

dengan:
c = posisi pusat matriks LBP
N = jumlah tetangga di sekeliling pusat matriks LBP
dan s adalah fungsi dengan persamaan:

$$s(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases} \quad (2)$$

Algoritma LBP-TOP akan melakukan proses ekstraksi ciri LBP pada tiga bidang[7]. Algoritma LBP-TOP dapat diilustrasikan sebagai berikut.



Gambar 3 Ilustrasi 3 Bidang LBP-TOP

Gambar di atas adalah ilustrasi dari sebuah berkas video yang terdiri dari *frame-frame* berjumlah T *frame*. Masing-masing *frame* berukuran sama, yakni MxN. LBP-TOP akan melakukan proses LBP pada bidang XY, XT dan YT. Bidang XY digunakan untuk menggambarkan ciri spasial dari video. Bidang XY diperoleh dari *frame* pertama dari video. Bidang XT dan YT digunakan untuk menggambarkan ciri temporal dari video. Bidang XT adalah bidang yang diperoleh dengan memotong balok tersebut secara melintang tepat di bagian tengah (posisi M/2). Bidang YT adalah adalah bidang yang diperoleh dengan memotong balok tersebut secara membujur tepat di bagian tengah (posisi N/2). Dari masing-masing bidang tersebut akan muncul ciri LBP. Tiga ciri LBP ini dapat digunakan sebagai ciri dari video tersebut.

4. ANALISIS KOMPLEKSITAS CROSS CORRELATION DAN LBP-TOP

Tujuan penelitian ini adalah untuk mengusulkan metode LBP-TOP sebagai metode deteksi local tampering pada video. Metode ini diusulkan karena berdasarkan analisis kompleksitas akan lebih baik dibandingkan metode cross correlation. Analisis kompleksitas dua metode tersebut dapat dijabarkan sebagai berikut.

Misalkan dilakukan proses deteksi local tampering pada video dengan resolusi M x N pixel dengan frame sejumlah T frame. Metode cross correlation akan melakukan proses pengecekan terhadap semua pixel yang ada pada video. Maka dengan menggunakan algoritma cross correlation, kompleksitas waktu yang dihasilkan adalah = M x N x T satuan waktu. Jika diasumsikan M = N = T = n, maka T(n) adalah kompleksitas waktu dari algoritma cross correlation.

Nilai T(n) = M x N x T
= n x n x n
= n^3

Maka untuk algoritma cross correlation, kompleksitas waktu yang dihasilkan adalah

$T(n) = n^3 = O(n^3)$

Di sisi lain, algoritma LBP-TOP akan melakukan proses ekstraksi ciri pada tiga bidang, yakni bidang XY yang berukuran M x N pixel, XT yang berukuran M x T pixel dan bidang YT yang berukuran N x T pixel. Dengan mengasumsikan M = N = T, maka T(n) untuk algoritma LBP-TOP dapat dijabarkan sebagai berikut.

Nilai $T(n) = (M \times N) + (M \times T) + (N \times T)$
$= (n \times n) + (n \times n) + (n \times n)$
$= n^2 + n^2 + n^2$
$= 3n^2$

Maka untuk algoritma LBP-TOP, kompleksitas waktu yang dihasilkan adalah

$T(n) = 3n^2 = O(n^2)$

Dapat terlihat bahwa dari kompleksitas waktu asimptotik kedua algoritma tersebut, algoritma LBP-TOP yang memiliki kompleksitas asimptotik $O(n^2)$ lebih efisien dibandingkan algoritma cross correlation yang memiliki kompleksitas asimptotik $O(n^3)$. Hasil analisis ini akan diperkuat pada tahap eksperimen.

5. RANCANGAN EKSPERIMEN

Tujuan eksperimen ini adalah untuk membuktikan hasil analisis perbandingan kompleksitas metode cross correlation dan metode LBP-TOP untuk mendeteksi local tampering pada video. Eksperimen dilakukan pada dua video yang mengalami local tampering. Adapun tahap dari eksperimen ini adalah sebagai berikut.

a. Menandai lokasi terjadinya tampering pada kelima video.
b. Menjalankan sistem deteksi local tampering menggunakan algoritma cross correlation dan LBP-TOP. Kedua algoritma tersebut dijalankan dengan terlebih dahulu melakukan pemotongan video menjadi sub-blok, lalu dilakukan pencocokan antar sub-blok menggunakan kedua algoritma tersebut.
c. Mengamati hasil deteksi dari kedua algoritma tersebut dan mencatat waktu eksekusi kedua algoritma tersebut.
d. Menganalisis perbandingan waktu eksekusi kedua algoritma.

Adapun parameter yang diujikan pada eksperimen tersebut adalah sebagai berikut.

a. Ukuran panjang dan lebar sub-blok: 40 dan 20 pixel
b. Jumlah frame sub-blok: 60 dan 30 frame
c. Overlap panjang & lebar sub-blok: 0% (tanpa overlap), 50% (overlap separuh)
d. Overlap jumlah frame sub-blok: 0% (tanpa overlap), 50% (overlap separuh)

6. HASIL EKSPERIMEN DAN KESIMPULAN

Berikut adalah hasil dari eksperimen yang dilakukan pada kedua video. Masing-masing table menunjukkan hasil pada masing-masing video. Kolom pertama menunjukkan ukuran sub-blok. Kolom kedua menunjukkan jumlah frame yang digunakan sebagai sub-blok. Kolom ketiga menunjukkan berapa ukuran overlap sub-blok. Kolom keempat menunjukkan berapa overlap jumlah frame. Kolom kelima adalah waktu eksekusi dari algoritma cross correlation. Kolom keenam adalah waktu eksekusi dari algoritma LBP-TOP.

Tabel 1 Hasil Eksperimen pada Video 1

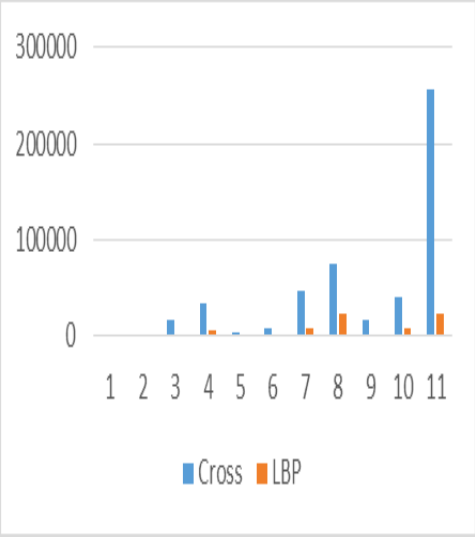
Ukuran sub-blok	Jumlah Frame	Ovelap Ukuran sub-blok	Overlap Jumlah Frame	Waktu eksekusi Cross Correlation	Waktu eksekusi LBP-TOP
40	60	0%	0%	974.38	188.34
40	60	0%	50%	2015.62	524.83
40	60	50%	0%	16868.29	1688.95
40	60	50%	50%	35053.58	6129.12
40	30	0%	0%	4138.44	776.02
40	30	0	50%	7687.69	2468.78
40	30	50%	0%	47758.15	7605.62
40	30	50%	50%	75201.53	22440.78
20	60	0%	0%	16315.23	1605.29
20	60	0%	50%	41285.66	7547.99
20	60	50%	0%	255663	23582.80

Tabel 2 Hasil Eksperimen pada Video 2

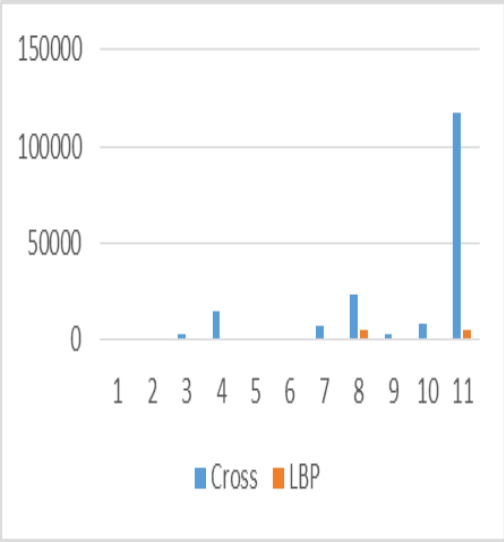
Ukuran sub-blok	Jumlah Frame	Ovelap Ukuran sub-blok	Overlap Jumlah Frame	Waktu eksekusi Cross Correlation	Waktu eksekusi LBP-TOP
40	60	0%	0%	241.84	51.19
40	60	0%	50%	491.76	139.87
40	60	50%	0%	2849.60	339.14
40	60	50%	50%	14449.24	1157.27
40	30	0%	0%	586.91	130.32
40	30	0	50%	1205.06	448.39
40	30	50%	0%	6968.90	1244.94
40	30	50%	50%	23610.59	4836.46
20	60	0%	0%	3127.51	379.85
20	60	0%	50%	8519.75	1380.90
20	60	50%	0%	117148	4836.38

Dari kedua tabel di atas, terlihat bahwa waktu eksekusi dari algoritma cross correlation selalu lebih tinggi dibandingkan algoritma LBP-TOP. Artinya, algoritma LBP-TOP bekerja lebih efisien dari sisi waktu jika dibandingkan dengan algoritma Cross Correlation.

Berikut adalah grafik performansi waktu dari kedua algoritma berdasarkan data pada tabel di atas. Sumbu horizontal menyatakan urutan konfigurasi parameter sesuai data pada tabel. Sumbu vertikal menyatakan waktu eksekusi dari kedua algoritma. Grafik biru mewakili algoritma cross correlation dan grafik merah mewakili algoritma LBP-TOP.



Gambar 4 Grafik Performansi Waktu pada Video 1



Gambar 4 Grafik Performansi Waktu pada Video 2

Dari data tersebut di atas, dapat disimpulkan bahwa hasil analisis kompleksitas waktu yang dijabarkan terbukti benar. Langkah berikutnya dari penelitian ini yang akan dilakukan adalah menganalisis lebih lanjut tentang deteksi local tampering video menggunakan algoritma LBP-TOP dan meneliti bagaimana hasil akurasi dari metode tersebut.

DAFTAR PUSTAKA

[1] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," *IT Security Incident Management and IT Forensics (IMF)*, 2011.

[2] S. Milani et al., "An overview on video forensics," *APSIPA Transactions on Signal and Information Processing*, vol. 1, p. E2, 2012.

[3] P. Bestagini, M. Tagliasacchi, S. Tubaro S. Milani, "Multiple compression detection for video sequences," in *2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP)*, 2012.

[4] M. Visentini-Scarzanella, M. Tagliasacchi, P. Dragotti, S. Tubaro P. Bestagini, "Video recapture detection based on ghosting artifact analysis," in *2013 IEEE International Conference on Image Processing (ICIP)*, 2013.

[5] S. Battaglia, S. Milani, M. Tagliasacchi, S. Tubaro P. Bestagini, "Detection of temporal interpolation in video sequences,"

in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2013.

[6] Paolo Bestagini, Simone Milani, and Marco Tagliasacchi, "Local tampering detection in video sequences," in *15th IEEE International Workshop on Multimedia Signal Processing*, Pula (Sardinia), 2013.

[7] M. Pietikainen, T. Maenpaa T. Ojala, "Multiresolution Gray Scale and Rotation Invariant Texture Analysis with Local Binary Patterns," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, 2002.

[8] A. Subramanyam and S. Emmanuel, "Video forgery detection using HOG features and compression properties," in *2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP)*, 2012.

[9] T. Okabe, Y. Sato M. Kobayashi, "Detecting forgery from staticscene video based on inconsistency in noise level functions," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 883–892, 2010.

[10] G. Zhao M. Pietikainen, "Local Binary Pattern Descriptors for Dynamic Texture Recognition," in *International Conference of Pattern Recognition*, 2006, pp. 211-214.