

ANALISIS KETAHANAN VIDEO WATERMARKING DENGAN METODE DUAL-TREE COMPLEX WAVELET TRANSFORM TERHADAP SERANGAN KAMERA DIGITAL

ANALYSIS OF ROBUSTNESS VIDEO WATERMARKING BASED ON DUAL-TREE COMPLEX WAVELET TO DIGITAL CAMERA ATTACK

Imamulkaer¹, Ida Wahidah², Ledya Novamizanti³

Fakultas Teknik Elektro, Universitas Telkom, Bandung, Jawa Barat 40257¹²³

imamulkaer@student.telkomuniversity.ac.id¹, wahidah@telkomuniversity.ac.id², ledyaldn@telkomuniversity.ac.id³

Abstrak - *Watermarking* adalah salah satu teknik yang dapat digunakan untuk melindungi hak cipta atas data multimedia seperti video, gambar, audio, maupun teks dengan cara menyisipkan informasi ke dalam data multimedia tersebut. Pada tugas akhir ini, dilakukan penyisipan menggunakan teknik *watermarking* dengan metode *Dual-Tree Wavelet Transform* (DT-CWT) ke dalam video berformat AVI dengan resolusi *Full High Definition* (FHD) berdurasi 10 detik dengan *frame rate* 30 fps. Perancangan dilakukan menggunakan *software* MATLAB dengan pengujian kualitas *watermarked* video menghasilkan nilai PSNR 39,2863 dB, dan BER 0,78% pada saat tanpa serangan. Penelitian ini tahan terhadap serangan *digicam*, walaupun dengan BER yang cukup tinggi, namun masih bisa terlihat secara kasat mata, yaitu dengan BER 17,9473%.

Kata Kunci: *Watermarking, Video Watermark, Dual-Tree Wavelet Transform, Digidam attack*

Abstract - *Watermarking* is one technique that can be used to protect copyright over multimedia data such as video, images, audio, and text by inserting information into the multimedia data. In this thesis, the insertion is done using watermarking techniques with *Dual-Tree Wavelet Transform* (DT-CWT) into AVI format video with *Full High Definition* (FHD) resolution of 10 seconds with 30 fps frame rate. The design is done using MATLAB software with *watermarked* video quality testing resulting in PSNR value of 39.2863 dB, and BER of 0.78% when without attack. This research is resistant to *digidam* attacks, although with high BER, it can still be seen in plain view, that is with BER of 17,9473

Key Words: *Watermarking, Video Watermark, Dual-Tree Wavelet Transform, Digidam attack*

1. Pendahuluan

Pembajakan video merupakan tindakan merugikan pihak pemilik hak cipta. Selama satu dekade terakhir, pembajakan video *online* telah menjadi perhatian yang signifikan bagi produsen film serta produsen video digital lainnya. Saat ini, pembajakan yang paling sering terjadi adalah pembajakan dengan rekaman digital (*digidam*). Seringnya, hasil dari rekaman digital yang berupa gambar ataupun video tersebut disebarluaskan secara massal dan *online* dengan mengunggah ke berbagai macam sosial media dan dapat diklaim oleh beberapa orang yang tidak bertanggung jawab sebagai miliknya. Pelanggaran hak cipta terhadap data digital ini dapat diminimalisir dengan menyisipkan informasi atau data yang disebut *watermarking*. *Watermarking* merupakan teknik penyisipan informasi atau data secara rahasia kedalam suatu data digital seperti gambar, audio, video, maupun teks. Video *watermarking* memiliki kelebihan jika dibandingkan dengan *image watermarking* dan *audio watermarking* karena data video merupakan sekumpulan gambar yang disatukan sehingga *watermark* bisa disisipkan diberbagai gambar (*frame*) yang ada pada data video sehingga lebih sulit dideteksi [1]. Berbagai teknik *watermarking* telah banyak diusulkan para peneliti, yaitu: DWT-DCT [2], SWT [3], DWT-SVD [4], SWT-SVD [5], DCT-GA [6], DWT-SS [7].

Pada Tugas Akhir ini, dilakukan teknik *watermarking* yang bersifat *blind watermarking* dengan data yang disisipkan berupa citra gambar disisipkan pada video dengan resolusi *Full High Definition* (FHD) dengan teknik video *watermarking* menggunakan metode DT-CWT. Metode DT-CWT dipilih karena berdasarkan penelitian terkait bahwa DT-CWT dapat menahan serangan *camcording*. DTCWT menghasilkan kualitas citra yang lebih baik dari pada DCT, dengan PSNR diatas 45 dB [8-9].

2. Dasar Teori

2.1. Teknik Watermarking

Teknik *watermarking* ditentukan oleh beberapa faktor, diantaranya adalah tempat penyisipan dan terlihat atau tidaknya watermark. Ada beberapa tempat penyisipan watermark atau media host watermark pada data digital seperti pada data yang berdomain ruang contohnya Least Significant Bit (LSB) dan pada data dengan domain frekuensi yaitu Discrete Wavelet Transform (DWT), Dual Tree Complex Wavelet Transform (DT-CWT), dan lain-lain.

Watermark yang disisipkan pada media host watermark dapat bersifat visible (terlihat) dan invisible (tidak terlihat). Visible watermark adalah membuat sebuah tanda kepemilikan yang terlihat secara visual ke dalam objek atau data. Sedangkan invisible watermark, merupakan tanda yang tidak terlihat secara visual sehingga pelaku pembajakan mengalami kesulitan ketika ingin mengklaim atau mengkomersilkan objek asli yang diinginkan [10].

Pada proses penyisipan, *Host Image* digabungkan dengan *watermark* yang telah melalui proses *Message Modulation* yang menyerupai prinsip modulasi pada jaringan, namun pada hal ini menumpangkan *key* ke dalam *watermark*, dimana *key* adalah kunci untuk mengekstraksi *watermark*. Kunci didapatkan dengan menggunakan metode *pseudo-random* dimana *pseudo-random* merupakan matriks 2-D berisi nilai 1 dan -1 yang dihasilkan secara acak menggunakan distribusi uniform. Setelah *watermark* melalui proses *Message Modulation*, dilakukan proses penguatan bit dengan koefisien nilai penguat α . Kemudian ditanamkan blok sinkronisasi untuk membantu mengembalikan gambar ke posisi semula jika terjadi perubahan disisi penerima.

Pada proses ekstraksi, proses *peak detection* dilakukan pada *watermarked image* yang berfungsi untuk mendeteksi posisi bit pertama pada *watermarked image* berdasarkan proses sinkronisasi yang telah ditanamkan pada proses penyisipan sebelumnya. Kemudian proses RST (*Rotate, Scaling, Translation*) *Correction* dilakukan dengan tujuan untuk memperbaiki posisi gambar ke posisi semula, Setelah melalui proses RST *Correction*, dilakukan proses *Message Demodulation* untuk mengekstraksi *watermark* dengan menggunakan kunci yang sama yang telah dimodulasi pada proses penyisipan.

2.2. Dual-Tree Complex Wavelet Transform

Dual-Tree Complex Wavelet Transform (DT-CWT) merupakan penyempurnaan dari *Discrete Wavelet Transform* (DWT). Perbedaan utama antara DWT dengan DT-CWT adalah bahwa DT-CWT menggunakan dua pohon filter. Penggunaan dua pohon filter menghasilkan dua kali jumlah koefisien *wavelet* sebagai DWT asli. Koefisien yang dihasilkan oleh dua pohon ini membentuk dua set yang dapat dikombinasikan untuk membentuk satu set koefisien kompleks yang mengandung bagian *real* dan *imaginer* dari formulir tersebut [20].

DT-CWT menggunakan 2 pohon DWT, pohon pertama menghasilkan bagian real dari transformasi sedangkan pohon kedua menghasilkan bagian imajiner. Dua pohon tersebut menggunakan 2 filter yang berbeda yang dirancang bersama sehingga transformasi keseluruhannya mendekati analitik. Kedua pohon DWT tersebut dinotasikan dengan $\psi_h(t)$ dan $\psi_g(t)$, untuk memenuhi syarat rekonstruksi sempurna yang dapat mengatasi kekurangan DWT, filter dirancang sedemikian rupa sehingga *wavelet* menjadi kompleks dan dapat diformulasikan dengan[20]:

$$\psi_h(t) + j\psi_g(t) \tag{1}$$

dimana j melambangkan bagian imajiner dari transformasi. Secara ekivalen, kedua pohon tersebut dirancang sedemikian rupa sehingga $\psi_g(t)$ mendekati Hilbert Transform dari $\psi_h(t)$.

$$\psi_g(t) \approx \mathcal{H}(\psi_h(t)) \tag{2}$$

Jika 2 pohon DWT yang dimiliki oleh DT-CWT direperesntasikan dengan matriks F_h dan F_g , maka DT-CWT dapat direpresentasikan dengan persamaan [20]:

$$F = \begin{bmatrix} F_h \\ F_g \end{bmatrix} \tag{3}$$

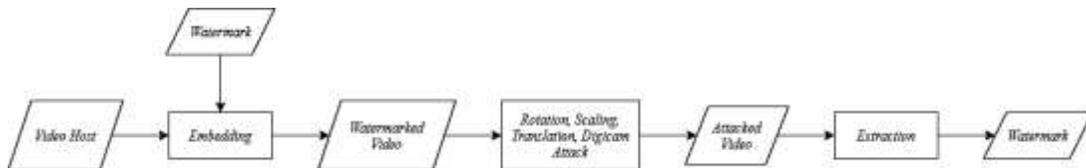
sehingga invers dari matriks F dapat dituliskan dengan persamaan [20]:

$$F^{-1} = \frac{1}{\sqrt{2}} [F_h^{-1} \ F_g^{-1}] \tag{4}$$

3. Desain Sistem

3.1. Perancangan Sistem

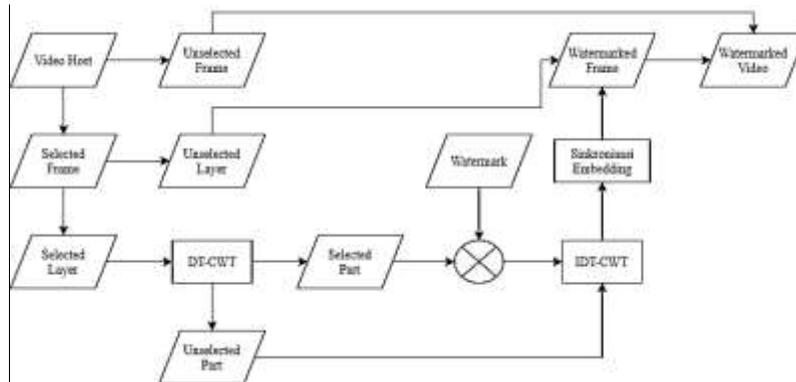
Pada perancangan sistem pada Tugas Akhir ini penulis memiliki sistematika secara keseluruhan tahapan dari proses perancangan hingga direpresentasikan dapat dilihat dari blok diagram sebagai berikut:



Gambar 1. Blok diagram sistem

3.2. Embedding

Proses *embedding*, bertujuan menyisipkan *watermark* yang merupakan citra biner kedalam *host frame* dari video.



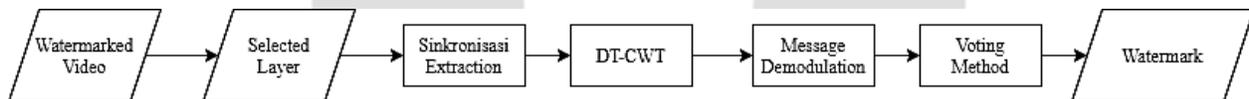
Gambar 2. Blok diagram proses *embedding*

3.2.1. Sinkronisasi Embedding

Sinkronisasi *embedding* merupakan proses penanaman blok sinkronisasi ke dalam *frame host* yang akan dideteksi disisi penerima. Fungsi dari sinkronisasi *embedding* adalah menanamkan blok sinkronisasi untuk dideteksi di sisi penerima agar dapat mengembalikan bit ke posisi semula jika terjadi perubahan sebelum masuk ke sisi penerima. Blok sinkronisasi yang ditanamkan merupakan matriks berisi nilai acak yang terdistribusi normal dengan ukuran matriks yang lebih kecil dari *frame host* kemudian direpetisi hingga sama dengan ukuran *frame host*. Blok sinkronisasi tersebut ditanamkan ke dalam *frame host* yang telah didekomposisi sehingga blok sinkronisasi tersebut tidak terlihat.

3.3. Extraction

Pada proses ekstraksi, bertujuan untuk mendapatkan kembali *watermark* yang telah disisipkan pada proses *embedding*.



Gambar 3. Blok diagram proses *extraction*

3.3.1. Sinkronisasi Extraction

Sinkronisasi *extraction* merupakan suatu proses untuk mendeteksi blok sinkronisasi yang telah ditanamkan pada proses *embedding*. Proses ini memiliki dua fungsi utama, yaitu *peak detection* dan *RST Correction*.

1. *Peak detection* adalah proses untuk mendeteksi posisi blok sinkronisasi yang telah tertanam pada *frame* yang telah tersisipi *watermark* (*watermarked frame*) sehingga dapat memperkirakan perubahan sudut dan skala yang terjadi pada *watermarked frame*. Proses ini dilakukan dengan menggunakan fungsi auto korelasi antara 2 masukan yaitu *watermarked frame* dengan blok sinkronisasi yang dibuat sama dengan blok sinkronisasi yang telah disisipkan pada *watermarked frame*. Proses auto korelasi didapatkan dengan persamaan [20]:

$$CC(m, n) = \frac{\sum_{j=1}^J f(j) g(j-m)}{[\sum_{j=1}^J f^2(j)]^{0,5} [\sum_{j=1}^J g^2(j-m)]^{0,5}} \tag{5}$$

Dimana, $CC(m, n)$ adalah hasil auto korelasi, j adalah koefisien nilai matriks, f adalah matriks untuk gambar yang diterima disisi ekstraksi, g adalah matriks yang dibangkitkan disisi penerima. Setelah proses auto korelasi, dilakukan transformasi radon untuk menghasilkan estimasi perubahan geometris pada masukan di sisi penerima [11].

2. Sedangkan *RST Correction* merupakan proses untuk memperbaiki perubahan tersebut untuk kembali ke posisi semula dengan menggunakan hasil perkiraan yang telah didapatkan dari proses *peak detection* [20].

3.4. Serangan Watermark

Pada penelitian ini akan diberikan serangan yang bertujuan untuk mengetahui perbedaan pada saat sebelum dan sesudah diberikan serangan. Serangan yang digunakan pada penelitian ini adalah *rotation*, *scaling*, *translation*, dan *digicam attack*.

- *Rotation* merupakan salah satu serangan yang diujikan kepada video yang telah disisipi *watermark* untuk mengetahui ketahanan *watermark* setelah diberikan perubahan sudut pada video yang telah disisipi *watermark*.
- *Scaling* bertujuan untuk merubah ukuran *frame* video yang telah disisipi *watermark*.
- Pengujian terhadap serangan *translation* ini, dilakukan 2 jenis translasi untuk melakukan serangan yaitu *Letterboxing* dan *Pillarboxing*, dimana *Letterboxing* adalah menambahkan kotak hitam pada atas dan bawah pada video sedangkan *Pillarboxing* adalah menambahkan kotak hitam pada kiri dan kanan pada video.
- *Digicam* merupakan simulasi serangan *camcording* kepada satu *frame* pada *video watermarking*. Pada pengujian ini, serangan dilakukan dengan menggunakan *frame* pertama pada *video host* untuk menjadi sampel untuk difoto. Kemudian hasil foto tersebut akan dijadikan masukan pada proses ekstraksi dimana hasil foto tersebut telah mengalami perubahan warna, sudut, serta perubahan nilai koefisien gambar.

3.5. Parameter pengujian

Pengujian terhadap kualitas *watermarked video* dilakukan dengan mengukur nilai dari *parameter Peak Signal to Noise Ratio* (PSNR), dan *Bit Error Rate* (BER),

3.5.1. Peak Signal to Noise Ratio

Peak Signal to Noise Ratio adalah rasio antara nilai maksimum dari sinyal yang diatur dengan noise yang berpengaruh. Berikut persamaan PSNR [1]:

$$PSNR = 10_{\log_{10}} \frac{255^2}{MSE} \quad (6)$$

Dimana,

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2 \quad (7)$$

Perhitungan PSNR dilakukan pada saat membandingkan antara *original host* dengan *watermarked host* pada proses *embedding* dan *original watermark* dengan *extracted watermark* pada proses *extraction*.

3.5.2. Bit Error Rate

Bit Error Rate (BER) adalah parameter yang digunakan untuk mengukur kualitas hasil ekstraksi dari watermark yang disisipkan pada file host. Berikut merupakan persamaan BER [1]:

$$BER = \frac{\text{jumlah bit error}}{\text{jumlah bit keseluruhan}} \times 100 \% \quad (8)$$

4. Pengujian dan Analisis

4.1. Lingkup Pengujian Sistem

Lingkup pengujian sistem pada Tugas Akhir ini dilakukan proses pengambilan data dengan beberapa spesifikasi yang telah ditentukan, yaitu gambar yang akan menjadi *watermark* merupakan citra biner dan video yang akan disisipi *watermark* merupakan file berekstensi .avi.

4.1.1. Image Watermark

Image watermark adalah citra biner yang akan digunakan untuk penyisipan dan melewati tahap kompresi sebagai objek penelitian, dengan ukuran 32×32, 64×64, 128×128, 256×256, dan 512×512 piksel berformat .png.



Gambar 4. *Image host*

4.1.2. Data Video

Data video atau file yang akan disisipi berupa video .avi, 30fps, dengan *aspect ratio* 16:9 berukuran 1920×1080 piksel (*Full High Definition*).



Gambar 5. Frame pertama pada video host.

4.2. Hasil Pengujian

4.2.1. Pengujian terhadap jenis layer, pohon DT-CWT, subband, bagian DT-CWT, resolusi citra, dan nilai penguat citra pada data video

Pengujian ini dilakukan untuk mengetahui performansi terbaik sistem video watermarking sebelum dilakukan serangan kepada watermarked video. Pengujian ini menghasilkan performansi terbaik sistem tanpa serangan pada layer V pada ruang warna YUV, pohon pertama DT-CWT, subband HH, pada bagian real dengan resolusi citra 64x64 piksel dan dengan nilai penguat α 40 dengan PSNR 39,2863 dB, dan BER 0,7813%. Contoh hasil ekstraksi pada saat tanpa serangan dapat dilihat pada Gambar 6.



Gambar 6. Hasil ekstraksi tanpa serangan

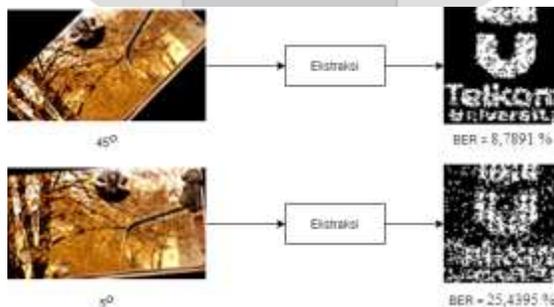
4.2.2. Pengujian terhadap serangan rotation

Rotation merupakan salah satu serangan yang diujikan kepada video yang telah disisipi watermark untuk mengetahui ketahanan watermark setelah diberikan perubahan sudut pada video yang telah disisipi watermark. Nilai hasil pengujian terhadap serangan rotation dapat dilihat pada Tabel 1.

Tabel 1 Hasil pengujian terhadap serangan rotation

Sudut	PSNR (dB)	BER (%)
1°	16,4885	11,792
3°	12,4148	14,8193
5°	11,2054	25,4395
7°	10,5508	14,7461
30°	8,1249	8,6492
45°	7,7934	8,7891

Nilai BER yang dihasilkan mengalami perubahan yang tidak linear. Hal tersebut dikarenakan perubahan sudut sulit dideteksi pada saat proses sinkronisasi di sisi ekstraksi ketika frame yang disisipi watermark mengalami perubahan sudut yang kecil. Contoh hasil ekstraksi serangan rotation dapat dilihat pada Gambar 7.



Gambar 7. Hasil ekstraksi serangan rotation

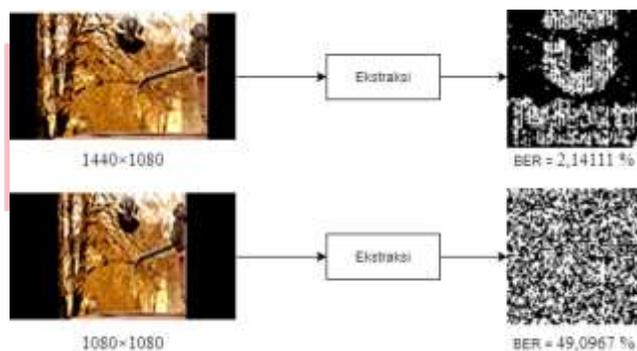
4.2.3. Pengujian terhadap serangan scaling

Scaling bertujuan untuk merubah ukuran frame video yang telah disisipi watermark. Hasil pengujian terhadap serangan scaling dapat dilihat pada Tabel 2.

Tabel 2. Hasil pengujian terhadap serangan *scaling*

Resolusi	PSNR (dB)	BER (%)
1440×1080	9,2476	2,14111
1080×1080	7,6518	49,0967
960×540	5,6411	43,0664
1728×972	8,976	16,9922
1334×756	6,6447	31,7871

PSNR yang dihasilkan setelah membandingkan antara video host dan video yang telah diberikan serangan *scaling* menghasilkan nilai yang rendah. Hal tersebut dikarenakan terjadinya perubahan yang besar terhadap *video host* setelah diberi serangan. Sedangkan BER yang dihasilkan bervariasi. Hal ini disebabkan oleh kemampuan proses sinkronisasi disisi ekstraksi untuk mengembalikan resolusi ke resolusi semula. BER maksimal terjadi ketika video diberi serangan *scaling* dengan skala (1:1). Contoh hasil ekstraksi serangan *scaling* dapat dilihat pada Gambar 8.



Gambar 8. Hasil ekstraksi serangan *scaling*

4.2.4. Pengujian terhadap serangan translation

Translation merupakan salah satu serangan geografis yang digunakan untuk menguji ketahanan *watermark* pada video yang telah disisipi *watermark*. Dalam pengujian terhadap serangan *translation* ini, dilakukan 2 jenis translasi untuk melakukan serangan yaitu *Letterboxing* dan *Pillarboxing*. Nilai hasil pengujian terhadap serangan *translation* dapat dilihat pada Tabel 3.

Tabel 3. Hasil pengujian terhadap serangan *translation*

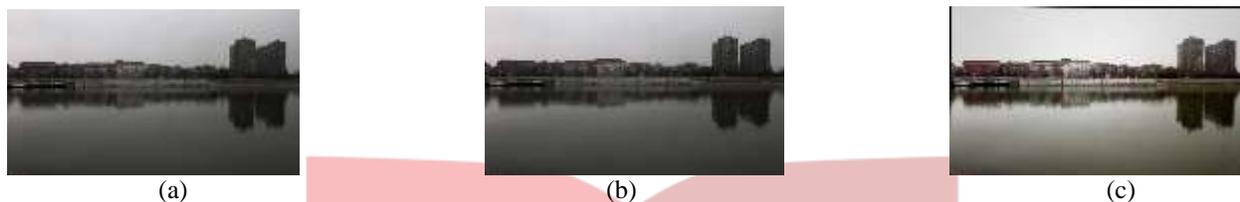
Jenis	Intensitas (%)	PSNR (dB)	BER
Letterboxing	5	13,4757	0.7813
	20	10,6223	0.7813
Pillarboxing	5	16,7785	0.7813
	20	13,005	0.7813

BER yang dihasilkan tidak berubah sama sekali. Hal tersebut dikarenakan serangan *translation* yang dilakukan tidak mengubah rasio video dan tidak merubah posisi *watermark* seperti pada serangan rotasi yang telah dilakukan sebelumnya, serta penempatan *watermark* yang tidak berada pada ujung *frame* pada video membuat serangan ini tidak berdampak sama sekali terhadap hasil ekstraksi *watermark* pada sisi ekstraksi. Sedangkan PSNR yang dihasilkan mengalami perubahan dan menghasilkan PSNR yang rendah karena terjadinya perubahan terhadap *video host* setelah diberi serangan *translation*.

4.2.5. Pengujian terhadap serangan digicam

Digicam merupakan salah satu serangan yang digunakan untuk menguji ketahanan *watermark*. Pada pengujian ini, serangan dilakukan dengan menggunakan *frame* pertama pada *watermarked video* untuk menjadi sampel untuk difoto. PSNR yang dihasilkan cukup rendah yaitu 19,1671 dB karena terjadinya perubahan yang cukup besar diantara hasil serangan *digicam* terhadap *frame host* yang disebabkan oleh keterbatasan alat serta teknik yang digunakan dalam serangan *digicam*. Setelah melakukan beberapa kali percobaan dengan menggunakan berbagai teknik pengambilan gambar, ruangan dan alat dengan spesifikasi yang berbeda-beda, akhirnya *watermark* bisa diekstraksi dengan BER yang cukup tinggi yaitu dengan nilai 34,5%. Meskipun nilai BER yang dihasilkan cukup tinggi, namun *watermark* hasil ekstraksi masih bisa dilihat cukup jelas. Kemudian serangan juga dilakukan pada

frame pertama di 3 video yang berbeda dan telah disisipi *watermark* dengan spesifikasi penyisipan yang sama dengan video sebelumnya. Contoh *frame* sebelum dan sesudah disisipi *watermark* serta setelah diberi serangan *digicam* dapat dilihat pada Gambar 9. ada Tabel 4 dapat dilihat bahwa nilai PSNR dan BER yang dihasilkan setelah menyisipkan *watermark* pada *video host* cukup baik. Perbedaan nilai tersebut dipengaruhi oleh tipe video yang digunakan sebagai *video host*. Kemudian hasil PSNR yang didapatkan setelah melakukan serangan *digicam* pada *frame* pertama video yang telah disisipi *watermark* mengalami penurunan yang besar karena terjadinya perubahan pada *frame* setelah diserang dengan serangan *digicam*. BER yang dihasilkan juga cukup besar namun masih dapat dilihat secara visual.



Gambar 9. *Frame* pertama video yang telah disisipi *watermark*: (a) *frame host*, (b) *watermarked host*, (c) setelah diserang

Tabel 4. Hasil pengujian terhadap serangan *digicam*

<i>Frame Host</i>	Sebelum diserang		Setelah diserang	
	PSNR (dB)	BER (%)	PSNR (dB)	BER (%)
Video_2	39,1682	0,8789	15,1423	22,3154
Video_3	40,5481	1,0742	21,4696	78,3912
Video_4	39,0561	0,8057	13,8000	17,9473

5. Kesimpulan dan Saran

5.1. Kesimpulan

Tugas Akhir ini telah mengusulkan teknik *video watermarking* dengan metode DT-CWT untuk mendapatkan kualitas *watermarked video* yang baik berdasarkan PSNR dan BER serta tahan terhadap serangan *camcording*. Metode DT-CWT digunakan untuk dekomposisi *video host* yang kemudian menjadi tempat penyisipan *watermark* yang disisipkan. Pada Pengujian dan analisis terhadap sistem yang telah dibuat, kualitas *watermarked video* yang tidak terlalu terganggu oleh *watermark* yang telah disisipkan. Hal ini terbukti dengan hasil pengukuran parameter performansi yang baik, yaitu dengan nilai PSNR 39,2863 dB, dan BER 0,7813% pada kondisi *watermarked video* belum diberi serangan. Namun, setelah *watermarked video* diberi serangan, terjadi perubahan yang cukup besar jika dilihat dari nilai PSNR setelah diserang dengan beberapa serangan seperti serangan geometris (rotation, scaling, dan translation). *Watermarked video* yang telah diberi serangan geometris menghasilkan nilai BER yang beragam, beberapa menghasilkan nilai yang baik dan beberapa yang lainnya menghasilkan nilai yang kurang baik. Seperti ketika *watermarked video* diberi serangan rescaling 1:1, menghasilkan BER yang maksimal yaitu dengan nilai 49,067%, sedangkan ketika *watermarked video* diberikan serangan *translation*, serangan tersebut tidak berpengaruh ke nilai BER sama sekali. Ketahanan *watermark* juga telah diuji terhadap serangan *digicam*, dimana serangan *digicam* mensimulasikan serangan *camcording*, karena serangan dilakukan hanya kepada *frame* pertama pada *watermarked video*. Serangan tersebut sangat dipengaruhi oleh spesifikasi alat yang digunakan dalam melakukan serangan, serta teknik pengambilan gambar dan intensitas cahaya pada ruangan pada saat melakukan serangan. Setelah melakukan beberapa kali percobaan melakukan serangan tersebut kepada *watermarked video*, didapatkan nilai BER setelah ekstraksi yang kurang baik, namun masih bisa terlihat secara kasat mata.

5.2. Saran

Setelah dilakukan pengujian dan analisis terhadap sistem yang telah dibuat, terdapat beberapa bahan evaluasi, maka dari itu beberapa saran, yaitu menggunakan metode penyisipan yang lain karena metode yang telah digunakan masih menghasilkan BER yang cukup tinggi setelah diberi serangan. Penggunaan alat dan teknik pengambilan gambar serta spesifikasi ruangan yang sangat baik untuk melakukan serangan *camcording* maupun *digicam* agar meminimalisir kerusakan yang terjadi pada *watermarked media*.

DAFTAR PUSTAKA

- [1] M. Asikuzzaman and M. R. Pickering, "An Overview of Digital Video Watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, 2018, doi: 10.1109/TCSVT.2017.2712162.
- [2] G. Budiman, L. Novamizanti and I. Iwut, "Genetics algorithm optimization of DWT-DCT based image Watermaking," *Journal of Physics: Conference Series*, vol. 795, 2017.
- [3] Y. Hafizhana, I. Safitri, L. Novamizanti and N. Ibrahim, "Image Watermarking pada Citra Medis menggunakan Compressive Sensing berbasis Stationary Wavelet Transform," *ELKOMIKA*, vol. 8, no. 1, 2020.
- [4] M. D. Godole, L. Novamizanti and I. N. A. Ramatryana, "RS Code and Compressive Sampling on Video Watermarking-based DWT-SVD," in 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, November 2019.
- [5] L. R. Shiddik, L. Novamizanti, I. N. A. N. Ramatryana and H. A. Hanifan, "Compressive Sampling for Robust Video Watermarking based on BCH Code in SWT-SVD Domain," in 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC), Bandung, Augustus 2019.
- [6] I. Iwut and L. Novamizanti, "Optimization of discrete cosine transform-based image watermarking by genetics algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 1, pp. 91-103, 2016.
- [7] Y. Yunawan, I. Safitri and L. Novamizanti, "Compressive Sensing for Image Watermarking Discrete Wavelet Transform and Spread Spectrum," in 2018 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, December 2018.
- [8] L. Novamizanti, A. L. Prasasti and I. F. N. Kiranda, "Comparison of discrete cosine transform and dual-tree complex wavelet transform based on arithmetic coding in medical image compression," *Journal of Physics: Conference Series* 1367 (1), 012021
- [9] L. Novamizanti and A. Kurnia, "Analisis Perbandingan Kompresi Haar Wavelet Transform dengan Embedded Zerotree Wavelet pada Citra," *ELKOMIKA*, vol. 3, no. 2, 2015.
- [10] F. Hartung, "Multimedia watermarking techniques," *Proc. IEEE*, vol. vol, no. 7, pp. 87no7pp1079–1107, 2002, [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=771066.
- [11] D. Society, "A Improved Video Watermarking Scheme Based on Spread-spectrum Technique Video Encoder Video Decoder," *Engineering*, pp. 511–514, 2010.
- [12] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Imperceptible and robust blind video watermarking using chrominance embedding: A set of approaches in the DT CWT domain," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 9, pp. 1502–1517, 2014, doi: 10.1109/TIFS.2014.2338274.
- [13] A. Samcovic and M. Milovanovic, "Robust digital image watermarking based on wavelet transform and spread spectrum techniques," 2015 23rd Telecommun. Forum, TELFOR 2015, pp. 811–814, 2016, doi: 10.1109/TELFOR.2015.7377589.
- [14] D. Jiao, Y. Xue, C. Wang, and F. Gao, "Dual-tree complex wavelet transform blind video watermark based on complete complementary codes," 2014 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2014, pp. 250–253, 2014, doi: 10.1109/ICSPCC.2014.6986192.
- [15] M. Asikuzzaman, M. J. Alam, A. J. Lambert, and M. R. Pickering, "Robust DT CWT-based DIBR 3D Video watermarking using chrominance embedding," *IEEE Trans. Multimed.*, vol. 18, no. 9, pp. 1733–1748, 2016, doi: 10.1109/TMM.2016.2589208.
- [16] F. C. Chang and H. C. Huang, "Discussions on capturing a watermarked image on an LCD monitor," 2019 IEEE 1st Glob. Conf. Life Sci. Technol. LifeTech 2019, pp. 141–144, 2019, doi: 10.1109/LifeTech.2019.8884044.
- [17] Z. S. Veličković, Z. N. Milivojević, and M. Z. Veličković, "A secured digital video watermarking in chrominance channel," 2018 23rd Int. Sci. Conf. Inf. Technol. IT 2018, vol. 2018-January, pp. 1–4, 2018, doi: 10.1109/SPIT.2018.8350858.
- [18] A. T. Nasrabadi, M. A. Shirsavar, A. Ebrahimi, and M. Ghanbari, "Investigating the PSNR calculation methods for video sequences with source and channel distortions," *IEEE Int. Symp. Broadband Multimed. Syst. Broadcast. BMSB*, vol. 0, pp. 0–3, 2014, doi: 10.1109/BMSB.2014.6873482.
- [19] R. Munir, "Comparison of secret color image sharing based on XOR operation in RGB and YCbCr color model," *Proc. 2017 6th Int. Conf. Electr. Eng. Informatics Sustain. Soc. Through Digit. Innov. ICEEI 2017*, vol. 2017-Novem, pp. 1–6, 2018, doi: 10.1109/ICEEI.2017.8312445.
- [20] I. W. Selesnick, R. G. Baraniuk, and N. G. Kingsbury, "The dual-tree complex wavelet transform," *IEEE Signal Process. Mag.*, vol. 22, no. 6, pp. 123–151, 2005, doi: 10.1109/MSP.2005.1550194.