

**PERANCANGAN DAN SIMULASI SISTEM WATERMARKING TERKOMPRESI
LWT-FFT PADA VIDEO YANG DIKOMPRESI MENGGUNAKAN COMPRESSIVE
SENSING DAN DWT**

*DESIGN AND SIMULATION COMPRESSED SYSTEM WATERMARKING LWT-FFT IN
VIDEO WHICH COMPRESSED USING COMPRESSIVE SENSING AND DWT*

Annisa Erikha Khairani¹, Iwan Iwut Tritoasmoro, S.T., M.T.², Irma Safitri, S.T., M.Sc.³

^{1,2,3} Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

¹annisaerikha99@gmail.com ²iwaniwuttritoasmoro@telkomuniversity.ac.id

³irmasaf@telkomuniversity.ac.id

Abstrak

Saat ini penyebaran data berbentuk video digital melalui internet menjadi hal yang sangat umum. Seperti cuplikan film, video klip dan video produk-produk komersial. Video yang disebarluaskan ini perlu diproteksi untuk menghindari penyalahgunaan yang tidak diinginkan seperti pembajakan hak cipta. Salah satu cara untuk menghindari hal ini adalah video watermarking. Video *watermarking* merupakan suatu penyisipan *watermark* pada video sebagai ciri khas hak cipta untuk menandai kepemilikan video. Tugas Akhir ini dirancang menggunakan *software MATLAB* dengan *Compressive Sensing (CS)* dan *Discrete Wavelet Transform (DWT)* sebagai kompresi citra image watermark untuk memperkecil ukuran file citra. Lalu digunakan metode *Lifting Wavelet Transform (LWT)* untuk mengubah video host menjadi beberapa sub-band, *Fast Fourier Transform (FFT)* untuk mengubah sinyal ke domain frekuensi agar tahan terhadap serangan-serangan dan penyisipan *Quantization Index Modulation (QIM)* sebagai metode penyisipan. Hasil pengujian dengan digunakan CS Measurement Rate 80% dan menghasilkan nilai BER 0,234 dari pengujian terhadap sample video yang memiliki *imprecentibility*, *capacity* dan *robustness* yang cukup baik. Pengujian MOS mendapatkan hasil nilai tertinggi pada skenario 1 yaitu baik 45%, skenario 2 yaitu sangat baik 30%, skenario 3 sangat baik 45%, dan skenario 4 baik 50%, skenario 5 cukup 40%, skenario 6 cukup 40%.

Kata kunci : *Video watermarking, Compressive Sensing, DWT, LWT, FFT*

Abstract

Nowadays the dissemination of data in the form of digital video over the internet has become a very common occurrence. Such as film footage, video clips and videos of commercial products. This widely distributed video needs to be protected to avoid unwanted misuse such as copyright piracy. Video watermarking is an insertion of watermark on the video as a copyright characteristic to mark the ownership of the video. In this final project designed a system using MATLAB software with *Compressive Sensing (CS)* and *Discrete Wavelet Transform (DWT)* as compression image watermark to reduces the file. And *Lifting Wavelet Transform (LWT)* method to change video host into several sub-band and *Fast Fourier Transform (FFT)* to change the signal to domain frequency in order to be resistant toward attacks and *Quantization Index Modulation (QIM)* as embedding method. The results of testing in this final project used CS Measurement Rate for 80% and produce the value of BER with average of 0,234 from testing towards sample video which has a good imprecentibility, capacity and robustness. MOS testing get the highest score in scenario 1 good 45%, scenario 2 very good 30%, scenario 3 very good 45%, scenario 4 good 50%, scenario 5 enough 40%, scenario 6 enough 40%.

Keywords : *Video watermarking, Compressive Sensing, DWT, LWT, FF*

1. Pendahuluan

Perkembangan teknologi yang pesat mempengaruhi banyak bidang, salah satunya adalah media digital. Media digital telah menggantikan peran media analog dan lainnya. Hal ini disebabkan oleh kelebihan yang dimiliki media digital. Namun, terdapat satu kelemahan dari penggunaan media digital, yaitu pembajakan dan perlindungan hak cipta. Pembajakan video adalah kegiatan memperoleh, menyalin, memproduksi dan menjual atau mendistribusikan video yang telah memiliki hak cipta tanpa persetujuan dari pemilik hak cipta yang merupakan tindakan kriminal. Pembajakan video online telah menjadi perhatian bagi produsen film.

Pembajakan tentu saja sangat merugikan bagi penciptanya, oleh karena itu pemilik hak cipta membutuhkan teknologi yang dapat melindungi karyanya dari pembajakan atau penyalahgunaan lainnya. Salah satu metode perlindungan hak cipta adalah dengan menggunakan teknik *watermarking*. *Watermarking* merupakan salah satu cabang dari ilmu *steganography*, yaitu teknik penyisipan informasi kedalam media data digital seperti citra, audio dan video secara rahasia [1].

Digital *watermarking* dikembangkan sebagai salah satu jawaban dari keresahan untuk mempertahankan keaslian hak cipta. Teknik *watermarking* bekerja dengan menyisipkan sedikit informasi berupa sinyal atau pola digital yang menunjukkan kepemilikan terhadap media digital tanpa mempengaruhi kualitasnya [2]. *Watermark* haruslah bersifat *imperceptible* atau tak dapat dilihat/tidak terdeteksi oleh indera penglihatan (*human visual system/HVS*) atau indera pendengaran (*human auditory system/HAS*). Dan dokumen asli dan watermark kita simpan dan rahasiakan, dokumen yang sudah disisipi *watermark* bisa dipublikasikan. *Video watermarking* merupakan suatu penyisipan *watermark* pada video sebagai ciri khas hak cipta untuk menandai kepemilikan video. Metode yang digunakan adalah metode *Compressive Sensing* (CS) dan *Discrete Wavelet Transform* (DWT) untuk pengompresian *image watermark*. Lalu digunakan metode *Lifting Wavelet Transform* (LWT) untuk mengubah video host menjadi beberapa sub-band, *Fast Fourier Transform* (FFT) untuk mengubah sinyal ke domain frekuensi agar tahan terhadap serangan-serangan dan penyisipan *Quantization Index Modulation* (QIM) sebagai metode penyisipan atau *embedding*. Dari hasil video *watermarking* tersebut, akan diukur parameter objektif menggunakan *Peak Signal to Noise Ratio* (PSNR), *Mean Square Error* (MSE) dan *Bit Error Rate* (BER), kemudian dilakukan penilaian secara subjektif menggunakan parameter *Mean Opinion Score* (MOS) untuk menentukan kualitas *watermark* yang telah di ekstraksi.

2. Dasar Teori

2.1. Video Digital

Video digital adalah jenis sistem video recording yang bekerja menggunakan sistem digital. Dibandingkan dengan video analog dalam hal representasi videonya. Biasanya, digital video direkam kedalam pita rekaman, kemudian didistribusikan melalui optical disc, misalnya VCD dan DVD. Salah satu alat yang dapat digunakan untuk menghasilkan video digital adalah *camcorder*, yang digunakan untuk merekam gambar video dan audio.

Video yang digunakan pada Tugas Akhir ini adalah video berformat MP4.

2.2 Digital Watermarking

Digital Watermarking adalah suatu teknik untuk menanamkan data atau informasi kriptografi ke dalam elemen multimedia, yaitu teks, gambar audio, dan video untuk melindungi hak cipta informasi [3].

2.3. Compressive Sensing (CS)

Compressive Sensing (CS) adalah sebuah metode kompresi dimana sample dengan jumlah yang lebih kecil yang diperoleh dari seluruh panjang sinyal *sparse* dengan mengambil pengukuran *non-adaptive* linier yang memperthankan struktur dari sinyal, dan menggunakan metode optimasi numerik, sinyal asli direkonstruksi dari pengukuran dengan jumlah yang lebih kecil. CS dapat merekonstruksi sinyal dengan menggunakan sejumlah pengukuran acak dan sinyal yang akan direkonstruksi harus *sparse*. Sinyal yang *sparse* mengandung beberapa koefisien sebagai *non-zero* dan koefisien lainnya adalah *zero* [4].

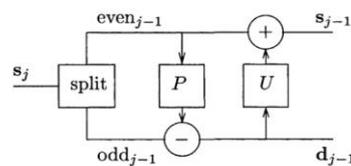
2.4. Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform mengubah sinyal waktu diskrit ke diskrit representasi wavelet. Wavelet digunakan untuk menganalisis bentuk sinyal gelombang sebagai kombinasi waktu dan frekuensi [3]. Sinyal pertama kali dilewatkan ke serangkaian sinyal *high pass filter* dan *low pass filter*. Setengah dari setiap output sinyal adalah sampel melalui operasi sub-sampling.

Transformasi wavelet dapat memberikan informasi tentang skala atau durasi waktu. Analisis data menjadi komponen frekuensi yang berbeda sesuai dengan skala resolusi. Cara mendapatkan representasi waktu dan skala sinyal menggunakan teknik subsampling operasi yaitu prinsip dasar DWT [5].

2.5 Lifting Wavelet Transform (LWT)

Watershed Menurut teori Wim Swelden pada tahun 1994 Lifting Wavelet Transform adalah sebuah metode yang dapat digunakan untuk membangun wavelet. Metode ini memiliki sifat dapat mentransformasikan multi resolusi karakter dan tidak bergantung pada transformasi fourier. LWT dianggap mampu menyelesaikan permasalahan transformasi wavelet di domain frekuensi secara langsung, dengan algoritma yang sederhana, operasi yang cepat dan permintaan memori yang kecil. Ada tiga tahapan yang digunakan pada metode LWT ini, diantaranya sebagai berikut [6]:



Gambar 1. Tiga langkah dalam proses blok Lifting Wavelet Transform

LWT adalah sebuah pendekatan alternatif untuk DWT untuk mengubah gambar ke domain frekuensi untuk aplikasi real time. Lifting wavelet adalah generasi kedua fast wavelet transform. Dalam lifting transformasi wavelet, naik dan turun sampling digantikan hanya dengan split dan menggabungkan di masing-masing tingkat. Komponen polyphase dari sinyal yang disaring secara paralel dengan koefisien filter wavelet yang sesuai, menghasilkan hasil yang lebih baik daripada up dan down sampling yang diperlukan dalam pendekatan DWT tradisional. Dibandingkan dengan wavelet umum, rekonstruksi citra dengan mengangkat wavelet baik karena, meningkatkan kelancaran dan mengurangi efek aliasing. Menggunakan LWT mengurangi kehilangan informasi, meningkatkan keutuhan tertanam watermark pada gambar dan membantu meningkatkan kekokohan watermark. [7]

2.6 Fast Fourier Transformation (FFT)

Fast Fourier Transform merupakan suatu algoritma penyempurnaan dari *Discrete Fourier Transform* (DFT), dimana FFT dapat menghitung algoritma *Fourier* diskrit dengan tingkat kompleksitas yang cukup rendah dan waktu komputasi yang cepat. FFT adalah teknik yang diperkenalkan oleh Gauss pada tahun 1805 untuk menghitung koefisien di dalam ekspansi trigonometri orbit asteroid [8]. Fungsi dari FFT adalah untuk mengubah sinyal dari domain waktu kedalam domain frekuensi untuk mengoperasikan FFT dibutuhkan transformasi *fourier aperiodic* dalam waktu diskrit. FFT sering diterapkan dalam beragam bidang terutama dalam pengolahan sinyal digital [9]. Formula untuk FFT seperti persamaan dibawah ini:

$$X(k) = \sum_{n=0}^{N-1} x(n)e^{-j\left(\frac{2\pi k}{N}\right)n} \quad (5)$$

$$W_N = e^{-j\frac{2\pi}{N}} \quad (6)$$

dengan $k = 0, \dots, N-1$ $n = 0, \dots, N-1$

Nilai $X(k)$ adalah nilai transformasi domain, $x(n)$ adalah nilai block media digital, sedangkan

N adalah jumlah data yang akan diubah ke domain frekuensi.

Algoritma FFT bekerja dengan cara membagi data menjadi indeks ganjil dan genap seperti formula dibawah ini:

$$X(k) = \sum_{n=0}^{N-1} x(n)W_N^{kn} \tag{7}$$

$$X(k) = \sum_{\text{genap}}^{(N-2)-1} x(n)W_N^{kn} + \sum_{\text{ganjil}}^{(\frac{N}{2})-1} x(n)W_N^{kn} \tag{8}$$

2.7 Quantization Index Wavelet (QIM)

Metode watermarking dengan skema *Quantization Index Modulation* diperkenalkan oleh Brian Chen dan Gregory W. Wornell pada tahun 1999. QIM adalah suatu metode penyisipan pada watermark. Teknik ini dianggap dapat memberi keseimbangan antara ketahanan atau *robustness* dan transparansi atau *transparency*.

Kuantisasi pada dasarnya dapat diterapkan di domain waktu atau frekuensi atau setelah proses transformasi. Penyisipan dilakukan data watermark pada nilai maksimal sinyal. Penggunaan parameter dengan nilai yang diubah-ubah untuk mencari hasil penyisipan terbaik dengan menggunakan delta (Δ).

Pada metode ini akan digunakan untuk proses *embedding* dan *extraction*. Berikut ini adalah persamaan untuk proses *embedding*:

$$\text{Delta } (\Delta) = \frac{1}{2^{(n-1)}} \tag{9}$$

$$F'(0) = \begin{cases} A_k, & \text{if } w=1 \\ B_k, & \text{if } w=0 \end{cases} \text{ and } \arg \min \|F(0) - Ak\| \tag{10}$$

$$A_k = \left(2k + \frac{1}{2}\right)\Delta, B_k = \left(2k - \frac{1}{2}\right)\Delta, k = 0, \pm 1, \pm 2, \dots \tag{11}$$

Berikut ini adalah persamaan untuk proses *extraction*:

$$\tilde{v}(k) = \text{mod} \left(\left\lceil \frac{F'(0)}{\Delta} \right\rceil, 2 \right) \tag{12}$$

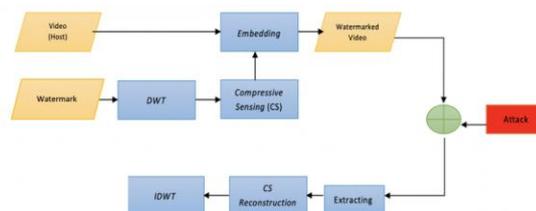
Keterangan:

- Δ : selisih perubahan amplituda setelah di kuantisasi
- $F'(0)$: sinyal ter-watermarked
- $F(0)$: sinyal asli

3. Model dan Perancangan Sistem

3.1 Perancangan Sistem

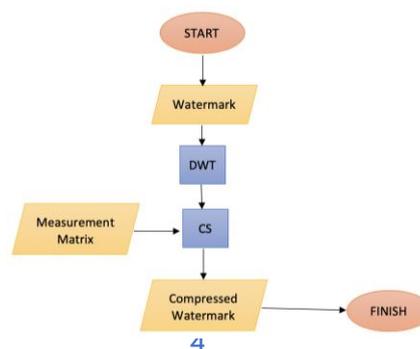
Sistem dirancang menggunakan Matlab 2017 dengan tahapan-tahapan sesuai dengan Gambar 2 berikut :



Gambar 2. Desain Sistem Video Watermarking

3.2 Proses Kompresi Watermark

Proses kompresi watermark pada penelitian ini menggunakan Compressive Sensing. Tahapan kompresi dapat dilihat pada gambar di bawah ini.

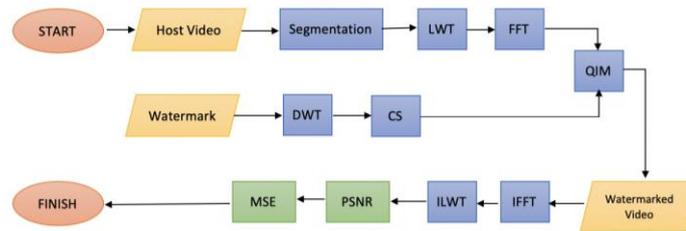


Gambar 3. Proses *Kompresi Watermark dengan CS*

Watermark sebagai input awal proses diberikan proses DWT untuk mendapatkan dan memisahkan frekuensi menjadi frekuensi rendah dan tinggi. Yang digunakan pada DWT merupakan wavelet jenis "Haar". Hasil transformasi ini adalah sinyal *sparse* yang akan menjadi sinyal yang dikompresi. Proses kompresi terjadi pada proses *measurement* dimana nilai sampling dari sinyal *sparse* direduksi menjadi ukuran matriks yang lebih kecil sesuai dengan ukuran matriks *watermark*.

3.3 Embedding

Tahap *Embedding* adalah proses menyisipkan image yang sudah terwatermark pada video asli host yang akan menghasilkan video terwatermark (*watermarked video*).



Gambar 4. Proses *Embedding Watermark*

1. Membaca file video (*host*).
2. Dilakukan proses segmentasi. Segmentasi dilakukan guna membagi host video kedalam beberapa frame dan durasi yang dihasilkan dari proses segmentasi bergantung pada jumlah frame yang diinginkan.
3. Sinyal yang telah di segmentasi dilakukan dekomposisi pada *low frequency* $[X_L(n)]$ dan *high frequency* $[X_H(n)]$ dengan membagi ke dalam elemen ganjil dan elemen genap yang dijadikan sub-band pada proses transformasi LWT.

$$P_{low} = \sum_{i=1}^n X_L^2(i) \tag{13}$$

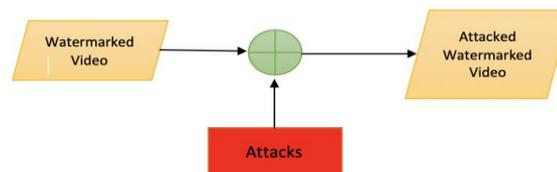
$$P_{high} = \sum_{i=1}^n X_H^2(i) \tag{14}$$

Proses LWT bergantung pada level LWT yang diterapkan dan jika yang digunakan LWT level 2 pada setiap frame maka akan didapatkan keluaran 4 komponen, yaitu, LL, LH, HL dan HH. Dipilih salah satu subband (HH) yang akan dilakukan pada proses selanjutnya.

4. Pada metode FFT, host akan ditransformasikan yang awalnya dalam domain waktu menjadi dalam domain frekuensi.
5. Watermark yang telah dikompresi (*Compressed Watermark*) disisipkan dengan keluaran FFT yang berupa host video yang telah melewati proses LWT dan FFT menggunakan metode QJM. Menghasilkan *watermarked video*.
6. *Re-adjust* kembali file video host dengan *invers* FFT untuk mengembalikan file video host ke domain waktu.
7. Dan proses *invers* LWT untuk mengembalikan *sub-band* yang tidak di proses sebelumnya. Untuk mendapatkan hasil keluaran ILWT yang merupakan hasil *watermarked video*.
8. Menghitung parameter kualitas PSNR dan MSE.

3.4 Attacks

Attacking adalah proses penyerangan dan pengecekan terhadap sistem watermarking dengan beberapa jenis penyerangan. Proses ini dilakukan untuk membuktikan seberapa kuat dan tahan sistem watermark yang dirancang terhadap serangan yang biasanya terjadi.



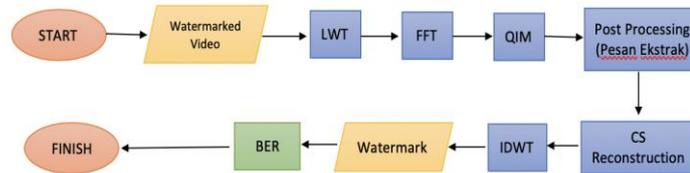
Gambar 5. Proses *Attacking*

Pada Gambar 5 menjelaskan proses *attacking* pada sistem *watermark* yang dilakukan pada Tugas Akhir ini. Proses *attacking* merupakan proses penyisipan watermark ke dalam host. Pada proses

attacking ini digunakan beberapa jenis serangan yang sering terjadi.

3.5 Extraction

Tahap Proses Ekstraksi adalah proses yang pada sistem watermarking yang berfungsi untuk memisahkan host dengan watermark yang telah disisipi sebelumnya.



Gambar 6. Proses *Extracting Watermark*

Pada Gambar 6 menjelaskan proses *extracting* watermark yang dilakukan pada Tugas Akhir ini. Proses ekstraksinya sebagai berikut:

1. Membaca file video terwatermark.
2. Algoritma LWT melakukan segmentasi dan dekomposisi ke beberapa *sub-band*.
3. Metode FFT untuk mengubah domain video host dari domain waktu ke domain frekuensi.
4. Ekstraksi dilakukan untuk memisahkan host dengan watermark menggunakan ekstrak QIM.
5. Proses pengembalian dilakukan dengan cara IFFT dan ILWT.
6. Didapatkan hasil dari ekstrak QIM berupa bit pesan.
7. Proses rekonstruksi CS dan IDWT pada watermark hasil ekstraksi menjadi citra watermark asli.
8. Didapatkan hasil *watermark* dan dapat dilakukan proses menghitung nilai parameter *Bit Error Rate* (BER).

3.4 Mean Square Error (MSE)

Mean Square Error adalah parameter yang digunakan untuk mengukur tingkat kesalahan pada watermarking video. MSE digunakan untuk mengukur jumlah maksimal karakter yang bias disisipkan dan mengukur tingkat kesalahan pada frame video yang telah disisipi data *hiding*. MSE dapat dinyatakan dengan persamaan berikut:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [f(i,j) - g(i,j)]^2 \quad (15)$$

3.5 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) merupakan tinjauan kualitas sebuah video secara objektif. PSNR digunakan untuk menggambarkan degradasi sebuah video akibat dari noising, encoding, kompresi atau error transmisi. PSNR digunakan untuk mengukur secara objektif kualitas video terwatermark. PSNR dapat digunakan untuk mengukur seberapa baik kualitas dari metode watermark yang digunakan. Semakin besar nilai PSNR maka akan semakin baik kualitas dari metode tersebut. Perhitungan PSNR dapat dicari dengan rumus sebagai berikut.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\sqrt{MSE}} \right) dB \quad (16)$$

3.6 Mean Opinion Score (MOS)

Mean Opinion Score (MOS) merupakan pengukuran yang digunakan dalam domain kualitas pengalaman atau pengamatan dan teknik telekomunikasi, yang mewakili kualitas keseluruhan dari stimulus atau sistem. Penilaian secara subjektif rata-rata aritmatika atas semua individu terhadap nilai pada skala yang telah ditentukan Pada Tugas Akhir ini dibagi menjadi 5 kategori yaitu, Sangat Baik, Baik, Cukup, Buruk, dan Sangat Buruk.

4. Analisis Hasil Pengujian

Pengujian sistem dilakukan untuk mengetahui seberapa baik performansi sistem yang telah dirancang. Citra yang digunakan untuk watermark pada pengujian ini yaitu citra black and white dan grayscale dengan format *.png yang masing-masing berukuran 256x256.





Gambar 6 (a) citra watermark 1 grayscale dan biner (b) citra watermark 2 grayscale dan biner (c) citra watermark 3 grayscale dan biner

Performansi tersebut dapat diketahui dengan melakukan analisis terhadap beberapa skenario parameter yaitu :

1. Parameter jenis video host
2. Parameter ukuran resolusi frame video host
3. Parameter ukuran resolusi pesan citra yang akan disisipkan
4. Parameter jenis pengukuran kualitas yang digunakan

4.1 Hasil Pengujian dan Analisis

4.1.1 Hasil pengujian kualitas video watermarking yang telah disisipkan watermark menggunakan parameter MSE dan PSNR

Tabel 1. Hasil Pengujian terhadap Pengukuran Kualitas Video Host 1

parameter	watermark 1		watermark 2		watermark 3	
	bw	gs	bw	gs	bw	gs
MSE	0,00099	0,01616	0,00015	0,314158	0,00338	0,01234
PSNR(dB)	30,0357	57,0874	38,1648	50,6451	24,7013	57,6792

Tabel 2. Hasil Pengujian terhadap Pengukuran Kualitas Video Host 2

parameter	watermark 1		watermark 2		watermark3	
	bw	gs	bw	gs	bw	gs
MSE	0,00199	0,01634	0,00044	0,31437	0,00301	0,01238
PSNR(dB)	26,9921	57,0645	33,5408	50,2201	25,2201	57,6666

Berikut ini adalah data hasil pengujian skenario pengujian 1 yang dijabarkan pada Tabel 1 dan Tabel 2, Tabel 1 merupakan hasil pengujian terhadap pengukuran kualitas video menggunakan parameter MSE dan PSNR pada video host 1 dan pada Tabel 2 merupakan hasil pengujian terhadap pengukuran kualitas video menggunakan parameter MSE dan PSNR pada video host 2. Dari tabel diatas dapat disimpulkan bahwa perbandingan nilai MSE dan PSNR pada Video Host 1 dan Video Host 2 yang telah disisipkan watermark tidak terlalu jauh. Hasil pengukuran kualitas Video Host 1 dan 2 yang telah disisipkan watermark baik *black and white* atau *grayscale* memiliki hasil nilai parameter MSE dan PSNR yang bagus dengan rata-rata nilai PSNR diatas 40dB.

4.1.2 Hasil pengujian kualitas video watermarking yang telah diekstraksi menggunakan parameter BER

Tabel 3. Pengukuran Kualitas Video Host 1 menggunakan Parameter BER

parameter	watermark 1		watermark 2		watermark 3	
	bw	gs	bw	gs	bw	gs
BER	0,00099	0,15006	0,00015	0,52661	0,00338	0,17549
Waktu (s)	1,0833	1,2787	1,8918	1,3454	1,0348	1,2028

Tabel 4. Pengukuran Kualitas Video Host 2 menggunakan Parameter BER

parameter	watermark 1		watermark 2		watermark 3	
	bw	gs	bw	gs	bw	gs
BER	0,00199	0,14973	0,00044	0,52830	0,00301	0,18448
Waktu (s)	1,0631	1,3051	1,2399	1,3121	0,9900	1,5429

Berikut ini adalah data hasil pengujian scenario pengujian 2 yang dijabarkan pada Tabel 3 dan Tabel 4, Tabel 3 merupakan hasil pengujian terhadap pengukuran kualitas video menggunakan parameter BER pada video host 1 setelah di ekstraksi dan pada Tabel 4 merupakan hasil pengujian terhadap pengukuran kualitas video menggunakan parameter BER pada video 2 setelah di ekstraksi. Nilai parameter BER setelah diekstraksi menghasilkan nilai pengukuran yang sangat baik dengan waktu yang sangat cepat

dengan nilai terbaik 0.00015 pada *watermark 2 black and white*.

4.1.3 Hasil pengujian ketahanan sistem watermarking saat diberi gangguan

1. AWGN (*Additive White Gaussian Noise*)

AWGN atau *Additive White Gaussian Noise* adalah model *noise* yang digunakan pada teori informasi untuk menirukan efek dari proses-proses acak yang terjadi di alam. Noise AWGN juga merupakan noise yang pasti terjadi dalam jaringan nirkabel manapun, memiliki sifat-sifat *additive*, *white*, dan *gaussian*. Sifat *additive* dikarenakan ditambahkan ke setiap suara yang mungkin *intrinsic* ke sistem informasi. *White* mengacu pada gagasan bahwa ia memiliki kekuatan yang seragam melintasi pita frekuensi untuk sistem informasi. Ini adalah analogi dengan warna putih yang memiliki emisi seragam pada semua frekuensi dalam spektrum yang terlihat. Dan *gaussian* karena memiliki distribusi normal dalam domain waktu dengan nilai domain waktu rata-rata nol.

Pada pengujian ini yang digunakan adalah video host terbaik yaitu host 1 dan citra watermark terbaik yaitu watermark 2 *black white*.

Tabel 5. Hasil Pengukuran Kualitas Video dengan Serangan AWGN

Parameter	MSE	PSNR	BER	Waktu Proses (s)
AWGN	0,3830	4,1677 dB	0,3830	1,5999

Pada pengujian serangan AWGN sistem akan diserang dengan noise yang menirukan efek atau gangguan yang berada di alam pada tabel 5. Pada pengujian AWGN mendapatkan hasil yang cukup dinilai dari hasil BER dengan toleransi 0,3. Hasil setelah mengalami serangan AWGN dan rekontruksi sedikit buruk/rusak tetapi masih dapat dilihat atau berpola. Disimpulkan sistem pada tugas akhir ini tahan terhadap serangan AWGN.

2. Rescalling

Rescalling yaitu serangan dengan cara mengubah ukuran citra yang asli ke ukuran yang lebih besar atau lebih kecil dari citra aslinya. Apabila citra asli setelah di rescalling menjadi ukuran lebih kecil dari citra Awal, maka ada pengurangan pixel pada saat proses rescalling. Pada penelitian ini akan dilakukan analisis ketahanan sistem terhadap serangan rescalling dengan nilai 0,25 dan 0,5.

Pada pengujian ini yang digunakan adalah video host terbaik yaitu host 1 dan citra watermark terbaik yaitu watermark 2 *black white*.

Tabel 6. Hasil Pengukuran Kualitas Video dengan Serangan Rescalling

Parameter	Ratio	MSE	PSNR (dB)	BER	Waktu (s)
<i>Rescalling</i>	0,25	0,392319	4,06361	0,39232	1,36389
	0,5	0,38760	4,11612	0,38760	1,37246

Pada pengujian serangan rescalling sistem akan mengalami penurunan host asli sesuai dengan ratio resize yang telah ditentukan. yaitu ratio 0.25 dan 0.5, Pada tabel 6. Pada pengujian rescalling mendapatkan hasil yang bervariasi saat kondisi ratio 0.25 dan 0.5 mendapatkan hasil yang cukup dengan toleransi BER 0.3, saat file host asli mengalami penurunan 0.25 dan 0.5 nilai BER adalah 0.3 dan gambar masih dapat terlihat dan berpola. Namun rata-rata BER dari kedua ukuran cenderung cukup dan gambar watermark setelah rekontruksi rata-rata masih dapat terlihat oleh mata dan berpola. disimpulkan sistem pada tugas akhir ini tahan terhadap serangan *rescalling*.

5. Kesimpulan

5.1 Kesimpulan

Tugas Akhir ini telah mengusulkan perancangan sistem watermarking dengan watermark yang dikompresi menggunakan CS DWT dan disisipkan pada host berupa video dengan menggunakan metode penyisipan QIM yang telah melewati proses LWT dan FFT.

Terdapat beberapa kesimpulan yang dihasilkan dari analisis pada skenario pengujian yang telah dilakukan pada Tugas Akhir ini. Berikut adalah beberapa kesimpulan:

1. Pada saat menggunakan CS dengan *Measurement Rate* 10-40% menghasilkan hasil yang sulit dilihat oleh kasat mata gambar rekontruksi watermark karena memiliki rata-rata nilai BER diatas 0,2.
2. Pada saat menggunakan CS dengan *Measurement Rate* 50-90% menghasilkan hasil yang dapat dilihat oleh kasat mata gambar rekontruksi watermark karena memiliki rata-rata nilai BER

- dibawah 0,2.
3. Pengujian serangan AWGN (*Additive White Gaussian Noise*) mendapatkan nilai BER 0.38675. Sistem Tugas Akhir ini tahan terhadap serangan AWGN.
 4. Pengujian serangan *Scalling* dengan *ratio resize* 0.25 dan 0.5 mendapatkan nilai BER 0,392319 dan 0,387604. Sistem Tugas Akhir ini cukup tahan terhadap serangan *scalling*.
 5. Pengujian MOS mendapatkan hasil nilai tertinggi pada skenario 1 yaitu baik 45%, skenario 2 yaitu sangat baik 30%, skenario 3 sangat baik 45%, dan skenario 4 baik 50%, skenario 5 cukup 40%, skenario 6 cukup 40%.
 6. Pengamatan subyektif dari hasil kualitas watermark setelah di rekontruksi dengan watermark aslinya rata-rata baik terlihat baik walaupun masih ada sedikit bagian yang kurang jelas atau kabur.

DAFTAR REFERENSI

- [1] Putro, B. 2016. "Aplikasi watermarking dengan Metode Least Signifivant Bit menggunakan MATLAB," *Jurnal Informatika dan Komputer*, vol.21, no.3.
- [2] P. Agung, Wiseto. 2001. "Digital Watermarking: Teknologi Pelindung HAKI Multimedia," *Elektro Indonesia*.
- [3] L. R. Shiddik, L. Novamizanti, I. N. A. N. Ramatryana, H. A. Hanifan. Compressive Sampling for Robuat Video watermarking based on BCH Code in SWT-SVD Domain. 2019 International Conf. on Sustainable Engineering and Creative Computing (ICSECC).
- [4] Bash, A. A. H. K. and Kayhan, S. K. 2015. "Watermarked Compressive Sensing Measurement Reconstructed by the Greedy Algorithms," *Internation Journal of Computer Theory and Engineering*, vol.7, no.3, p.219-222.
- [5] Y. Yunawan, I. Safitri, L. Novamizanti. Compressive Sensing for Image Watermarking Discrete Wavelet Transform and Spead Spectrum. 2018 International Conference on Control, eletronics, renewable Energy and Communication (ICCEREC).
- [6] Andraini, T. 2019. "Perancangan dan Analisis CompressiveSampling pada Watermarking Audio Stereo berbasis QIM dengan Teknik Gabungan LWT-FFT-SVD," *Jurnal Telkom University*.
- [7] P. B. Santoso, R. D. Atmaja, I. Safitri, "Analisis dan Implementasi Citra Watermarking dengan Metode Discrete Wavelet Transform (DWT) – Lifting Wavelet Transform (LWT) dan Singular Value Decomposition (SVD)," *eProceedings of Engineering*, vol. 5, no. 1, April 2018.
- [8] S. N. Neyman, I. N. P. Pranyana, and B. Sitohang. 2014. "A New Copyright Protection for Vector Map using FFT based Watermarking," *TELKOMNIKA Telecommunication Comp. Electron. Control.*, vol. 12, no.2, p.367.