

# SISTEM WATERMARKING INTEGRITAS DATA BERBASIS GAMBAR DENGAN MENGGUNAKAN METODE SPREAD SPECTRUM DAN ERROR CORRECTION CODES (ECC) BOSE-CHAUDHURI-HOCQUENGHEM (BCH) UNTUK TELEMEDIS

## WATERMARKING SYSTEM DATA INTEGRITY BASED ON PICTURE USING SPREAD SPECTRUM AND EROR CORRECTION CODES (ECC) BOSE-CHAUDHURI-HOCQUENGHEM (BCH) METHODS FOR TELEMEDIC

Putri Nian Sari<sup>1</sup>, Dr.Ida Wahidah,S.T.,M.T.<sup>2</sup>, M.Faris Ruriawan,S.T.,M.T.<sup>3</sup>.

<sup>1,2</sup>Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

<sup>3</sup>Prodi S1 Teknik Komputer, Fakultas Teknik Elektro, Universitas Telkom

<sup>1</sup> [putrinians@student.telkomuniversity.ac.id](mailto:putrinians@student.telkomuniversity.ac.id), <sup>2</sup>[Wahidah@telkomuniversity.ac.id](mailto:Wahidah@telkomuniversity.ac.id),

<sup>3</sup>[muhammad.faris.ruriawan@telkomuniversity.ac.id](mailto:muhammad.faris.ruriawan@telkomuniversity.ac.id)

### Abstrak

Telemedis merupakan salah satu layanan perawatan kesehatan yang efektif digunakan dan dirancang untuk memberikan perawatan kesehatan jarak jauh menggunakan komunikasi elektronik. Dengan adanya telemedis di negara berkembang ini dapat menawarkan solusi, seperti mengurangi keseluruhan biaya pengobatan, mengurangi masalah transportasi dan waktu, dan meningkatkan kualitas perawatan kesehatan di daerah tersebut. Telemedis digunakan antar dokter dengan pasien, dan bisa juga antar dokter umum dengan dokter spesialis untuk pertukaran informasi kesehatan. Namun, akses dan distribusi informasi teknologi dapat menimbulkan masalah terutama terkait dengan keamanannya, salah satunya pada data rekam medis.

Layanan telemedis terdapat data informasi pasien yang harus dilindungi agar tidak mudah dimanipulasi atau diserang oleh orang yang tidak bertanggung jawab. Oleh karena itu diperlukan sebuah sistem untuk melindungi citra medis tersebut, pada penelitian ini akan dibangun sistem *watermarking* dengan metode *spread spectrum* dan *error correction codes* BCH. Citra grayscale sebagai citra medis atau citra hostnya, kemudian akan disisipkan citra biner yang berupa sebuah logo sebagai citra watermarknya. Watermark yang akan disisipkan disebar secara random ke dalam spektrum dari data host sebagai covernya. Kemudian dikodekan menggunakan BCH codes dengan nilai parameter pengujian yang telah ditentukan.

Penelitian Tugas Akhir ini menghasilkan performansi sistem yang cukup handal dengan parameter BCH (63, 16) dengan nilai rata-rata BER = 0 dan nilai PSNR  $\geq 58$  dB. Namun sistem ini kurang mampu menangani jenis serangan *rotate* 1°, 3°, dan juga serangan *scaling* ketika diperkecil. Karena menghasilkan nilai BER yang cukup tinggi. Sehingga pesan didalamnya mengalami kerusakan.

**Kata kunci :** *Watermarking, Spread Spectrum, Error Correction Codes BCH*

### Abstract

*Telemedicine is one of the effective health care services used and designed to provide long-distance health care using electronic communication. With telemedicine in developing countries it can offer solutions, such as reducing overall medical costs, reducing transportation problems and time, and improving the quality of health care in the area. Telemedicine is used between doctors and patients, and can also be between general practitioners and specialist doctors for the exchange of health information. However, access and distribution of information technology can cause problems, especially related to security, one of which is on medical record data.*

*Telemedicine services contain patient information that must be protected so that they are not easily manipulated or attacked by irresponsible people. Therefore we need a system to protect the medical image, in this study a watermarking system with a spread spectrum method and BCH error correction codes will be built. The grayscale image as a medical image or the image of its host, then a binary image in the form of a logo will be inserted as the watermark image. The watermark to be inserted is distributed randomly into the spectrum of the host data as the cover. Then it is coded using BCH codes with predetermined test parameter values.*

*This Final Project research produces a fairly reliable system performance with BCH parameters (63, 16) with an average value of BER = 0 and PSNR value  $\geq 58$  dB. However, this system is less able to deal with rotate attacks of 1°, 3° and also scaling attacks when minimized. Because it produces a fairly high BER value. So the message inside is defect.*

**Key Words:** *Watermarking, Spread Spectrum, Error Correction Codes BCH*

### 1. Pendahuluan

Telemedis merupakan salah satu teknologi layanan pertukaran informasi data medis secara jarak jauh menggunakan komunikasi elektronik, yang akan meningkatkan status kesehatan pasien. Informasi data medis pasien yang bersifat privasi harus dilindungi dari pihak yang tidak bertanggung jawab agar tidak terjadi manipulasi data, pencurian data medis,

mengubah atau bahkan merusak data medis. Data citra medis mengandung informasi sensitif dan ketika citra tersebut dikirim pada jaringan yang tidak aman, maka akan menjadi rentan terhadap serangan. Untuk mencegah hal semacam itu maka dibutuhkan suatu sistem keamanan untuk melindungi citra medis. Digital *watermarking* telah berkembang sebagai solusi untuk mengatasi masalah keamanan citra medis tersebut.

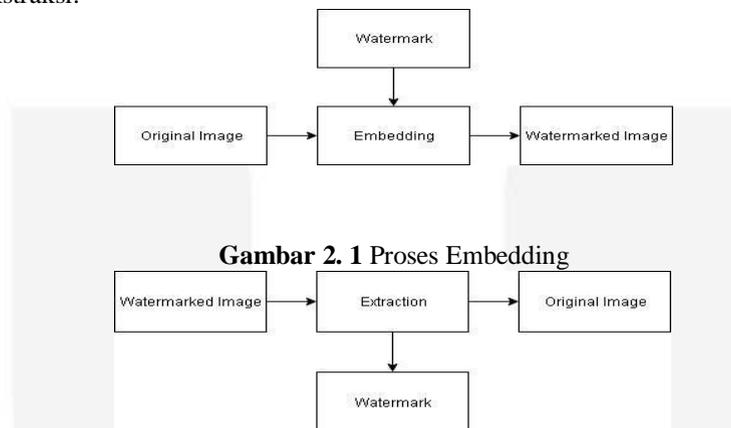
Digital *watermarking* merupakan teknik penyisipan atau menyembunyikan informasi *watermark* ke dalam media digital seperti gambar/citra, audio, video dan teks. Informasi *watermark* dapat juga berupa gambar/citra, audio, video dan teks. *Watermarking* pada citra medis digunakan untuk mengotentikasi dan menyelidiki integritas citra medis. Sistem *watermarking* citra medis dapat dipecah menjadi tiga kategori : *robust*, *fragile*, dan *semi-fragile*. *Robust* menilai sejauh mana *watermark* kuat bertahan setelah mengalami segala proses perubahan pada datanya. *Fragile* digunakan untuk perlindungan integritas, yang harus sangat sensitif terhadap perubahan sinyal. Kita dapat menentukan apakah data telah dirusak. *Semi-fragile watermarking* mampu mentolerir beberapa derajat perubahan pada gambar yang ditandai *watermark*. Oleh karena itu untuk memenuhi sistem keamanan yang handal diperlukan teknik tambahan yaitu *Error Correction Codes* pada saat proses penyisipan. Teknik ini mampu mendeteksi *error* sekaligus mengoreksi kesalahan bit selama proses *watermarking*.

## 2. Dasar Teori

### 2.1 Digital Watermarking

*Digital Watermarking* merupakan suatu teknik yang digunakan untuk melindungi media digital seperti video, audio, gambar/citra dan teks dengan cara menyembunyikan atau menyisipkan informasi tersebut ke dalam konten media lainnya. Tujuan digital *watermarking* adalah untuk menanamkan beberapa informasi rahasia dan informasi tambahan dalam media sampul yang nantinya dapat diekstraksi atau dideteksi untuk berbagai keperluan seperti otentikasi, identifikasi kepemilikan, perlindungan konten dan perlindungan hak cipta. Karakteristik penting dari *watermarking* digital adalah *robustness* dan *imperceptibility* terhadap berbagai jenis serangan atau manipulasi gambar yang umum seperti *rotation* (rotasi), *filtering* (penyaringan), *scaling* (penskalaan), *cropping* (pemotongan) dan kompresi. Efisiensi algoritma digital *watermarking* benar-benar didasarkan pada *robustness watermark* yang tertanam terhadap berbagai jenis serangan. Setiap digital teknik *watermarking* mencakup dua algoritma:

1. sebagai algoritma embedding dan
2. sebagai algoritma ekstraksi.



Gambar 2.2 Proses Ekstraksi

### 2.2 Citra Medis

*Watermarking* di bidang medis memiliki banyak aplikasi praktis, misalnya *telediagnosis*, *teleconference* antar dokter, dan pembelajaran jarak jauh dari tenaga medis. Dengan adanya teknologi tersebut maka memudahkan untuk saling menukar gambar medis antara sesama dokter, spesialis, dan ahli radiologi yang menyediakan platform untuk membahas dan berkonsultasi tindakan diagnostik. Menggunakan teknik *watermarking* tidak hanya akan menjamin kerahasiaan dan keamanan data yang dikirim tetapi juga integritas dari citra medis tersebut.

### 2.3 Spread Spectrum

Dalam teknik *watermarking Spread Spectrum*, *watermark* tersebar di beberapa lokasi yang sudah ditentukan, sehingga bit-bit *watermark* sangat kecil dan tidak mudah terdeteksi [6]. Cara penyebaran *watermark* dengan menggunakan random permutasi. Sebelum *watermark* disisipkan, terlebih dahulu menentukan lokasi penyisipannya berdasarkan dari resolusi citra host. Setelah lokasi sudah ditetapkan, selanjutnya *watermark* disisipkan ke dalam citra host, bit-bit *watermark* akan menyebar secara acak pada lokasi yang sudah ditentukan sebelumnya. Kemudian dikalkulasikan dengan besaran koefisien penyisipan untuk mendapatkan nilai parameter performansi terbaik pada sistem yang telah dibuat. Penyebaran bit-bit *watermark* di beberapa bagian citra host memastikan tingkat keamanan terhadap serangan yang tidak disengaja atau disengaja karena lokasi *watermark* yang sulit terdeteksi.

Kemudian *watermark* dapat diekstraksi dengan cara mendapatkan kembali lokasi dimana bit-bit *watermark* yang telah disisipkan tadi dan dibagi dengan besaran koefisien penyisipan, sehingga *watermark* dapat dipulihkan dengan memisahkan dari citra hostnya.

**2.5 BCH Codes**

Kode BCH merupakan kelas kode siklik yang mencakup huruf biner dan non-biner. Kode BCH biner dapat dibangun dengan parameter (n, k, t): di mana, n = panjang blok/kode yang akan dikirim, k = bit informasi (urutan biner asli), t = jumlah maksimal kesalahan bit yang dapat diperbaiki oleh sistem BCH. Pada tahun 1961 teknik ini dikembangkan oleh *Gorenstein* dan *Zieler* dengan menggunakan simbol dari *Galois Field* (GF). Kode BCH untuk setiap bilangan bulat  $m \geq 3$  memiliki parameter berikut:

- $n = 2^m - 1$ : yang mampu memperbaiki kesalahan t dan memiliki dimensi  $k = n - m * t$ ,
- $n - k \leq mt$ : jumlah digit *parity check*
- $d_{min} \geq 2t + 1$ : jarak minimal.

n	k	t	Generator polynomial, $g_i(x)$ (octal)
7	4	1	$g_1(x) = p(x) = 13$
	1	3	$g_1(x) \cdot (15) = 177$
15	11	1	$g_1(x) = p(x) = 23$
	7	2	$g_1(x) \cdot (37) = 721$
	5	3	$g_2(x) \cdot (7) = 2467$
	1	7	$g_3(x) \cdot (31) = 77777$
31	26	1	$g_1(x) = p(x) = 45$
	21	2	$g_1(x) \cdot (75) = 3551$
	16	3	$g_2(x) \cdot (67) = 10765 \ 7$
	11	5	$g_3(x) \cdot (57) = 54233 \ 25$
	6	7	$g_5(x) \cdot (73) = 31336 \ 5047$
	1	15	$g_7(x) \cdot (151) = 17777 \ 77777 \ 7$
	63	57	1
51		2	$g_1(x) \cdot (127) = 12471$
45		3	$g_2(x) \cdot (147) = 17013 \ 17$
39		4	$g_3(x) \cdot (111) = 16662 \ 3567$
36		5	$g_4(x) \cdot (15) = 10335 \ 00423$
30		6	$g_5(x) \cdot (155) = 15746 \ 41655 \ 47$
24		7	$g_6(x) \cdot (133) = 17323 \ 26040 \ 4441$
18		10	$g_7(x) \cdot (165) = 13630 \ 26512 \ 35172 \ 5$
16		11	$g_{10}(x) \cdot (7) = 63311 \ 41367 \ 23545 \ 3$
10		13	$g_{11}(x) \cdot (163) = 47262 \ 23055 \ 27250 \ 155$
7		15	$g_{13}(x) \cdot (13) = 52310 \ 45543 \ 50327 \ 1737$
1		31	$g_{15}(x) \cdot (141) = 77777 \ 77777 \ 77777 \ 77777 \ 7$

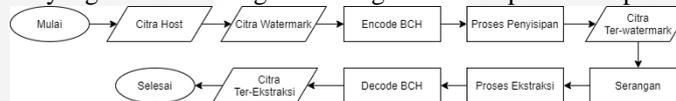
**Gambar 2.3** Parameter Kode BCH

Dalam Pengkodean BCH mengalami dua proses utama, yaitu *encoding* dan *decoding*. Proses *encoding* yaitu proses pembentukan *codeword* yang berisi gabungan bit informasi dan bit *parity*. Proses *decoding* yaitu proses pendeteksian *error* sekaligus pengkoreksian *error* apabila ditemukan *error*, pada proses ini juga dilakukan pengambilan kembali bit informasi.

**3. Perancangan Sistem**

**3.1 Gambaran Umum Sistem**

Secara umum model sistem yang akan dirancang untuk Tugas Akhir dapat dilihat pada gambar berikut:



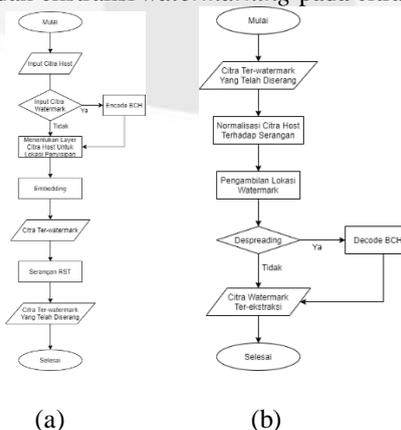
**Gambar 3.1** Diagram Blok Sistem Secara Umum.

Pada **Gambar 3.1** terlihat bahwa sistem *watermarking* yang dilakukan pada penelitian terbagi menjadi tiga proses yaitu penyisipan, serangan dan ekstraksi. Pada proses penyisipan, citra host akan disisipi citra *watermark*. Keluaran dari proses penyisipan adalah citra *ter-watermark*. Citra yang telah *ter-watermark* diuji dengan berbagai serangan seperti *Rotation*, *Scaling*, dan *Translation* (RST). Setelah diberi serangan, citra tersebut diekstrak pada blok ekstraksi untuk dilakukan proses pemisahan antara citra host asli dengan citra watermark asli.

**3.2 Perancangan Sistem**

**3.2.1 Penyisipan dan Ekstraksi Watermark**

Berikut adalah sistem penyisipan dan ekstraksi *watermarking* pada citra medis:



(a)

(b)

### Gambar 3.2 Diagram Alur (a) Proses Penyisipan dan Serangan (b) Proses Ekstraksi dan Serangan

Pada **Gambar 3.2** (a) merupakan proses embedding. Proses embedding adalah proses ketika citra *watermark* disisipkan ke dalam citra host untuk melindungi informasi yang ada didalamnya dari pihak yang tidak berwenang. Berikut penjelasan mengenai tahap-tahap pada saat proses embedding:

1. Memilih file citra sebagai citra host. File citra yang akan digunakan menggunakan format .jpg yang berupa citra grayscale.
2. Memilih file citra sebagai citra *watermark*. File citra yang akan digunakan menggunakan format .jpg yang berupa citra logo Tel-U atau citra biner.
3. Jika sistem menggunakan pengkodean BCH maka perlu melakukan proses encoding BCH pada citra *watermark*. Deret biner yang dihasilkan dari citra *watermark* kemudian akan diolah pada proses encoding BCH. Tiap  $k$  bit akan diubah menjadi  $n$  bit sebagai inputan encoding citra *watermark*. Hingga menghasilkan bit informasi untuk diteruskan.
4. Jika sistem tidak menggunakan BCH maka tidak perlu melakukan proses encode BCH, dan lanjut ke tahap selanjutnya.
5. Penentuan lokasi penyisipan *watermark* ditentukan dari  $\frac{1}{4}$  layer citra host.
6. Selanjutnya proses embedding, yaitu melakukan *spreading* sesuai dengan bit pengalinya. Penyebaran bit-bit *watermark* ke dalam spektrum citra host pada lokasi yang telah ditentukan menggunakan random permutasi.
7. Dihasilkan citra yang telah ter-*watermark*.
8. Diberikan salah satu serangan RST (*Rotate, Scaling, Translation*) untuk menguji ketahanan sistem.
9. Dihasilkan citra host yang telah ter-*watermark*.

**Gambar 3.2** (b) merupakan proses ekstraksi. Proses ekstraksi adalah proses perolehan kembali citra host dan citra *watermark*. Pengujian ketahanan sistem *watermarking* akan diuji dalam proses ekstraksi ini dengan cara memberikan beberapa tipe serangan yang berbeda. Berikut penjelasan mengenai tahap-tahap pada saat proses ekstraksi:

1. Didapatkan citra yang ter-*watermark* yang telah diserang.
2. Kemudian sistem akan menormalisasi citra host dari serangan tersebut.
3. Pengambilan kembali lokasi dimana *watermark* disebar.
4. Selanjutnya melakukan proses *dispreading*. *Dispreading* merupakan kebalikan dari proses *spreading*.
5. Proses *dispreading* menghasilkan bit informasi yang selanjutnya akan diproses dalam BCH decoder untuk mendeteksi error dan melakukan pengkoreksian apabila ditemukan error.
6. Hasil decoding ini kemudian akan menampilkan citra *watermark* yang sudah di ekstraksi.
7. Hasil dari ekstraksi tersebut akan dibandingkan dengan data awal sebelum dilakukan embedding sehingga dapat diketahui nilai-nilai parameter pengujiannya.

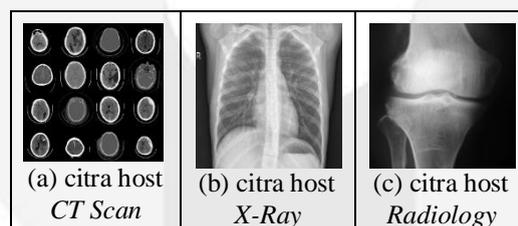
## 4. Implementasi dan Pengujian Sistem

### 4.1 Skenario Pengujian

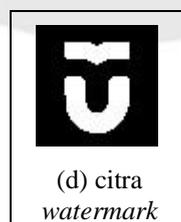
Penelitian ini melakukan 2 skenario pengujian. Yaitu pengujian kualitas citra pada saat melakukan proses embedding dan ekstraksi. Dan pengujian ketahanan citra pada saat diberi serangan.

Citra *host* yang digunakan adalah citra medis *grayscale*. Terdapat 3 macam citra *host* untuk pengujian kualitas citra, yaitu citra *CT Scan*, citra *X-Ray* dan citra *Radiology*. Ketiganya memiliki 5 resolusi yang berbeda yaitu  $512 \times 512$ ,  $720 \times 720$ ,  $1024 \times 1024$ ,  $1536 \times 1536$ , dan  $2048 \times 2048$ . Sedangkan citra *watermark* yang digunakan adalah citra logo biner, dengan resolusi yang berbeda yaitu  $64 \times 64$ ,  $128 \times 128$ , dan  $256 \times 256$ .

Gambar 4.1 Citra Host



Gambar 4.2 Citra Watermark



### 4.2 Pengujian parameter resolusi citra host

Pengujian ini dilakukan menggunakan 2 citra *host* yang berbeda. Citra *CT Scan* dan Citra *X-Ray*. Masing-masing citra *host* memiliki 5 resolusi yaitu  $512 \times 512$ ,  $720 \times 720$ ,  $1024 \times 1024$ ,  $1536 \times 1536$ , dan  $2048 \times 2048$ . Kemudian disisipkan oleh citra *watermark* dengan resolusi  $128 \times 128$ .

**Tabel 4.1** Tabel dari pengaruh resolusi citra *host* terhadap parameter sistem.

Citra Host	CT Scan				X-Ray				Radiology			
	BER	MSE	PSNR (dB)	SSIM	BER	MSE	PSNR (dB)	SSIM	BER	MSE	PSNR (dB)	SSIM
512×512	0	1,3349	46,8763	0,9999	0	1,3816	46,7267	0,9999	0	1,3857	46,7138	0,9999
720×720	0	0,6737	49,8458	0,9999	0	0,7026	49,6632	0,9999	0	0,7037	49,6566	0,9999
1024×1024	0	0,3313	52,9278	0,9999	0	0,3478	52,7164	0,9999	0	0,3487	52,7061	0,9999
1536×1536	0	0,1466	56,4685	0,9999	0	0,1547	56,2345	0,9999	0	0,155	56,2265	0,9999
2048×2048	0	0,0819	58,997	0,9999	0	0,0869	58,737	0,9999	0	0,0872	58,725	0,9999

Berdasarkan dari **Tabel 4.1** menunjukkan hasil dari pengujian ketiga jenis citra *host* dengan 5 resolusi yang berbeda. Ketiga jenis citra menghasilkan nilai BER dan SSIM yang serupa. Yaitu nilai BER = 0. Nilai BER dihasilkan berdasarkan dari perhitungan presentase jumlah kesalahan bit pada citra *watermark* yang telah diekstraksi dibandingkan dengan citra *watermark* asli. Dan nilai SSIM yang mendekati 1 yaitu SSIM = 0,9999 yang artinya citra yang sebelum dilakukan penyisipan dengan yang sudah dilakukan penyisipan memiliki kemiripan hampir 100%. Sedangkan jika dilihat dari parameter PSNR dapat disimpulkan bahwa semakin besar resolusi citra *host* maka akan semakin baik PSNR nya. PSNR pada ketiga jenis citra dengan resolusi  $2048 \times 2048$  yaitu sebesar  $\geq 58$  dB.

#### 4.3 Pengujian Pengaruh Koefisien Penyisipan Terhadap Sistem

Koefisien Penyisipan pada sistem ini sebagai besaran pengali atau pembagi dari pesan. Pengujian ini dilakukan menggunakan resolusi citra *host*  $2048 \times 2048$ . Kemudian disisipkan resolusi citra *watermark*  $256 \times 256$ . Serta pengkodean BCH yang digunakan adalah (63, 16). Pengujian ini dilakukan untuk mengetahui pengaruh resolusi koefisien penyisipan terhadap sistem.

**Tabel 4.2** Tabel dari pengaruh koefisien penyisipan terhadap parameter sistem.

Koefisien Penyisipan	CT Scan				X-Ray				Radiology			
	BER	MSE	PSNR (dB)	SSIM	BER	MSE	PSNR (dB)	SSIM	BER	MSE	PSNR (dB)	SSIM
5	0	0,0824	58,9703	0,9999	0	0,087	58,7343	0,9999	0	0,0872	58,725	0,9999
10	0	0,3278	52,9734	0,9999	0	0,3478	52,7172	0,9999	0	0,3486	52,7073	0,9999
15	0	0,7337	49,4752	0,9999	0	0,7818	49,1995	0,9999	0	0,7797	49,2112	0,9999
20	0	1,305	46,9747	0,9999	0	1,3872	46,7093	0,9999	0	1,365	46,7294	0,9999

Berdasarkan dari **Tabel 4.2** dapat dilihat bahwa semakin kecil nilai koefisien penyisipannya maka semakin besar nilai PSNRnya, pada saat nilai koefisien 5 menghasilkan nilai rata-rata PSNR = 58,8098 dB. Dan pada saat nilai koefisien 20 menghasilkan PSNR yang rendah dengan nilai rata-rata PSNR = 46,8044 dB. Sebelum menghitung nilai PSNR terlebih dahulu menghitung nilai MSE. Nilai MSE merupakan nilai *error* kuadrat rata-rata antara citra asli dengan citra hasil penyisipan. Dilihat dari **tabel 4.4** semakin tinggi nilai PSNR menghasilkan MSE yang rendah. MSE yang semakin mendekati nilai 0 mengartikan kualitas citra yang hampir mirip dengan citra aslinya. Sedangkan pada nilai BER dan SSIM menghasilkan nilai yang stabil pada setiap nilai koefisien penyisipan, yaitu nilai BER = 0 dan nilai SSIM = 0,9999 yang mengartikan kualitas citra sangat baik.

#### 4.4 Pengujian Ketahanan Watermark Terhadap Serangan Rotate

Serangan rotasi dilakukan dengan memutar citra ter-*watermark* searah jarum jam. Pengujian dilakukan sebanyak 5 kali dengan nilai derajat yang berbeda yaitu,  $-1^\circ$ ,  $-3^\circ$ ,  $-45^\circ$ ,  $-90^\circ$ , dan  $-180^\circ$ . Tanda (-) pada rotasi mengartikan rotasi diputar searah jarum jam.

**Tabel 4.3** Tabel Ketahanan Watermark Terhadap Serangan Rotate.

Rotate (degree)	Tanpa BCH		Dengan BCH	
	BER	PSNR <sub>ext</sub> (dB)	BER	PSNR <sub>ext</sub> (dB)
$1^\circ$	0,4084	52,0194	0,404	52,0664
$3^\circ$	0,4018	52,0901	0,3867	52,2569
$45^\circ$	0,2385	54,3555	0,2385	54,3555
$90^\circ$	0	--	0	--
$180^\circ$	0	--	0	--

Berdasarkan **Tabel 4.3** diatas dapat dilihat hasil dari pengujian ketahanan sistem terhadap serangan *rotate* yang tidak menggunakan pengkodean BCH memiliki parameter performansi yang lebih rendah dibandingkan dengan yang menggunakan pengkodean BCH. Berikut hasil dari pengujian ketahanan serangan rotate:

**Gambar 4.3** Pengujian Ketahanan Sistem Terhadap Serangan Rotasi.

Rotate °	Citra Yang Diserang	Watermark Ter-ekstraksi	Citra Yang Diserang (Tanpa BCH)	Watermark Ter-ekstraksi (Tanpa BCH)
1°				
3°				
45°				
90°				
180°				

**4.5 Pengujian Ketahanan watermark terhadap serangan *Scaling***

Serangan scaling dilakukan dengan mengubah skala citra. baik itu memperbesar citra, merubah aspek rasio citra atau memperkecil citra. Dengan nilai penskalaan 50% (1024×1024), 80% (1639×1639), (1153×2048), (1537×2048), 150% (3072×3072), dan 200% (4096×4096).

**Tabel 4.4** Pengujian Ketahanan watermark terhadap serangan *Scaling*

Scaling	Tanpa BCH		Dengan BCH	
	BER	PSNR <sub>ext</sub> (dB)	BER	PSNR <sub>ext</sub> (dB)
1024×1024	0,2851	53,58	0,2324	54,468
1639×1639	0,1687	55,8596	0,1745	55,7113
1153×2048	0,1562	56,1926	0,1428	56,5828
1537×2048	0,0734	59,4687	0,0219	64,712
3072×3072	0,0224	64,6165	0	∞
4096×4096	0,0209	64,9094	0	∞

Berdasarkan dari **Tabel 4.5** diatas dapat dilihat hasil dari pengujian ketahanan sistem terhadap serangan *scaling* yang tidak menggunakan pengkodean BCH memiliki parameter performansi yang lebih rendah dibandingkan dengan yang menggunakan pengkodean BCH. Dari 6 kali pengujian, hasil yang paling rusak pada saat dilakukan *scaling* 50% (1024×1024) karena menghasilkan nilai BER yang paling tinggi yaitu BER = 0,2549 pada saat tanpa menggunakan pengkodean BCH dan BER = 0,2385 pada saat menggunakan pengkodean BCH.

**Gambar 4.4** Pengujian Ketahanan watermark terhadap serangan *Scaling*

Scaling	Citra Yang Diserang	Watermark Ter-ekstraksi	Citra Yang Diserang (Tanpa BCH)	Watermark Ter-ekstraksi (Tanpa BCH)
50% (1024×1024)				
80% (1639×1639)				
16:9 (1153×2048)				
4:3 (1537×2048)				
150% (3072×3072)				
200% (4096×4096)				

**4.6 Pengujian Ketahanan watermark terhadap serangan *Translation***

Serangan translasi dilakukan dengan menggeser di sepanjang garis lurus dari satu lokasi koordinat ke lokasi koordinat lainnya pada citra. Khusus pada pengujian Tugas Akhir ini dilakukan pergeseran ke kanan dan ke bawah. Dan juga translasi pillar boxing dan letter boxing.

**Tabel 4.5** Pengujian Ketahanan watermark terhadap serangan *Translation*

Translation	Tanpa BCH		Dengan BCH	
	BER	PSNR <sub>ext</sub> (dB)	BER	PSNR <sub>ext</sub> (dB)
[-25 25]	0,0048	71,2441	0	∞
[25 -50]	0,0139	66,6957	0	∞
[-50 50]	0,0109	67,7223	0	∞
[50 -75]	0,0175	65,6811	0	∞
Pillar Boxing [5% 5%]	0,111	57,6743	0,0871	58,7277
Letter Boxing [5% 5%]	0,111	57,6743	0,0871	58,7277

Berdasarkan dari **Tabel 4.6** diatas dapat dilihat hasil dari pengujian ketahanan sistem terhadap serangan *translation* yang tidak menggunakan pengkodean BCH memiliki parameter performansi yang lebih rendah dibandingkan dengan yang menggunakan pengkodean BCH sama seperti pengujian serangan sebelumnya. Dari 5 kali pengujian, hasil yang paling rusak pada saat dilakukan *translation* [30 30] tanpa menggunakan pengkodean BCH pada tabel 4.15 dan tabel 4.17. Namun hasil yang paling baik saat dilakukan *translation* [10 10] baik yang menggunakan pengkodean BCH ataupun yang tanpa menggunakan pengkodean BCH. Berikut hasil ketahanan citra terhadap serangan translasi:

**Gambar 4.5** Pengujian Ketahanan Citra Terhadap Serangan Translation

Translation	Citra Yang Diserang	Watermark Ter-ekstraksi	Citra Yang Diserang (Tanpa BCH)	Watermark Ter-ekstraksi (Tanpa BCH)
[-25 25]				
[25 -50]				
[-50 50]				
[50 -75]				
Pillar Boxing [5% 5%]				
Letter Boxing [5% 5%]				

## Kesimpulan dan Saran

### 5.1 Kesimpulan

Dari hasil analisis pengujian sistem watermarking citra medis menggunakan metode *spread spectrum* dan *Error Correction Codes Bose-Chaudhuri-Hocquenghem* (BCH), dapat diambil kesimpulan :

1. Perancangan sistem watermarking citra medis dengan menggunakan metode *Spread Spectrum* dan *Error Correction Codes Bose-Chaudhuri-Hocquenghem* (BCH) berhasil dilakukan.
2. Hasil dari sistem sistem watermarking citra medis dengan menggunakan metode *Spread Spectrum* dan *Error Correction Codes Bose-Chaudhuri-Hocquenghem* (BCH) dipengaruhi berdasarkan resolusi citra *host*, jenis citra medis yang digunakan, citra *watermark*, koefisien penyisipan, dan nilai parameter pengkodean BCH.
3. Jenis citra medis seperti citra *host CT Scan* menghasilkan nilai parameter performansi yang lebih rendah dibandingkan dengan jenis citra *host X-Ray* dan citra *host Radiology*.

### 5.2 Saran

Berdasarkan dari hasil pengujian dan analisis yang telah dijabarkan diatas, penulis menyadari masih terdapat kekurangan. Maka dari itu, penulis ingin memberi saran agar penelitian selanjutnya dapat menghasilkan sistem yang lebih baik lagi. Adapun beberapa saran dari penulis, yaitu :

1. Menggunakan tambahan metode transformasi untuk sistem *watermarking* agar lebih *robust*.
2. Pada penelitian ini menggunakan parameter BCH (7,4) dan (63,16), pada penelitian selanjutnya diharapkan mampu mengembangkan nilai parameter tersebut agar hasil yang didapat lebih maksimal.
3. Menggunakan citra *watermark* selain biner, contohnya seperti *grayscale*.
4. Menggunakan jenis serangan lain.

### Daftar Pustaka

- [1] A. N. a. S. A. R. A.-B. Seyed Mojtaba Mousavi, "Watermarking Techniques used in Medical Images: a Survey," *NCBI*, pp. 714-729, 2014.
- [2] M. C. Jasni Mohamad Zain, "Security in Telemedicine: Issues in Watermarking Medical Images," *International Conference: Sciences of Electronic, Technologies of Information and Telecommunications (SETIT)*, 2005.
- [3] S. S. Baljit Kaur, "Digital Watermarking and Security Techniques: A Review," *International Journal of Computer Science And Technology (IJST)*, vol. 8, no. 2, p. 44, 2017.
- [4] V. M. P. S. H. Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques," *IEEE International Conference on Industrial Informatics*, p. 709, 2005.
- [5] V. S. Lalit Kumar Saini, "A Survey of Digital Watermarking Techniques and its Applications," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 2, no. 3, pp. 70-71, 2014.
- [6] T. Todorov, "Spread Spectrum Watermarking Technique For Information System," *International Journal "Information Theories & Applications*, vol. 11, pp. 406-407.
- [7] C. W. X. Z. Yunpeng Zhang, "RST Resilient Watermarking Scheme Based on DWT-SVD and Scale-Invariant Feature Transform," *MDPI*, pp. 8-9, 2017.
- [8] A. N. T. RD. Kusumanto, "Pengolahan Citra Digital Untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi RGB," *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011*, 2018.
- [9] B. K. M. D. A. M. Amit Kumar Singh1, "Multiple Watermarking on Medical Images Using Selective Discrete Wavelet Transform Coefficients," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 1-8, 2015.
- [10] P. R. L. X. Shanshan Liu, "Evaluating Direct Compare for Double Error Correction Codes," *IEEE Transactions on Device and Materials Reliability*, vol. 17, no. 4, pp. 802-804, 2017.
- [11] A. M. M. D. Amit Kumar Singh, "Multilevel Encrypted Text Watermarking on Medical Images Using Spread Spectrum," *Wireless Personal Communications*, p. 18, 2015.
- [12] H. V. S. S. P. S. A. M. Basant Kumar, "Secure Spread-Spectrum Watermarking for Telemedicine Applications," *Journal of Information Security*, 2011.
- [13] Y.-K. W. Ching-Tang Hsieh, "Digital Image Multiresolution Watermark Based on Human Visual System Using Error Correcting Code," *Tamkang Journal of Science and Engineering*, vol. 4, no. 3, p. 202, 2001.
- [14] F. Y. C. Fung, "A Survey of the Theory of Error-Correcting Codes," p. 8, 2008.
- [15] B. K. M. D. A. M. Amit Kumar Singh, "Robust and Imperceptible Spread Spectrum Watermarking for Telemedicine Applications," *RESEARCH ARTICLE*, 2015.
- [16] M. T. Appl, "Double expanding robust image watermarking based on Spread Spectrum technique and BCH coding," *Seyyed Hossein Soleymani, Amir Hossein Taherinia*, 2017.
- [17] N. Srivadana, "Digital Watermarking," *International Journal For Technological Research In Engineering*, vol. 1, no. 3, pp. 13-14, 2013.

