ISSN 2622-8130 VOL 20, NO 1, APRIL 2019

Pengamanan Data Teks Dengan NTRU Dan Modulus Function Pada Koefisien IHWT Citra Warna

Ronsen Purba[1], Irpan Adiputra Pardosi[2], Harry Darmawan[3], Aldo Alex Sitorus[4]
Jurusan Teknik Informatika, STMIK Mikroskil
[1]ronsen@mikroskil.ac.id, [2]irpan@mikroskil.ac.id, [3]131111777@mikroskil.ac.id,
[4]131113786@mikroskil.ac.id

Abstrak

Perkembangan informasi digital telah menyebabkan meningkatnya teknologi informasi keamanan untuk melindungi suatu data teks yang mengandung kerahasian. Steganografi merupakan salah satu solusi untuk pengamanan data teks dengan melakukan proses penyembunyian data teks pada suatu gambar (citra) sehingga orang lain tidak mengetahui keberadaan data teks tersebut. Kriteria steganografi yang baik adalah imperceptibility, fidelity, robustness dan recovery. Salah satu metode steganografi adalah CD (Coefficient Difference) yang diadopsi dari PVD (Pixel Value Differencing) yang melakukan penyembunyian pada domain spasial menggunakan selisih dari 2 nilai piksel sehingga menghasilkan jumlah modifikasi nilai piksel yang besar, membuat tingkat imperceptibility menurun. Metode modulus function digunakan untuk mengatasi kelemahan pada CD dengan menggunakan fungsi modulus pada penyisipannya sehingga dapat memperkecil modifikasi nilai piksel pada penyisipan sehingga meningkatkan tingkat imperceptibility. Dalam penelitian ini digunakan metode IHWT (Integer Haar Wavelet Transform) untuk menjaga tingkat imperceptibility. Untuk meningkatkan keamanan, metode kriptografi NTRU digunakan terhadap pesan rahasia sebelum pesan rahasia disembunyikan pada citra. Hasil pengujian menunjukan bahwa penggabungan metode NTRU, IHWT dan modulus function menghasilkan nilai imperceptibility yang baik dengan melihat nilai PSNR diatas 40 dB dan citra stego tahan terhadap serangan noise salt and pepper dengan nilai maksimal 0,002% dan serangan penambahan kontras dengan nilai maksimal satu

Kata Kunci : pengamanan data teks, imperceptibility dan transformasi

Abstract

The development of digital information have caused the rise of information technology security to protect text data that contains secret. Steganography is one of many solutions for securing text data by hiding the text data on an image so that another party would not know the existence of such data. Criteria of a good steganography involves imperceptibility, fidelity, robustness dan recovery. One steganographic method is CD (Coefficient Difference), adopted from PVD (Pixel Value Differencing) which does hiding in spatial domain using difference of two pixel values that results in large modification of pixel values, reducing imperceptibility. Modulus function is used to solve such shortcoming in CD by using the modulus function on embedding, minimizing pixel modification during the process, resulting in improved imperceptibility. In this final project, IHWT (Integer Haar Wavelet Transform) are used to keep imperceptibility high. To improve the security, cryptographic method NTRU is applied on the secret message before it is hidden in image. The result showed that the combination of NTRU, IHWT and modulus function yields good imperceptibility, with PSNR value above 40 dB while the stego image resist salt and pepper noise attack of 0,002% and contrast addition of maximum amount one

Keyword : *Text data security, Imperceptibility and Transformation*

1. PENDAHULUAN

Keamanan data merupakan isu penting dalam proses pengiriman data, yang disebabkan semakin rentannya data yang beredar juga karena ancaman *cyber crime* [1]. Dampak dari *cyber-crime* mengarah pada faktor ekonomi, psikologi, keamanan negara dan lainnya [2]. Salah satu upaya mengatasinya dengan teknik steganografi, yang memungkinkan untuk melakukan komunikasi data antara satu pihak dengan pihak lain yang berkepentingan tanpa dicurigai oleh pihak yang tidak berkepentingan.

Steganografi umumnya memiliki dua tipe domain yakni transformasi dan spasial. Steganografi domain transformasi lebih tahan terhadap serangan, dibandingkan dengan domain spasial [3]. Pada penelitian lain disampaikan algoritma DWT *(Discrete Wavelet Transform)* merupakan salah satu transformasi dengan teknik steganografi domain transformasi. Penggunaan *floating point* pada DWT dapat menyebabkan hilangnya beberapa informasi saat citra direkonstruksi serta menyebabkan waktu komputasi yang lebih besar. IWT *(Integer Wavelet Transform)* ialah perkembangan dari DWT yang bertujuan untuk menghindari kelemahan tersebut [4]. IHWT *(Integer Haar Wavelet Transform)* merupakan IWT yang dikembangkan dari DHWT *(Discrete Haar Wavelet Transform)* dengan tujuan memisahkan data untuk menciptakan nilai transformasi. Salah satu penelitian tentang domain transformasi [5], dengan metode pengujian MSE dan PSNR menunjukkan bahwa kualitas citra stego dengan teknik IHWT menggunakan metode steganografi *modulus function* mencapai tingkat *imperceptibility* dan *fidelity* (aspek penyamaran pesan tersisip) lebih tinggi dibandingkan dengan menggunakan metode steganografi CD *(Coefficient Difference).*

Namun, dengan memanfaatkan kelemahan yang terdapat pada steganografi, para pelaku *cyber crime* dapat dengan mudah mengakses data yang disembunyikan. Sehingga, berbagai pihak mengemukakan bahwa hanya dengan steganografi saja dianggap sudah tidak mampu lagi memberikan pengamanan terhadap data yang akan dikirimkan [6]. Oleh sebab itu, diperlukan penerapan teknik kriptografi untuk mengacak isi pesan rahasia sebelum dilakukan teknik steganografi, sehingga pesan rahasia sulit ditemukan keberadaanya dan sekalipun berhasil ditemukan, pesan rahasia tersebut juga masih dalam bentuk acak sehingga tidak terbaca. Salah satu algoritma dari teknik kriptografi adalah NTRU yang merupakan algoritma kriptografi kunci asimetris. Permasalahan kriptografi kunci asimetris adalah penggunaan waktu yang lama pada pembangkitan kuncinya, pada penelitian [7] menunjukkan bahwa algoritma NTRU lebih cepat dalam prosesnya dibandingkan dengan RSA (*Rivest-Shamir-Adleman*) karena operasi bilangan bulat dan pemfaktoran pada RSA menghasilkan nilai yang besar. Dalam prosesnya NTRU memanfaatkan operasi terhadap polinom sehingga pada penerapannya pesan terlebih dahulu diubah ke dalam struktur polinomial untuk dapat dilakukan proses enkripsi dan dekripsi [7].

Tujuan penelitian ini untuk mengimplementasikan NTRU dan metode steganografi *modulus function* koefisien IHWT pada suatu citra warna untuk menghasilkan sistem pengamanan data teks yang bersifat rahasia. Dalam upaya mencapai hal ini, maka perlu dibatasi ruang lingkup pembahasan mencakup: 1). citra penampung adalah citra RGB 24bit dengan format *.bmp*, 2). tingkat transformasi IHWT adalah 1 kali, 3). nilai parameter w*eighting factor (α)* = 2 untuk mendapatkan nilai pada baris dan kolom dari *citra* stego. Nilai parameter NTRU telah ditetapkan sesuai standar *security level* yang di rekomendasi [8], untuk menghindari kesalahan pada saat enkripsi dan dekripsi maka pengujian ketahanan citra stego terhadap *noise*

salt and pepper dan kontras dengan persentase *noise* pengujian 0,005% yang akan dilakukan berulang-ulang sebanyak 10 kali pada masing-masing parameter set dan bit sisip.

2. METODE PENELITIAN

2.1 Kajian Pustaka

2.1.1 NTRU

NTRU diperkenalkan pada tahun 1996 yang ditemukan oleh Jeffery Hoffstein, Jill Pipher, dan Joseph Silverman. Algoritma ini dipublikasikan pada tahun 1999 dan berganti nama menjadi NTRUEncrypt [9]. Pendekatan yang dilakukan untuk menghasilkan algoritma NTRU adalah dengan menggunakan struktur matematika *polynomial ring* $Z[X]/(X^N - 1)$. Algoritma dapat digambarkan sebagai berikut [10]:

1. *Plaintext* diubah dahulu ke dalam bentuk *polynomial m*
2. Tentukan parameter set yang digunakan untuk membangkitkan kunci enkripsi dan kunci dekripsi. Dengan cara membangkitkan sebuah polinomial *f* dimana jumlah dari koefisien dengan nilai 1 adalah sama dengan parameter d_f dan *f* dapat di inverskan dengan modulo *p* dan modulo *q* kemudian bangkitkan sebuah polinomial acak *g*. *Public key* adalah *h* dan *private key* adalah *f*, untuk polinomial *f* temukan f^{-1} modulo *q* dan f^{-1} modulo *p* dimana $f * f_q \equiv 1 \pmod q$ dan $f * f_p \equiv 1 \pmod p$. Selanjutnya lakukan proses enkripsi dengan menghitung:

$$h = p * fq * g \pmod q \quad (1)$$

3. Pesan di enkripsi dengan *NTRU* menggunakan kunci enkripsi dengan membangkitkan sebuah polinomial acak *r* di dalam [-1, 0, 1]. Untuk mengenkripsi *m*, gunakan polinomial yang dipilih secara acak *r* dan *h* untuk menghitung polinomial *ciphertext* menggunakan:

$$e = r * h + m \,(mod\ q) \quad (2)$$

4. Penerima pesan acak terlebih dahulu menghitung f_p dengan menghitung polinomial *a*, *b* dan *m* dengan persamaan sebagai berikut:

$$a = f * e \,(mod\ q) \quad (3)$$
$$b = a \,(mod\ p) \quad (4)$$
$$m = fp * b \,(mod\ p) \quad (5)$$

5. Selanjutnya ubah polinomial m ke string untuk mendapatkan pesan asli.

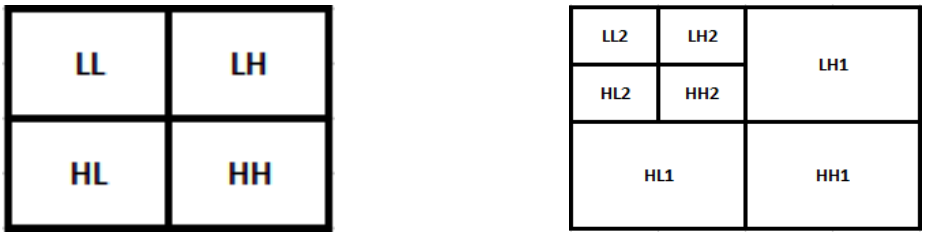
2.1.2 IHWT

Metode IHWT dikembangkan dari DHWT melalui sebuah *lifting scheme* yang digunakan pada media gambar dengan cara mengubah bilangan bulat nilai pixel dari sebuah gambar ke dalam koefisien wavelet integer dan sebaliknya. Untuk mengubah gambar menjadi *wavelet subband,* citra dibagi menjadi 2x2 blok yang tidak saling tumpang tindih seperti matriks ini [5]:

$$\begin{bmatrix} I_{m,n} & I_{m,n+1} \\ I_{m+1,n} & I_{m+1,n+1} \end{bmatrix} \quad (6)$$

Algoritma dari proses transformasi pada IHWT adalah sebagai berikut: Representasi blok 2x2 dari citra dimana diasumsikan $I_{m,\,n}$ adalah sebuah pixel pada baris m dan kolom n dari setiap blok citra. Lalu, IHWT akan diterapkan pada setiap blok gambar untuk mendapatkan *wavelet*

coefficient pada *subbands* LL, HL, LH, dan HH. *Subbands wavelet* dapat dilihat pada gambar di bawah ini



(a) (b)

Gambar 1. a. Dekomposisi tingkat 1 dan b. Dekomposisi tingkat [5]

$$LL = \left\lfloor \frac{\left\lfloor \frac{I_{m,n}+I_{m,n+1}}{2} \right\rfloor + \left\lfloor \frac{I_{m+1,n}+I_{m+1,n+1}}{2} \right\rfloor}{2} \right\rfloor$$

$$LH = \left\lfloor \left\lfloor \frac{I_{m,n}+I_{m,n+1}}{2} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{I_{m+1,n}+I_{m+1,n+1}}{2} \right\rfloor \right\rfloor$$

$$HL = \left\lfloor \frac{I - I_{m,n+1} + I_{m+1,n} - I_{m+1,n+1}}{2} \right\rfloor$$

$$HH = I_{m,n} - I_{m,n+1} - I_{m+1,n} + I_{m+1,n+1} \quad (7)$$

Inverse Integer Haar Wavelet (IIHWT) dilakukan pada sekelompok *coefficient* untuk merekonstruksi kembali ke citra *cover* aslinya dari masing-masing *subband*

$$\begin{bmatrix} I'_{m,n} & I'_{m,n+1} \\ I'_{m+1,n} & I'_{im+1,n+1} \end{bmatrix} \quad (8)$$

Algoritma proses rekonstruksi yaitu dengan merepresentasikan blok 2x2 dari citra yang direkonstruksi menjadi seperti dibawah ini:

$$I'_{m,n} = LL + \left\lfloor \frac{LH+1}{2} \right\rfloor + \left\lfloor \frac{HL + \left\lfloor \frac{HH+1}{2} \right\rfloor + 1}{2} \right\rfloor$$

$$I'_{m,n+1} = I'_{m,n} - \left(HL + \left\lfloor \frac{HH+1}{2} \right\rfloor \right)$$

$$I'_{m+1,n} = LL + \left\lfloor \frac{LH+1}{2} \right\rfloor - LH + \left\lfloor \frac{HL + \left\lfloor \frac{HH+1}{2} \right\rfloor - HH + 1}{2} \right\rfloor$$

$$I'_{m+1,n+1} = I'_{m+1,n} - \left(HL + \left\lfloor \frac{HH+1}{2} \right\rfloor \right) \quad (9)$$

2.1.3 Modulus Function

Metode ini memodifikasi sisa dari 2 pixel bersebelahan $P_{(i,x)}$ dan $P_{(i,y)}$ untuk mendapatkan kualitas citra stego yang lebih baik, tahapan proses penyisipan dan ekstraksi yang dilakukan metode *modulus function* adalah sebagai berikut [5] :

a. Definisikan nilai *Threshold* (*T*).
b. Diketahui 2 piksel berurutan dari sebuah citra sampul, Hitung sisa (r_k) dari 2 piksel berurutan:

$$r_k = (g_{ij} + g_{ij+1}) mod\ 2^T \quad (10)$$

Dimana r_k adalah sisa dari dua pixel berurutan g_{ij} dan g_{ij+1} dalam grup *k*. Jika r_k= negatif, maka hitung kembali $r_k = r_k + 2^T$ sampai r_k menghasilkan nilai positif.

c. Sisip bit-bit sisip *T* ke dalam kedua piksel dengan menyesuaikan :
   i. $r_k > t_k$ dan $m \leq (2^T)$ dan $g_{i,j} \geq g_{i,j+1}$,
   $(g'_{i,j}, g'_{i,j+1}) = (g_{i,j} - \left\lceil \frac{m}{2} \right\rceil, g_{i,j+1} - [\frac{m}{2}])$
   ii. $r_k > t_k$ dan $m \leq 2^T$ dan $g_{ij} < g_{ij+1}$,
   $(g'_{ij}, g'_{ij+1}) = (g_{ij} - \lfloor m/2 \rfloor, g_{ij+1} - \lceil m/2 \rceil)$
   iii. $r_k > t_k$ dan $m > 2^T$ dan $g_{ij} \geq g_{ij+1}$,
   $(g'_{ij}, g'_{ij+1}) = (g_{ij} + \lfloor m'/2 \rfloor, g_{ij+1} + \lceil m'/2 \rceil)$;
   iv. $r_k > t_k$ dan $m > 2^T$ dan $g_{ij} < g_{ij+1}$,
   $(g'_{ij}, g'_{ij+1}) = (g_{ij} + \lceil m'/2 \rceil, g_{ij+1} + \lfloor m'/2 \rfloor)$;
   v. $r_k \leq t_k$ dan $m \leq 2^T$ dan $g_{ij} \geq g_{ij+1}$,
   $(g'_{ij}, g'_{ij+1}) = (g_{ij} + \lfloor m/2 \rfloor, g_{ij+1} + \lceil m/2 \rceil)$
   vi. $r_k \leq t_k$ dan $m \leq 2^T$ dan $g_{ij} < g_{ij+1}$,
   $(g'_{i,j}, g'_{i,j+1}) = (g_{i,j} + \lceil m/2 \rceil, g_{i,j+1} + \lfloor m/2 \rfloor)$
   vii. $r_k \leq t_k$ dan $m > 2^T$ dan $g_{ij} \geq g_{ij+1}$,
   $(g'_{ij}, g'_{ij+1}) = (g_{ij} - \lceil m'/2 \rceil, g_{ij+1} - \lfloor m'/2 \rfloor)$;
   viii. $r_k \leq t_k$ dan $m > 2^T$ dan $g_{ij} < g_{ij+1}$,
   $(g'_{i,j}, g'_{i,j+1}) = (g_{i,j} - \left\lceil \frac{m'}{2} \right\rceil, g_{i,j+1} - [\frac{m'}{2}])$ (11)

Dimana t_k adalah nilai desimal dari bit-bit pesan sisip dengan panjang *T*,

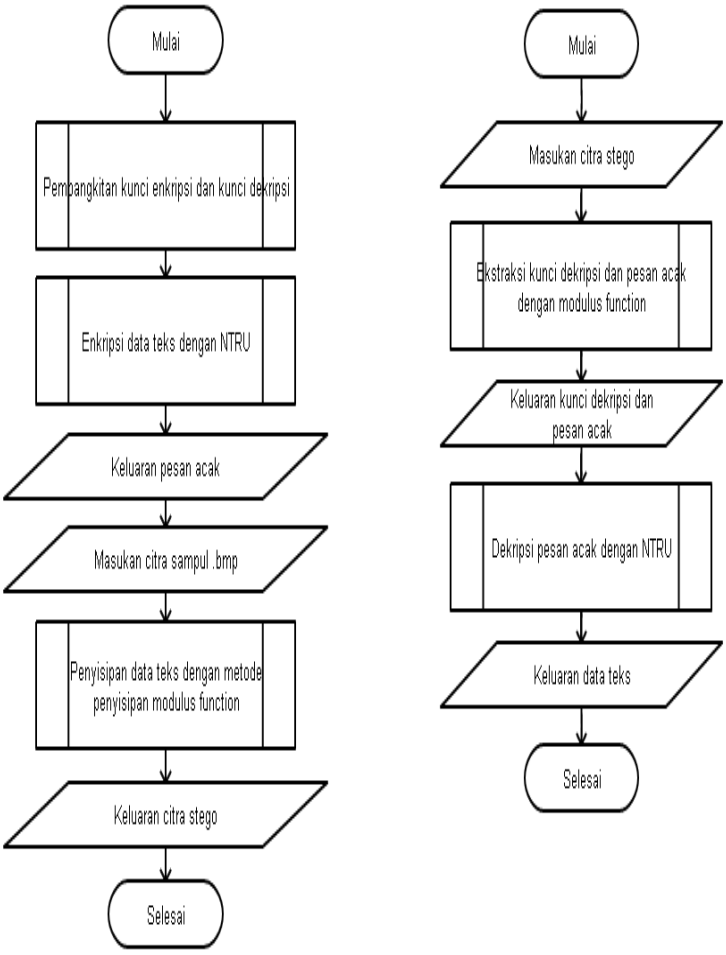
$$m = |r_k - t_k|, m' = 2^T - m \quad (12)$$

dan (g'_{ij}, g'_{ij+1}) adalah nilai baru piksel/koefisien setelah penyisipan. Pada proses pengambilan kembali, kita dapat dengan cepat mengekstrak data rahasia tanpa menggunakan citra asal, dengan menghitung:

$$r_k = (g'_{ij} + g'_{ij+1}) mod\ 2^T \quad (13)$$

2.2 Alur Proses

Dalam penelitian ini, cara kerja sistem dalam mengamankan data yang dirancang mengikuti flowchart berikut:



Gambar 2. Gambaran umum pengamanan data teks pada citra stego dan pengambilan kembalinya

2.2.1 Alur Proses Pengamanan Data Teks

Sistem mengamankan data teks dengan mengikuti langkah-langkah berikut:

1. Kunci dekripsi (privat) dan enkripsi (publik) dibangkitkan terlebih dahulu dengan langkah-langkah sebagai berikut [10]:
   a. Parameter set (N, q, df, dr, dg, panjang pesan maksimum) ditentukan terlebih dahulu sesuai dengan yang tertera pada.
   b. Membangkitkan polinomial f dan g secara acak, dimana koefisien – koefisien polinomial berada dalam [-1, 0, 1]. Untuk f jumlah koefisien dengan nilai 1 adalah sebanyak df-1 dan koefisien -1 adalah sebanyak df. Untuk g, jumlah koefisien bernilai 1 dan -1 masing-masing sebanyak dg.
   c. Menghitung nilai fp dan fq dengan menemukan invers dari f modulo p dan f modulo q. Jika tidak ditemukan fp dan fq, kembali ke langkah b.
   d. Menghitung kunci publik h dengan persamaan (1).
   e. Keluaran kunci enkripsi h dan kunci dekripsi f.
2. Selanjutnya dilakukan enkripsi data teks dengan NTRU, dengan langkah-langkah sebagai berikut:
   a. Masukan data teks

b. Mengubah data teks ke dalam bentuk polinomial m
c. Membangkitkan polinomial r secara random, dimana jumlah koefisien bernilai 1 dan -1 adalah sebanyak parameter dr.
d. Mendapatkan polinomial pesan acak e dengan persamaan (2).
e. Keluaran pesan acak e

3. Selanjutnya dilakukan penyisipan dengan *modulus function*, dengan langkah-langkah sebagai berikut:
   a. Mengubah polinomial kunci dekripsi f dan polinomial pesan acak e kedalam bentuk biner, mendapatkan bitstream kunci dekripsi dan bitstream ciphertext.
   b. Menyatukan bitstream kunci dekripsi dan ciphertext menjadi *bitstream* pesan sisip.
   c. Menghitung panjang *bitstream* pesan sisip.
   d. Membangkitkan Threshold secara acak.
   e. kunci stego = Nilai Threshold + Panjang bitstream kunci privat + Panjang *bitstream* pesan acak + parameter set NTRU
   f. Masukan citra sampul
   g. Menghitung kapasitas dari citra sampul, jika kapasitas tidak memenuhi, kembali ke langkah e.
   h. Untuk menghindari nilai pixel melebihi kisaran nilai 0 s/d 255, modifikasi seluruh nilai piksel citra dengan persamaan:

$$I(m,n) = \begin{cases} \alpha T, & jika\ I(m,n) < \alpha T \\ 255 - \alpha T, & jika\ I(m,n) > 255 - \alpha T \end{cases} \quad (14)$$

   Dimana *I(m,n)* adalah piksel citra pada baris *m* dan kolom *n*, α adalah faktor bobot integer, dan *T* adalah nilai Threshold.
   i. Melakukan transformasi tingkat 1 dengan IHWT menggunakan persamaan (8) untuk setiap blok 2x2 (7) dari citra, sehingga menghasilkan 4 *subband* yaitu LL, HL, LH, dan HH.
   j. *Bitstream* Pesan disisipkan pada koefisien *subband* HL, LH dan HH dengan *modulus function* menggunakan persamaan (10) s/d (12).
   k. Melakukan invers/rekonstruksi terhadap *subband* LL, HL, LH, dan HH dengan persamaan (9), untuk mendapatkan citra stego.
   l. Keluaran citra stego.

2.2.2 Alur Proses Pengambilan Data Teks

Sistem mengambil kembali data teks dengan mengikuti langkah-langkah berikut:

1. Melakukan ekstraksi dengan langkah-langkah sebagai berikut:
   a. Masukkan citra stego
   b. Melakukan transformasi IHWT tingkat 1 pada citra stego dengan persamaan (7)
   c. Kemudian lakukan proses ekstraksi menggunakan persamaan (10) untuk mendapatkan *bitstream* dari nilai bit-bit tersisip.
   d. Keluaran *bitstream* pesan tersisip.
   e. Pisahkan *bitstream* kunci dekripsi dan pesan acak dari dari *bitstream* pesan tersisip.
2. Dekripsi dengan NTRU dilakukan dengan menghitung polinomial a, b dan m. dengan persamaan (3), (4), dan (5).

Setelah polinomial m didapatkan, polinomial m diubah menjadi string untuk menghasilkan kembali data teksnya.

2.3 Metode Pengukuran

2.3.1 Perkiraan Kapasitas Tampung Citra

Metode untuk perkiraan kapasitas tampung sebuah citra sampul dihitung dengan rumus:

$$Kapasitas\_tampung = \frac{\left(Jumlah\ piksel * \frac{3}{4}\right)}{2} * saluran * Threshold \quad (15)$$

Dimana:

a. Jumlah piksel = Panjang piksel * lebar piksel dari citra sampul
b. Saluran = 3 Komponen dari citra sampul yaitu R, G dan B.
c. *Threshold* = Panjang bit sisip yang bernilai 1, 2 dan 3.

2.3.2 Pengukuran Kapasitas Tampung Citra

Untuk menghitung PSNR dibutuhkan hasil perhitungan dari MSE. MSE adalah nilai error kuadrat rata-rata antara citra cover dengan citra tersteganografi, secara matematis dapat dirumuskan sebagai berikut [11]:

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2 \quad (16)$$

Setelah diperoleh nilai *MSE* maka nilai *PSNR* dapat dihitung dari kuadrat nilai maksimum dibagi dengan *MSE*. Semakin rendah nilai *MSE* maka akan semakin baik, dan semakin besar nilai *PSNR* maka semakin baik kualitas citra steganografi. Secara matematis, nilai PSNR dirumuskan sebagai berikut:

$$PSNR = 10 \log\left(\frac{MAXi^2}{MSE}\right) \quad (17)$$

Dimana MAXi = nilai maksimum dari pixel citra yang digunakan. Jika nilai PSNR diatas 40dB maka kualitas citra bagus.

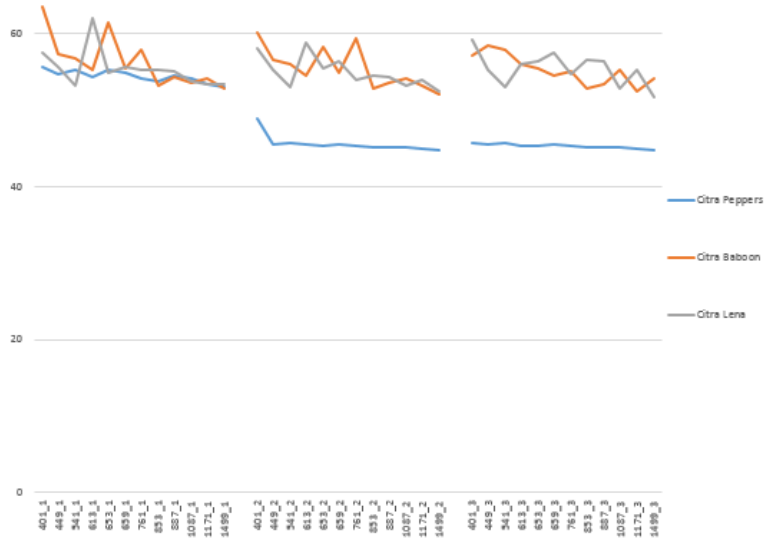
3. HASIL DAN PEMBAHASAN

Untuk pengujian, sampel citra yang digunakan adalah *BaboonRGB*, *LenaRGB*, dan *PeppersRGB*, yang di ambil dari: http://www.eecs.qmul.ac.uk/~phao/CIP/Images/. Pengujian dibagi terhadap 2 aspek, *imperceptibility* dan *robustness*. Dalam pengujian tersebut menggunakan citra sampul RGB dengan format .bmp serta berdimensi 512x512. Dengan parameter kriptografi yaitu parameter set sesuai standar *security level* IEEE dan parameter steganografi yaitu bit sisip acak dari 1-3. Pada pengujian ini menggunakan perangkat keras ASUS A44H dengan spesifikasi *intel® celeron®* CPU B800 @ 1.50GHz (2 CPUs) dan RAM 2GB. Berikut tabel rencana pengujian yang akan dilakukan:

Tabel 1. Tabel rencana pengujian

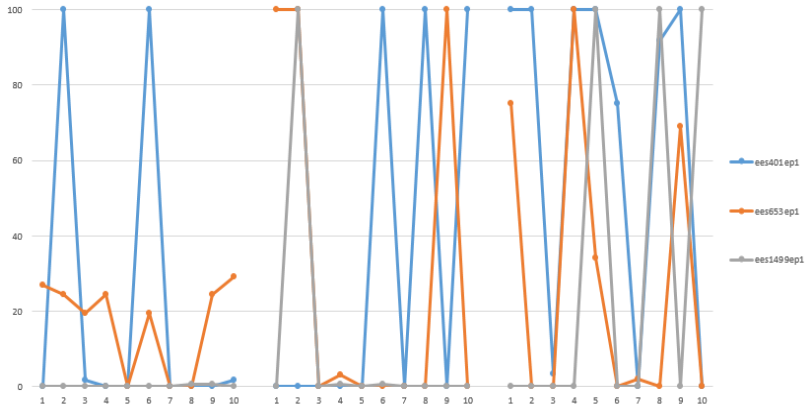
Nama citra	Ukuran citra	Parameter set	Bit sisip
BaboonRGB	512x512	ees401ep1 s/d ees1499ep1	1 s/d 3
LenaRGB	512x512	ees401ep1 s/d ees1499ep1	1 s/d 3
PeppersRGB	512x512	ees401ep1 s/d ees1499ep1	1 s/d 3

Pada pengujian terhadap *imperceptibility* kami menggunakan keseluruhan dari parameter set terhadap masing-masing bit sisip dan masing-masing citra berdimensi 512x512, sedangkan pada pengujian *robustness noise* dan kontras kami hanya menggunakan 3 parameter set yaitu ees401ep1, ees653ep1 dan ees1171ep1 terhadap seluruh bit sisip. Citra pada pengujian *noise* hanya citra *peppers* dengan persentase nilai 0,005% sedangkan citra pada kontras kami menggunakan citra *peppers* dan baboon dengan nilai -6 s/d 27. Pengujian *imperceptibility* diukur menggunakan PSNR. Pada gambar 2 di bawah merupakan grafik dari pengujiannya:

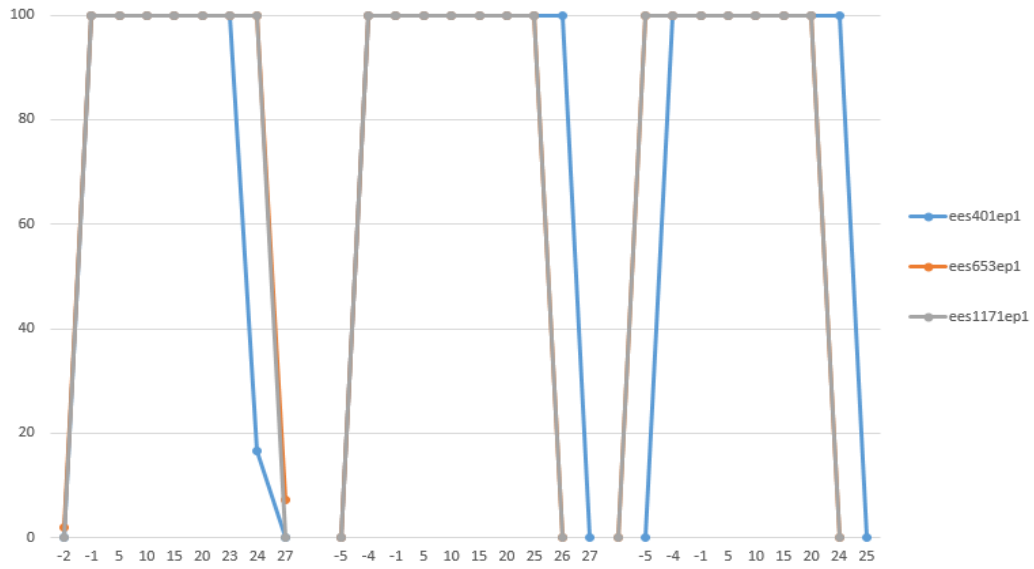


***Gambar 2. Grafik pada pengujian* imperceptibility**

Pada pengujian *imperceptibility* dari grafik diatas, dapat disimpulkan bahwa metode ini menghasilkan nilai PSNR diatas 40dB yang dimana citra dikatakan memiliki kualitas baik.Pada pengujian *robustness* kami menggunakan *noise salt and pepper* yang dibangkitkan sebanyak persentase dari ukuran citra, kemudian diacak posisinya pada citra stego sedangkan pengujian kontras dilakukan dengan menambah semua nilai komponen citra sebesar nilai kontras yang dimasukkan. Berikut grafik dari hasi pengujiannya:



***Gambar 3. Grafik pada pengujian* robustness *terhadap* noise**



Gambar 4. Grafik pada pengujian* robustness *terhadap kontras

Sumbu y dari Gambar (3) dan (4) diatas menunjukkan persentase kembali pesan, dimana sumbu x pada Gambar (3) menunjukkan iterasi percobaan dengan posisi noise yang acak setiap kalinya, sedangkan sumbu x pada Gambar (4) menunjukkan nilai kontras yang ditambahkan pada citra stego. Berdasarkan persentase kembali pesan pada grafik hasil pengujian *robustness* terhadap *noise* di atas dapat dilihat bahwa dengan nilai persentase *noise* yang sangat kecil pada citra yaitu 0,005% dapat menyebabkan pesan kembali dan tidak kembali sama sekali atau dengan kata lain sistem ini sangat sensitif terhadap *noise salt and pepper*. Namun, pada pengujian *robustness* terhadap kontras menghasilkan nilai yang tergantung pada citra yang digunakan, pada citra *peppers* dengan tahan sampai nilai kontras 24.

4. KESIMPULAN

Berdasarkan hasil pengujian yang sudah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Kualitas citra hasil dari segi *imperceptibility* termasuk kategori baik dengan nilai PSNR diatas 40 dB
2. Penambahan noise dalam ukuran kecil saja pada citra sangat berdampak citra.
3. Pengaruh ketahanan citra terhadap kontras sangat tergantung pada citra yang digunakan.

5. SARAN

Adapun saran yang dapat digunakan untuk pengembangan penelitian ini menjadi lebih baik adalah sebagai berikut:

1. Media tempat penyembunyian dapat dilakukan dengan format lain seperti video.
2. Pada penelitian ini, tingkat transformasi IHWT yang dilakukan adalah 1 kali, penelitian selanjutnya dapat dicoba dengan tingkat transformasi yang lebih tinggi dengan harapan hasil yang lebih baik.

DAFTAR PUSTAKA

[1] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, “Privacy and

cybersecurity: The next 100 years," *Proc. IEEE*, vol. 100, no. SPL CONTENT, pp. 1659–1673, 2012.
[2] I. Technology, "Cyber-Crimes and their Impacts : A Review Cyber-Crimes and their Impacts : A Review," no. July, 2015.
[3] C. Yashwanth Roy and M. Kumar Goel, "Review on Image Steganography," *Indian J. Sci. Technol.*, vol. 9, no. 47, 2016.
[4] N. Raftari and A. M. E. Moghadam, "Digital image steganography based on Integer Wavelet Transform and assignment algorithm," *Proc. - 6th Asia Int. Conf. Math. Model. Comput. Simulation, AMS 2012*, pp. 87–92, 2012.
[5] P. W. Adi, F. Z. Rahmanti, and N. A. Abu, "High quality image steganography on integer Haar Wavelet Transform using modulus function," *Proc. - 2015 Int. Conf. Sci. Inf. Technol. Big Data Spectr. Futur. Inf. Econ. ICSITech 2015*, no. February 2016, pp. 79–84, 2016.
[6] B. Li, J. He, and J. Huang, "A survey on image steganography and steganalysis," *J. Inf. Hiding*, vol. 2, no. 2, pp. 142–172, 2011.
[7] N. Challa and J. Pradhan, "Performance Analysis of Public key Cryptographic Systems RSA and NTRU," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 8, 2007.
[8] R. Behnia, M. O. Ozmen, and A. A. Yavuz, "Lattice-Based Public Key Searchable Encryption from Experimental Perspectives," *IEEE Trans. Dependable Secur. Comput.*, pp. 1–14, 2018.
[9] J. Hoffstein, D. Lieman, J. Pipher, and J. H. Silverman, "NTRU: A public key cryptosystem," pp. 1–17, 1999.
[10] P. G. Tata, H. Narumanchi, and N. Emmadi, "Analytical study of implementation issues of NTRU," *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 700–707, 2014.
[11] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *J. Syst. Softw.*, vol. 81, no. 1, pp. 150–158, 2008.