BAB II

TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Penelitian Terkait

Dari beberapa penelitian yang telah di lakukan oleh peneliti terdahulu, hasil menunjukan tentang kinerja IHWT dan *Coeffisient Difference* pada media image digital. Penelitia tersebut diantaranya adalah sebagai berikut:

Chung-Ming Wang, Nan- I wu, Chwei- Shyong Tsai, Min- Shiang Hwang[1]. Pada penelitiannya, penulis membandingakan pixel value differencing dan modulus function untuk penyisipan pesan rahasia. Pada PVD dari dua piksel berturut- turut untuk merekam informasi pesan rahasia yang lebih banyak dan lebih fleksibel. Skema embedding data rahasia dapat secara signifikan dikurangi dengan optimal. Selain itu, juga dapat memecahkan batas rentang (0 - 255) dari dua sisi.

Nur Azman Abu, Prajanto Wahyu Adi, dan Othman Mohd[2]. Dalam penelitian ini, penulis mengusulakan sebuah metode yang digunakan untuk menyembunyikan pesan rahasia pada domain *Integer Haar Wavelet Transform* (IHWT) dengan cara menghitung nilai perbedaan antara dua koeffisien dari wavelet tetangga. Perbedaan koefisien dihitung dalam jumlah presisi yang terbatas yang sesuai kompatibel dengan IWT. Pada penelitian ini menggunakan nilai ambang batas untuk menyisipkan pesan rahasia pada *image- cover*. Dan hasil dari penelitian ini menunjukan bahwa, pesan yang disisipkan pada 1- level IHWT yang diterapkan pada metode *Coefficient Difference*. Metode yang di usulkan dapat dengan mudah mengungguli kinerja dari IHWT dan PMM dalam hal imprecebiliti dan kapasitas maksimum.

Jianyun Xu, Andrew H. Sung, Peipei Shi, Qingzhong Liu [3], pada penelitiannya menyimpulkan karena keuntungan dari transformasi wavelet, terutama bilangan bulat transformasi wavelet, peneliti lebih suka menggunakan Integer Haar Wavelet Transform (IHWT) melalui skema angkat yang telah digunakan oleh [3] untuk bekerja pada domain frekuensi gambar. IHWT ini dikembangkan dari Discrete Haar Wavelet Transform melalui skema angkat. Ini mengubah bilangan bulat nilai-nilai pixel dari suatu gambar ke dalam koefisien bulat wavelet dan sebaliknya. Dalam rangka untuk mengubah gambar ke subbands wavelet, sebuah gambar dibagi menjadi 2x2 blok non-overlapping. Dan telah ditemukan bahwa transformasi DWT dengan fungsi Haar Wavelet memberikan pemulihan gambar yang lebih baik.

J. K. Mandal dan Debashis Das [4]. Dalam tulisan ini, telah dibahas metode steganografi untuk menyembunyikan pesan rahasia dengan menggunakan metode *Pixel Value Differencing* (PVD) dan juga menjamin bahwa tidak ada nilai piksel yang disisipkan melebihi nilai kisaran antara 0 sampai 255 dalam stego- image. Peneliti telah menggunakan metode PVD asli yang mana nilai piksel tidak melebihi batas - batas kisaran. Pada penelitian lain mengusulkan metode lain untuk diterapkan pada proses embedding data dan memberikan kapasitas penyisipan yang sama dengan PVD asli dengan kualitas stego- image diterima.

Tabel 2. 1 Penelitian Terkait

No	Penulis	Tahun	Judul	Metode	Hasil
1.	Chung-Ming Wang, Nan- I wu, Chwei-Shyong	2007	A high quality steganographic method with pixel	Pixel Value Differencing dan Modulus Function.	Pada PVD dari dua piksel berturut- turut untuk merekam informasi pesan rahasia yang lebih banyak dan lebih

	Tsai, Min-Shiang Hwang		value differencing and modulus function.		fleksibel. Skema embedding data rahasia dapat secara signifikan dikurangi dengan optimal. Selain itu, juga dapat memecahkan sisi dua piksel keluar dari batas [0 255].
2.	Nur Azman Abu, Prajanto Wahyu Adi, Othman Mohd	2014	Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform	Coefficient Difference dan IHWT	hasilnya menunjukan bahwa IHWT dan *Coefficient Difference* dapat dengan mudah mengungguli metode yang mengimplementasikan IHWT dan *Pixel Metode Mapping* (PMM) dalam hal kapasitas maksimum serta imperceptibility
3.	Jianyun Xu, Andrew H. Sung, Peipei Shi, Qingzhong Liu	2004	JPEG Compression Immune Steganography Using Wavelet Transform	Wavelet Transform	IHWT ini dikembangkan dari Discrete Haar Wavelet Transform melalui skema angkat. Ini mengubah bilangan bulat nilai-nilai pixel dari suatu gambar ke dalam koefisien bulat wavelet dan sebaliknya.

4.	J. K. Mandal dan Debashis Das	2012	Steganography using Adaptive Pixel Value Differencing (APVD) of Gray Image Through Exclusion of Overflow/ Underflow	Adaptive Pixel Value Differencing (APVD)	Telah dibahas steganografi dengan PVD dan menunjukan bahwa tidak ada nilai pixel yang melebihi kisaran [0 255] pada stego-image. Menggunakan PVD dalam kisaran [0 255] dan memberikan kapasitas yang embedding yang sama dengan PVD asli dengan kualitas stego- image diterima.

2.2 Tinjauan Pustaka

2.2.1 Steganografi

Pesatnya perkembangan internet dekade ini semakin mempermudah pengiriman pesan. Tapi, bagaimana dengan keamanan informasi yang ada dalam pesan tersebut. Pesan yang dikirim lewat internet sering kali disadap atau dibajak oleh orang lain yang tidak berwenang untuk kepentingan lain (guna kejahatan). Salah satu cara mengamankan pesan yang dikirim lewat internet yaitu dengan menggunakan steganografi. Pada peristiwa penyerangn gedung WTC 11 September 2001 Steganografi digunakan oleh para teroris untuk melakukan komunikasi.

Kata steganografi berasal dari dua suku kata yakni Steganos yang memiliki arti rahasia atau penutup, dan Garphia yang berarti menulis atau menggambar. Steganografi merupakan teknik menyembunyikan informasi sehingga tidak dapat terdeteksi atau terbaca oleh orang lain. Dimana, data hanya dapat dibaca atau dideteksi oleh pemilik dan penerima data [9].

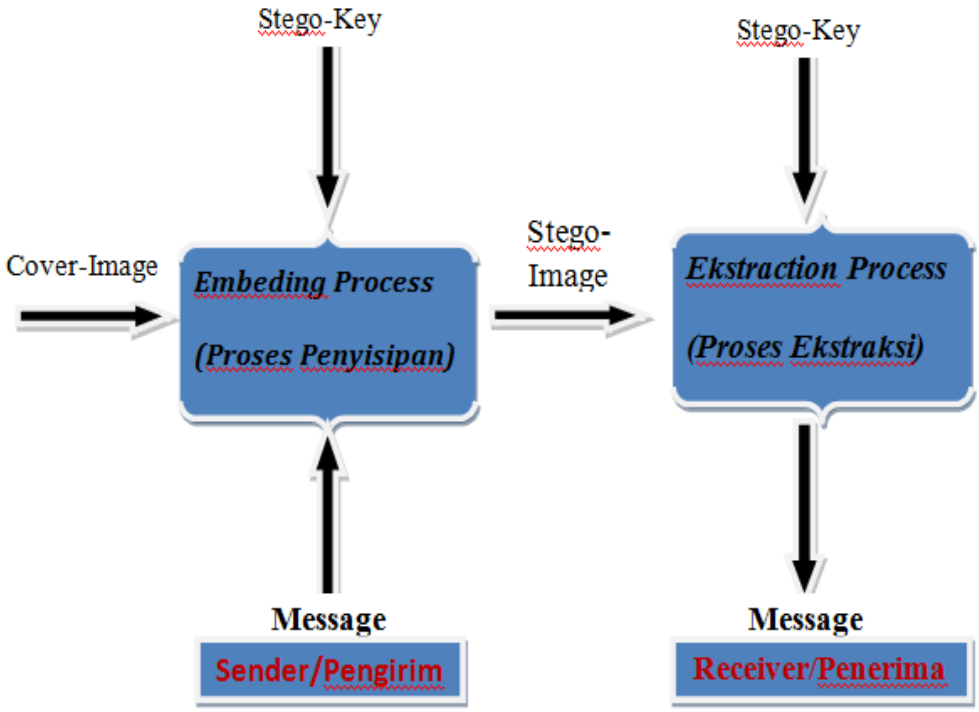
Dari pembahasan lain, kata *Steganography* berasal dari bahasa Yunani yakni *Steganos* yang berarti terselubung atau tersembunyi dan *Grapein* yang memilki arti menulis, sehingga steganography kurang lebih berarti "menulis karya yang terselubung atau tersembunyi" [10].

Steganografi digunakan sebagai teknik untuk mengamankan data sementara terdiri dari dua bagian yaitu induk dan pesan. Di sisi lain, teknik ini terbagi dalam penyisipan dan pengekstrakan proses. Umumnya, Steganografi mungkin dapat menggunakan kunci untuk disisipkan dalam induk yang disebut kunci Stego. Melalui kunci terpilih, pemilik dapat mengekstrak file stego dan menghasilkan file asli.

Steganografi mempunyai banyak sekali metode komunikasi untuk penyembunyian pesan dan terus dikembangkan dengan penemuan-penemuan metode baru. Metode ini tidak tampak, seperti tanda tangan digital, pengaturan kata, microdots, komunikasi spectrum lebar dan juga jalur tersembunyi.

Beberapa istilah yang biasa di gunakan dalam steganografi adalah sebagai berikut:

1. *Embedded message* atau *hiddentext,* yakni pesan yangdi sembunyikan.
2. *Cover-objeck* atau *cover-image*, yakni pesan atau gambar yang digunakan untuk menyembunyikan atau menyisipkan pesan (*Embedded message*).
3. *Stego- image* yaitu pesan yang sudah berisi *embedded message*.
4. *Stego- key* yakni kunci yang digunakan untuk menyisikan atau menyembunyikan dan menaampilakan kembali *embedded message*.



Gambar 2. 1 Gambaran Sistem

Diatas merupakan gambaran dari system steganografi pada umumnya, dimana *sender* (pengirim pesan) dilakukan proses embedding (proses penyisipan/ penyembunyian pesan) yang akan dikirim secara rahasia ke *receiver* (penerima pesan). Pesan rahasia di masukkan atau disisipkan pada *cover-image* dengan rumusan key (kunci tertentu) sehingga data tersembunyi dalam *stego.* Di bagian receiver (penerima pesan), dilakukan proses akstraksi guna memisahkan pesan rahasia dengan data yang di jadikan sebagai cover untuk penyembunyian pesan tadi dengan membalik kunci yang sama dalam proses *embedding*. Jadi, hanya pengirim dan penerima pesan yang tau kunci ini dan dapat membuka untuk mengetahui isi pesan rahasia ini.

Steganografi adalah teknik yang digunakan untuk mengamankan pesan (data) sementara yang terdiri dari dua bagian yakni cover dan pasan. Dalam definisi lain, teknik ini terbagi dalam proses penyisipan dan pengekstrakan. Umumnya, steganografi menggunakan kunci untuk menyisipkan dalam cover disebut dengan key-Stego. Melelui kinci pilihan, *sender* dan *receiver* dapat mengekstrak file stego shingga terpisah dari cover dan menjadi file asli.

Banyak hal yang di implementasikan dengan memanfaatkan steganografi diantaranya sebagai contoh adalah:

1. Dibidang kesehatan, digunakan untuk informasi penjelas dengan menyertakan sebuah gambar hasil pempriksaan (seperti menyertakan hasil X-ray sebagai catatan dokter).
2. Dibidang IT, sebagai sarana komunikasi privasi peer-to-peer, mengirimkan informasi rahasia pada web untuk mengghidari penyadapan dan penyebaran informasi data, digunakan untuk menyembunyikan data rahasia pada jaringan untuk menghindari penyalahgunaan data.
3. Dibidang kesenian, sebagai pelindung hak cipta (untuk memberikan tanda pada hasil karya fotografer).

Criteria yang harus ada pada steganografi adalah:

1. *Imperceptibility*, adalah pesan yang disembunyikan tidak dapat di deteksi oleh panca indra sehingga orang yang tidak memiliki wewenang tidak dapat mengetahui isi pesan yang disisipkan.
2. *Fidelity*, adalah gambar yang digunakan sebagai *cover-image* tidak banyak berubah sehingga tidak menimbulkan kecurigaan adanya pesan yang disisipkan.
3. *Recovery*, adalh pesan yang disispkan harus dapat di ekstraksi kembali.

4. *Robustness*, pesan rahasia yang disisipkan harus tahan terhadap manipulasi yang dilakukan pada *cover*,(misalnya tahan terhadap kompresi, penentuan threshold, dls).

Tabel 2. 2 Perbedaan antara Steganografi, Kriptografi, dan Watermarking [9]

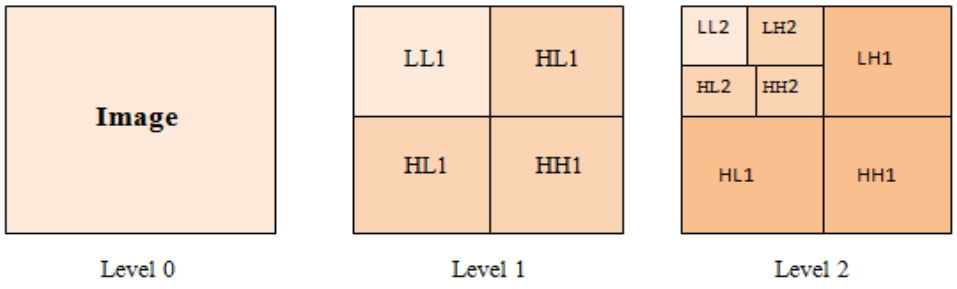
Karakteristik	**Steganografi**	**Kriptografi**	**Watermarking**
Data rahasia	Text, gambar, audio, video, protocol/ IP	Plaintext	Gambar, video, audio
Kunci	Ya/ tidak	Ya	Ya/ tidak
Kapasitas data	Besar	Sangat kecil	Kecil
Ekstraksi	Bias digunakan untuk semua induk	Hanya bisa digunakan pada kriptografi saja	Hanya bias digunakan pada watermarking saja
Aksi	Detected	De-cipher	Remove/ replace
Serangan	Steganalysis	Cryptanalysis	Image processing
Kenampakan	Tidak	Ya	Ya/ tidak
Deteksi	Sangat susah	Mudah	Susah
Hasil	Stego-file	Cipher-text	Watermark-file
Tujuan akhir	Secret communication	Data protection	Authentication

Hasil dari table 2.2 merupakan analisis dari beberapa jurnal dan rangkuman ini dibuat dalam bentuk tabel untuk menunjukan perbandingan antara steganografi, kriptografi, dan watermarking. Maka, dari table 1 tersebut menjadi alasan bagi penelitian ini untuk menggunakan menggunakan metode steganografi dalam penelitian ini. Dengan hasil table tersebutlah dapat menjadi alasan bagi peneliti untuk mempelajari dan mendalami system keamanan dengan menggunakan teknik steganografi.

2.2.2 Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) merupakan transformasi linear yang berkerja pada data vektor yang kekuatan panjang integernya dua, kemudian di ubah menjadi angka vector yang berbeda dengan panjang vector yang sama. DWT telah di implementasikan pada steganografi dan memperbarui metode dari *Discrete Cosine Transform* (DCT). Dengan DWT akan menutupi kekurangan dari DCT yaitu pemadatan energy tanpa ada blok artefak yang menghalangi. Saat ini, DWT digunakan untuk berbagai macam pengolahan sinyal aplikasi, serperti simulasi distribusi antenna nirkabel, penghapusan kebisingan pada audio, dan juga audio dan video kompresi. Wavelet transform banya digunakan dalam aplikasi yang sangat baik, karena sebagian besar dari sinyal kehidupan nyata yang dihadapi adalah variasi waktu pada alam. Dan wavelet telah mengkonsentrasikan energinya di waktu dan baik untuk analisis transien, sinyal waktu yang bervariasi.

DWT dibagi menjadi beberapa komponen dalam bentuk pita frekuensi yang disebut dengan band yang dikenal dengan sub. Satu set dalam fitur DWT adalah vektor yang mengandung energi koefisien wavelet dihitung subbands pada skala berturut- turut. Pada pengolahan citra digital, 2- Dimensi *Discrete Wavelet Transform* (2D - DWT) gambar 2 – dimensi di uraikan menjadi empat sub-band, seperti pada gambar berikut:



Gambar 2. 2 2- Dimensi DWT

Keterangan: LL = Horizontal dan vertikal rendah, LH = horizontal dan vertikal tinggi, HL = horizontal tinggi dan vertikal rendah, HH = horizontal dan vertikal tinggi .

LL adalah nilai rata-rata dari gambar yang memiliki sinyal frekuensi rendah, untuk HL, LH, dan HH mewakili bagian horizontal, vertical dan diagonal dari masing – masing gambar. Intinya, dua dimensi wavelet transform dilakukan dengan menerapkan satu dimensi dari wavelet filter pada rangka horizontal kemudian diikuti dengan urutan vertical.

Pada aplikasi 2- dimensi, ada tingkatan dekomposisi, yang pertama dilakukan adalah DWT di vertical arah, di ikuti dengan DWT di horizontal arah. Setelah dekomposisi pada tingkat pertama, image di bagimenjadi 4 sub-band seperti di atas yaitu LL1, LH1, HL1, dan HH1. Setiap tingkat dekomposisi yang berurutan, sub-band LL dari tingkat sebelumnya digunakan untuk input. Pada dekomposisi tingkat ke dua, DWT diterapkan pada band LL1 yang akan di urai lagi menjadi empat sub-band yaitu LL2, LH2, HL2, dan HH2. Begitu pun untuk dekomposisi tingkat ketiga, DWT dari Band LL2 di uraikan lagi menjadi empat sub band lagi yakni LL3, LH3, HL3, dan HH3. Hal tersebut dapat menyebabkan 10 sub-band per komponen dan LH1, HL1, dan HH1 memiliki pita frekuensi tertinggi, sementara LL3 mengandung pita frekuensi yang terendah.

2.2.3 Integer Wavelet Transform (IWT)

Pada umumnya, domain wavelet sangat memungkinkan untuk digunakan dalam proses penyembunyian data di daerah *Human Visual System* (HVS) terhadap daerh yang kurang sensitive, seperti pada daerah detail band resolusi tinggi (HL, LH, dan HH). Menyembunyikan data rahasia pada daerah ini sangat memungkinkan kita untuk meningkatkan kekuatan atau kekokohan sementara dengan mempertahankan kualitas yang baik.

Integer Wavelet Transform (IWT) memetakan integer data set ke integer data set lain. Pada *Discrete Wavelet Transform*, digunakan filter wavelet titik floating koefisien sehingga saat kita menyembunyikan data di koefisien tersebut setiap transaksi dari nilai- nilai floting dari piksel harus bilangan bulat dan dapat menyebabkan hilangnya beberapa informasi yang tersembunyi yang dapat menimbulkan kegagalan dari system data yang disembunyikan [9][10].

Untuk menghindari masalah presisi floating point atau hilangnya informasi dari filter wavelet saat menginputkan integer bilangan bulat seperti pada image digital, outputnya tidak lagi bilangan bulat yang tidak memungkinkan pengembalian yang sempurna dari gambar inputan dan dalam hal ini aka nada hilangnya informasi seperti membalik, mengubag atau menambah informasi lain.

Karena perbedaan dalam bilangan bulat dari *Integer Wavelet Transform* (IWT) dan *Discrete Wavelet Transform* (DWT) sub-band LL pada kasus IWT merupakan perubahan terdekat dengan skala yang lebih kecil dari gambar asli dan dalam kasus DWT LL yang dihasilkan sub-band akan terdistori. Untuk itu, mengangkat skema merupakan salah satu dari beberapa teknik yang dapat digunakan untuk integer bilangan bulat pada transformasi wavelet.

2.2.4 Integer Haar Wavelet Transform (IHWT)

Dilihat keunggulan dari wavelet transform, untuk berkerja pada domain image frekuensi terutama pada bilangan bulat transformasi wavelet, sehingga peneliti lebih suka menggunakan *Integer Wavelet Transform* (IHWT). *Integer Haar Wavelet Transform* dikembangkan melalui skema angkat dari *Discrete Haar Wavelet Transform* (DHWT).

Sebuah image akan dirubah menjadi 2x2 blok non-overlapping untuk mengubah gambar ke dalam sub-band wavelet.

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix}$$

Berikut merupakan cara memproses 1D HDWT dalam vertical dan di ikuti 1D HDWT dalam arah horizontal:

$$cA = \left\lfloor \frac{\left\lfloor \frac{w+x}{2} \right\rfloor + \left\lfloor \frac{y+z}{2} \right\rfloor}{2} \right\rfloor \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$$cH = \left\lfloor \frac{w-x+y-z}{2} \right\rfloor \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(2)$$

$$cV = \left\lfloor \frac{w+x}{2} \right\rfloor - \left\lfloor \frac{y+x}{2} \right\rfloor \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

$$cD = w - x - y + z \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots....(4)$$

cA merupakan nilai piksel dari LL, cH sebagai HL, cV sebagai LH, dan cD merupakan nilai piksel dari HH.

Untuk membangun koefisien wavelet, IHWT akan di lakukan pada setiap individu koefisien di setiap sub-band. Hal tersebut akan mengakibatkan blok 2x2 pada ukuran piksel seperti berikut. Disini penulis menggunakan fungsi lifting pada horizontal dan vertical 1D Invers HDWT untuk mengembalikan sinyal komposit asli dari koefisien.

$$\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} w' & x' \\ y' & z' \end{bmatrix}$$

Secara matematis Invers-HDWT dapat dirumuskan sebagai berikut:

$$w' = cA + \left\lfloor \frac{cV+1}{2} \right\rfloor + \left\lfloor \frac{cH + \left\lfloor \frac{cD+1}{2} \right\rfloor + 1}{2} \right\rfloor \quad \text{.....(5)}$$

$$x' = w' - \left(cH + \left\lfloor \frac{cD+1}{2} \right\rfloor \right) \quad \text{.....(6)}$$

$$y' = cA + \left\lfloor \frac{cV+1}{2} \right\rfloor - cV + \left\lfloor \frac{cH + \left\lfloor \frac{cD+1}{2} \right\rfloor - cD + 1}{2} \right\rfloor \quad \text{.....(7)}$$

$$z' = y' - \left(cH + \left\lfloor \frac{cD+1}{2} \right\rfloor \right) - cD \quad \text{.....(8)}$$

w', x', y', z' merupakan bentuk invers dari cA, cH, cV, dan cD.

Frequensi bagian terendah dari DCT, F (0,0) dan 3-level koefisien perkiraan 3 cA mewakili semua sub-band terendah dari sinyal asli. Dan sebagian F(0,0) akan tetap utuh di bawah kuantisasi setiap tingkat itu. Untuk

itu[16], penulis menganggap bahwa informasi yang tertanam dalam 3 cA akan kebal terhadap tingkat tertinggi dari JPEG kompresi.

2.2.5 Coefficient Different

Coefficient Differece merupakan sebuah algoritma yang digunakan untuk menyembunyikan pesandengan memanfaatkan nilai perbedaan antara dua nilai koefisien wavelet tetangga [3]. Teknik coefficient difference ini di adaptasi dari *Pixel Value Differencing* (PVD). Metode *Coefficient Difference* ini menanamkan dan menyembunyikan pesan rahasia dengan nilai-nilai yang berbeda pada jumlah presisi yang terbatas dan cocok dalam *Integer Wavelet Transform* (IWT).

Dengan metode *Coefficient Difference* pada sebuah komputer baru dan efisien berbasis steganografi untuk embedding pesan rahasia pada sebuah image

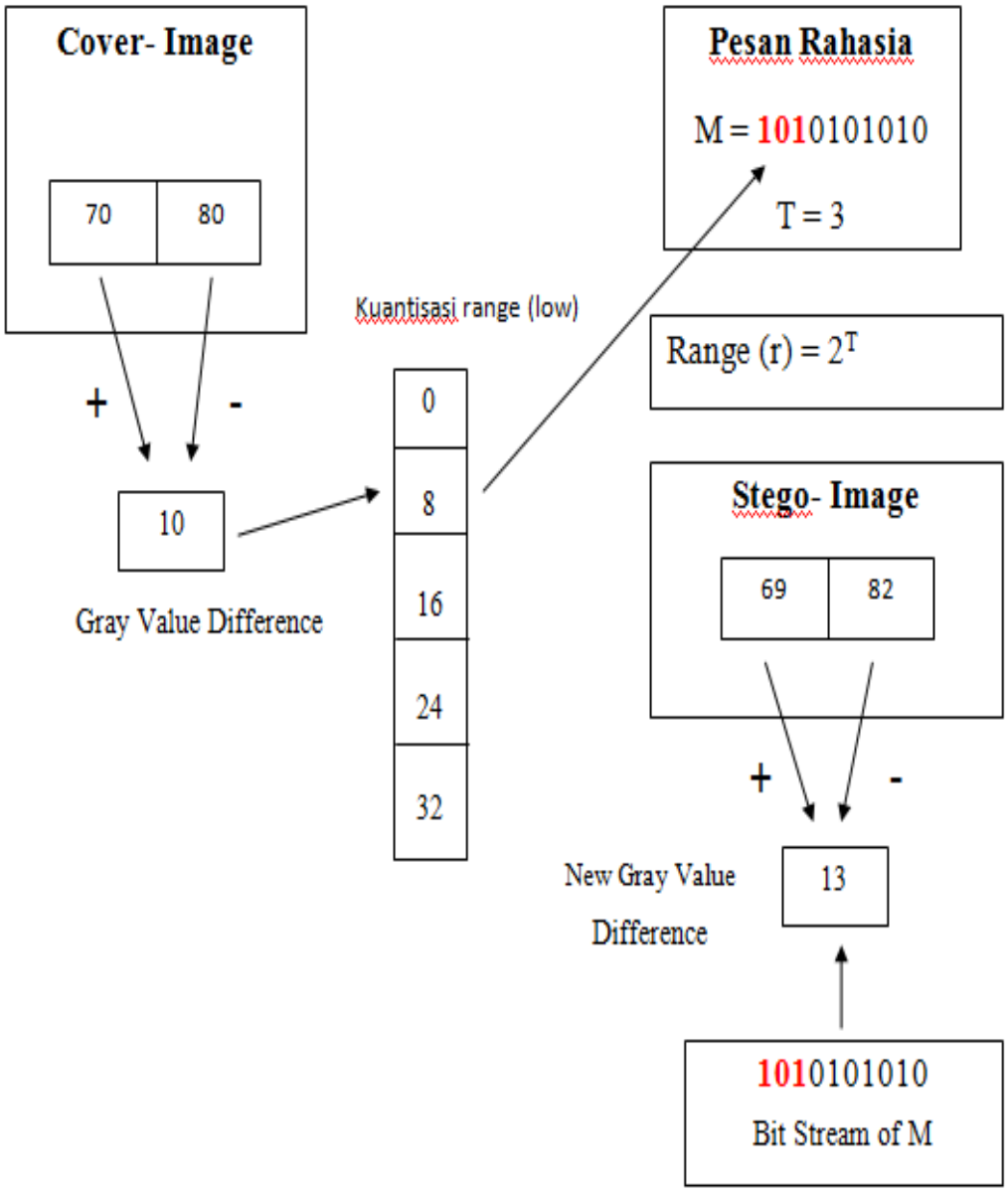
tanpa menghasilkan perubahan yang nyata. Tidak perlu referensi dari image asli saat pemanggilan kembali pesan rahasia yang tertanam pada *stego- image*.

Metode *Coeficient Difference* ini memanfaatkan karakteristik dari visi sensitive manusia s untuk variasi nilai abu- abu. Pesan rahasia yang ditetanam pada *cover-image* dengan cara mengganti nilai perbedaan dari dua blok piksel di *cover- image* dan bit pesan rahasia akan disisipkan atau di tanam pada nilai perbedaan dari *cover- image*.

Coefficient Difference tidak hanya memberikan cara yang lebih baik dalam proses embedding data dalam jumlah besar menjadi *cover- image* dengan imperceptions, tapi juga memberikan cara mudah untuk memberkan kerahasiaan data. Metode penyisipan data ini dapat dengan mudah diperluas untuk efisiensi pembawaan pesan, seperti memberikan keterangan penjelasan hak milik dalam audio dan video bahkan pada image oleh embedding data dalam setiap pasangan piksel yang berdekatan sinyal dari data strem.

Sebuah gambaran dari proses penyisipan pesan rahasia ditunjukan pada gambar berikut. Dimana pesan rahasia yang akan di sisipkan pada *cover-image* diubah dulu dalam bentuk biner. Kemudian menentukan nilai ambang batas (T) yang nantinya digunakan untuk menentukan rentang kuantisasi (r). tentukan nilai selisih dari dua piksel yang saling berdekatan dari *cover- image* dan tentukan nilai perbedaan piksel yang baru sebagai hasil dari nilai piksel *stego- image.*

Coefficient Difference merupakan metode yang sangat cocok untuk digabungkan dengan IHWT untuk diterapkan pada citra digital, karena pada citra hanya terdapat angka berupa integer sehingga tidak ada informasi yang hilang karena presisi floting point.



Gambar 2. 3 Sebuah Ilustrasi dari Perhitungan *Coefficient Difference*

Secara matemetis dapat ditulis sebagai berikut:

$$r = 2^T$$

$$D = | I_{(x)} - I_{(x+1)} |$$

$$D' = l_k + M$$

$$I' = I'_{(x)} , I'_{(x+1)}$$

$$s = | D - D' |$$

$$I'_{(x)} = I_{(x)} - \left\lfloor \frac{s}{2} \right\rfloor$$

$$I'_{(x+1)} = I_{(x+1)} + \left\lceil \frac{s}{2} \right\rceil$$

Ket: r = rentang / range

T = ambang batas / Threshold

I = citra / cover- image

D = nilai difference / selisih

D' = nilai selisih yang baru

l_k = nilai lower dari rentang kuantisasi

M = pesan yang disisipkan

s = nilai selisih mutlak dari D dan D'

I' = nilai piksel baru dari citra

2.2.6 Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang di ukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dengan satuan decibel (dB). PSNR digunakan untuk mengetahui perbandingan kualitas citra asli sebelum dan sesudah disisipi pesan. Untuk menentukan PSNR, terlebih dahulu harus menentukan nilai dari MSE (Mean Square Error). MSE adalah nilai error kuadrat rata- rata antara host images dengan stego images

Semakin kecil nilai MSE semakin bagus produk steganografi yang digunakan. Artinya, kualitas citra setelah disisipi pesan rahasia hamper sama dengan kualitas dari citra asli sebelum disisipi pesan rahasia. Hasil MSE berbanding terbalik dengan hasil PSNR. Jika nilai MSE semakin kecil maka nilai PSNR akan semakinbesar. MSE didefinisikan sebagai berikut:

$$\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} . \sum_{y=1}^{N} (Sxy - Cxy)^2$$

Dimana x dan y adalah koordinat dari citra, M dan N dimensi dari citra, S_{xy} menyatakan Stego- image dan C_{xy} adalah *host- image*.

Dalam suatu pengembangan dan pelaksanaan rekontruksi citra diperlukan perbandingan antara *Stego-Image* dan *Host-Image*. Nilai PSNR yang lebih tinggi menyatakan bahwa citra tidak rusak. Jadi untuk nilai PSNR mendekati 50 maka algoritma yang di ujikan sudah bagus dan layak untuk di implementasikan. PSNR dapat dinyatakan sebagai berikut:

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Tabel 2. 3 Nilai PSNR

PSNR (dB)	Kualitas Citra
60	Istimewa (excellent)
50	Bagus (good)
40	Layak (reasonable)
30	Cukup (poor picture)
20	Tidak dapat di pakai (unusable)

Berikut contoh perhitungan MSE dan PSNR:

7	1	1	5
2	3	4	3
5	0	6	4
4	5	6	7

Host Image

6	1	1	3
3	3	3	2
5	3	6	1
1	5	6	3

Stego Image

MSE = 1 + 0 + 0 + 4 + 1 + 0 + 1 + 1 + 0 + 9 + 0 + 9 + 9 + 0 + 0 + 1 /16

MSE = 51/16

MSE = 3.1875

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{3.1875} \right) = 43.0963$$

2.2.7 SSIM

SSIM merupakan kualitas matriks yang terkenal yang digunakan untuk mengukur kesamaan antara citra asli dengan citra yang telah di kompresi atau pun citra yang telah disisipi pesan rahasia. SSIM indek mengolah matrik dari 2 gambar yang di bandingkan. SSIM ini dikembangkan oleh Wang et al. SSIM ini berkorelasi dengan persepsi kualitas *Human Visual System* (HVS). Perancangan SSIM tidak mengembangkan metode error dengan penjumlahan tradisional, dengan pemodelan setiap distorsi gambar sebagai kombinasi dari tiga factor yaitu distorsi kontras, distorsi pencahayaan dan kehilangan korelasi. Secara matematis SSIM dapat di tulis sebagai berikut:

$$\mathrm{SSIM}(x,y) = l(x,y)\, c(x,y)\, s(x,y)$$

$$\text{Dimana, } \begin{cases} l(x,y) = \dfrac{2\mu_x 2\mu_y + C_1}{\mu^2 x + \mu^2 y + C_1} \\ c(x,y) = \dfrac{2\sigma_x 2\sigma_y + C_2}{\sigma^2 x + \sigma^2 y + C_2} \\ s(x,y) = \dfrac{\sigma_{xy} + C_3}{\sigma_x + \sigma_y + C_3} \end{cases}$$

Istilah pertama di (4) adalah fungsi pencahayaan perbandingan yang mengukur kedekatan mean dua gambar ' luminance (uF dan ug). Faktor ini maksimal dan sama dengan 1 hanya jika uF = ug. Istilah kedua adalah perbandingan kontras fungsi yang mengukur kedekatan kontras dua gambar. Berikut kontras diukur dengan standar deviasi σf dan σg. Istilah ini adalah maksimal dan sama dengan 1 hanya jika σf = σg. Istilah ketiga adalah fungsi struktur perbandingan yang mengukur koefisien korelasi antara dua gambar f dan g. Catatan σfg bahwa adalah kovarians antara f dan g.

Nilai-nilai positif dari indeks SSIM berada di [0,1]. Nilai 0 berarti tidak ada korelasi antara gambar, dan 1 berarti bahwa f = g. Konstanta positif C 1, C 2 dan C 3 digunakan untuk menghindari denominator null.

Sebenarnya, SSIM di desain sebagai metode baru yang lebih baik dri MSE dan PSNR[…]. SSIM menggunakan informasi structural dari degradasi gambar , dimana tiap- tiap piksel gambar memiliki dependensi yang membawa informasi penting tentang structural dari gambar secara visual.

Matriks SSIM didapat dari perhitungan 2matrik gambar (x,y) yang memiliki ukuran n x m. rumus dari SSIM sebagai berikut:

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

μ_x adalah nilai rata- rata dari x σ_y^2 adalah nilai varian dari y

μ_y adalah nilai rata- rata dari y σ_{xy} adalah nilai covarian dari xy

σ_x^2 adalah niali varian dari x

$C_1 = (K_1L)^2$, $C_2 = (K_2L)^2$ merupakan dua variable untuk menstabilkan devisi yang memiliki dominator yang rendah.

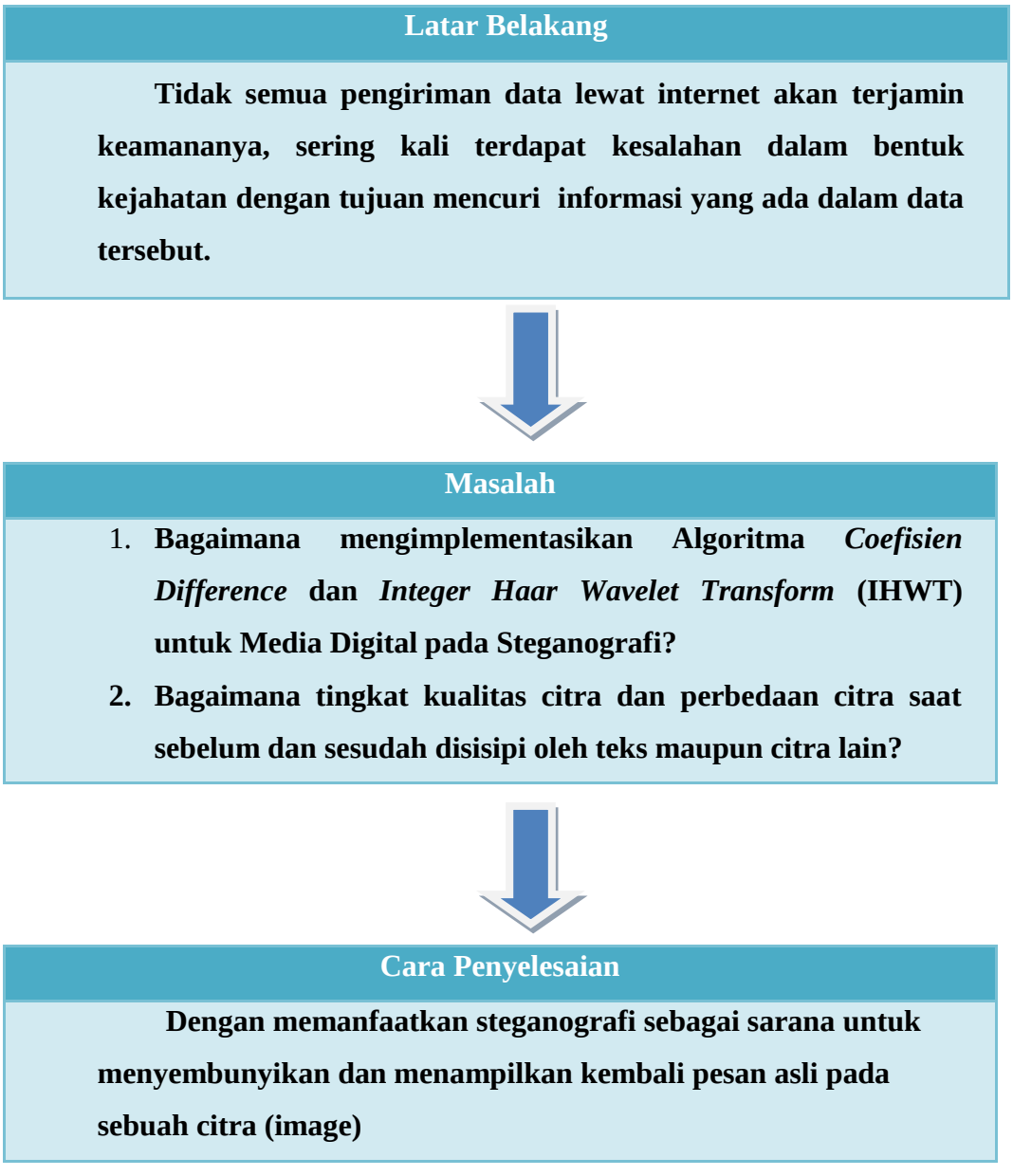
L adalah rentang piksel-value.

$K_1 = K_2 = 0.01$ merupakan nilai default.

Hasil perhitungan SSIM adalah nilai decimal antara 0 dan 1. Dimana nilai decimal semakin mendekati angka 1 maka berarti 2 gambar yang di bandingkan semakin menyerupai atau dapat dikatakan semakin mendekati 1 maka kedua gambar semakin mirip dan juga sebaliknya semkin mendekati 0 maka 2 gambar semakin tidak mirip.

2.2.8 Kerangka Pemikiran

Kerangka pemikiran dalam penelitian ini adalah sebagai berikut:



Metode

Coefficient Diffeence dan Integer Haar Wavelet Transform (IHWT)

Implementasi dan Pengujian

Menggunakan Matlab

Pengujiannya dengan PNSR an SSIM

Hasil

1. **Dapat menunjukan hasil implementasi Algoritma *Coefisien Difference* dan *Integer Haar Wavelet Transform* (IHWT) untuk Media Digital pada Steganografi**
2. **Dapat mengukur tingkat kualitas citra dan perbedaan citra setelah dan sebelum disisipi oleh teks maupun citra lain (pesan).**