

BAB III

METODOLOGI PENELITIAN

3.1. Pengembangan Aplikasi

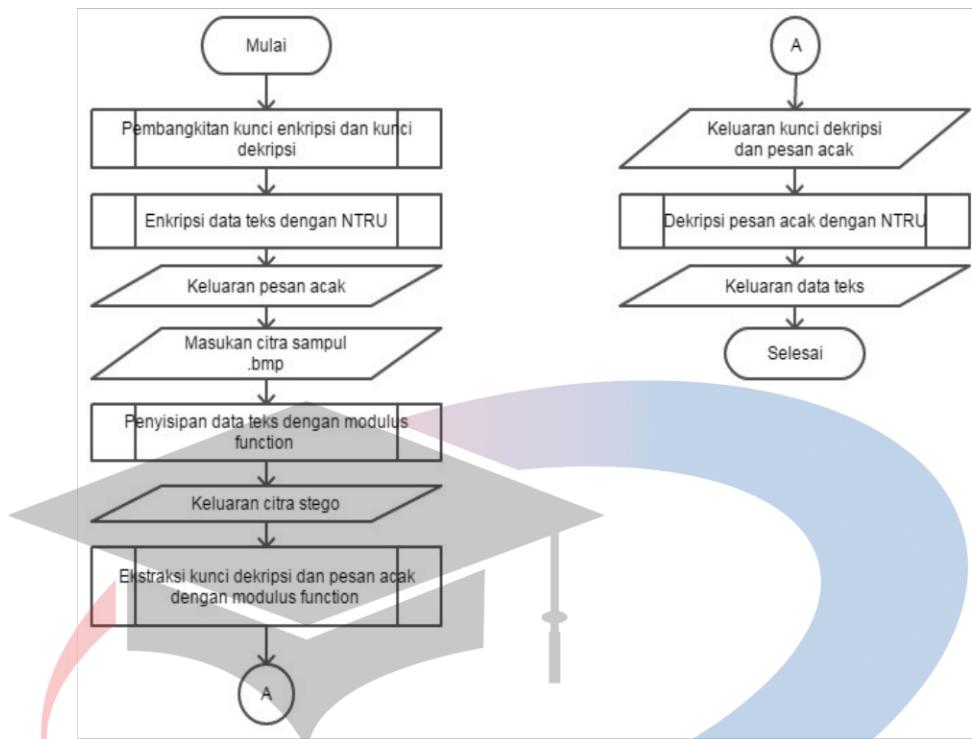
3.1.1. Analisis Sistem

Dalam membangun sebuah perancangan sistem, maka terlebih dahulu dilakukan analisis terhadap perangkat lunak yang akan dibangun. Proses analisis yang akan dilakukan mencakup analisis proses dan analisis kebutuhan. Analisis kebutuhan terdiri dari kebutuhan fungsional dan *non* fungsional. Kebutuhan fungsional menggunakan *use case* dan kebutuhan *non* fungsional menggunakan PIECES serta untuk analisis proses menggunakan *flowchart*.

3.1.1.1. Analisis Proses

Analisis proses digunakan untuk menjelaskan proses kerja pada perangkat lunak untuk menyelesaikan permasalahan yang ada, meliputi proses penyembunyian data teks dan proses ekstraksi data teks. Proses tersebut dapat dilihat dari *flowchart* di bawah ini:



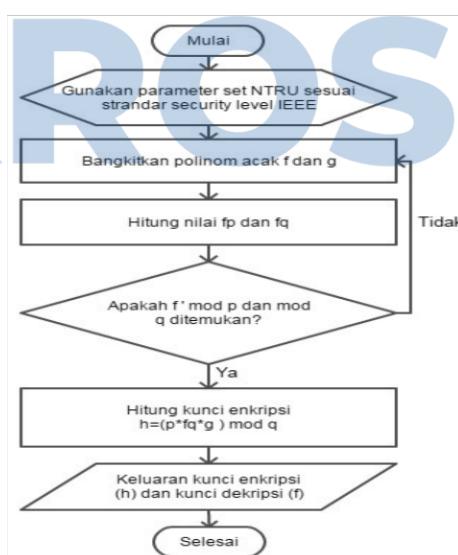


Gambar 3.1. *Flowchart* proses penyisipan dan enkripsi data teks

Berikut adalah langkah-langkah proses dari penyisipan dan ekstraksi data teks:

- Pembangkitan Kunci Enkripsi Dan Kunci Dekripsi.

Tahapan awal ialah membangkitkan kunci enkripsi dan kunci dekripsi, proses pembentukan kunci dapat dilihat dari *flowchart* di bawah ini:



Gambar 3.2. *Flowchart* pembangkitan kunci enkripsi dan kunci dekripsi

Pada proses ini, untuk membangkitkan kunci pengguna harus terlebih dahulu menentukan parameter yang digunakan *NTRU* yang terdapat pada tabel 2.1 Karena perhitungan polinomial terlalu besar dan luas maka kita misalkan $N = 7$, $p = 3$, $q = 32$, $df = 2$ dan polinomial acak dari $f = x - x^2 + x^3$ serta $g = -1 + x^2 - x^3 + x^4$. Sebelum membangkitkan kunci enkripsi dan kunci dekripsi perlu di bangkitkan polinomial fp dan fq dengan cara menghitung nilai $Q = A:B$, $R = A \bmod B$ dan $t = t1 - (Q*t2)$ dengan asumsi nilai $t1 = 0$ serta $t2 = 1$. Sehingga didapatkan hasil perhitungannya adalah sebagai berikut:

Iterasi pertama:

$$Q = x^7 - 1 : x^3 - x^2 + x = x^4 + x^3 - x - 1 \bmod 3 = x^4 + x^3 + 2x + 2,$$

$$R = x^7 - 1 \bmod x^3 - x^2 + x = x - 1 \bmod 3 = x + 2,$$

$$t1 = 0 \text{ dan } t2 = 1,$$

$$t = 0 - (x^4 + x^3 + 2x + 2 * 1) = x^4 + x^3 + 2x + 2$$

$$0 - (x^4 + x^3 + 2x + 2) = -x^4 - x^3 - 2x - 2$$

$$-x^4 - x^3 - 2x - 2 \bmod 3 = 2x^4 + 2x^3 + x + 1.$$

Iterasi kedua :

$$Q = x^3 - x^2 + x : x + 2 = x^2 + -3x + 7 \bmod 3 = x^2 + 1,$$

$$R = x^3 - x^2 + x \bmod 3 = -14 \bmod 3 = -2 \bmod 3 = 1$$

$$t1 = 1 \text{ dan } t2 = 2x^4 + 2x^3 + x + 1,$$

$$t = 1 - (x^2 + 1 * 2x^4 + 2x^3 + x + 1) = 2x^6 + 2x^5 + 2x^4 + 3x^3 + x^2 + x + 1,$$

$$1 - (2x^6 + 2x^5 + 2x^4 + 3x^3 + x^2 + x + 1) = -2x^6 - 2x^5 - 2x^4 - x^2 - x$$

$$-2x^6 - 2x^5 - 2x^4 - x^2 - x \bmod 3 = x^6 + x^5 + x^4 + 2x^2 + 2x.$$

Iterasi ketiga :

$$Q = x + 2 : 1 = x + 2 \bmod 3 = x + 2,$$

$$R = 0 \bmod 3 = 0,$$

$$t1 = 2x^4 + 2x^3 + x + 1 \text{ dan } t2 = x^6 + x^5 + x^4 + 2x^2 + 2x,$$

$$t = 2x^4 + 2x^3 + x + 1 - (x^2 + 1 * x^6 + x^5 + x^4 + 2x^2 + 2x)$$

$$= x^7 + 3x^6 + 3x^5 + 2x^4 + 2x^3 + 6x^2 + 4x \bmod 3 = x^7 + 2x^4 + 2x^3 + x,$$

$$= x^7 + 2x^4 + 2x^3 + x - (x^7 + 2x^4 + 2x^3 + x) = x^7 - 1.$$

Berikut tabel hasil dari pencarian polinomial dari fp dengan nilai dari perhitungan diatas:

Tabel 3. 1. Tabel hasil pencarian polinomial fp dari parameter NTRU dengan nilai $N = 7$, $p = 3$, $q = 32$ dan $df = 2$

k	A	B	Q	R	t1	t2	t
init	$x^7 - 1$	$x^3 - x^2 + x$	-	-	0	1	-
1	$x^7 - 1$	$x^3 - x^2 + x$	$x^4 + x^3 + 2x + 2$	$x + 2$	0	1	$2x^4 + 2x^3 + x + 1$
2	$x^3 - x^2 + x$	$x + 2$	$x^2 + 1$	1	1	$2x^4 + 2x^3 + x + 1$	$x^6 + x^5 + x^4 + 2x^2 + 2x$
3	$x + 2$	1	$x + 2$	0	$2x^4 + 2x^3 + x + 1$	$x^6 + x^5 + x^4 + 2x^2 + 2x$	$x^7 - 1$
4	1	0	-	-	$x^6 + x^5 + x^4 + 2x^2 + 2x$	$x^7 - 1$	-

Untuk nilai f_q , proses perhitungan nilai dengan parameter NTRU dengan nilai $N = 7$, $p = 3$, $q = 32$ dan $df = 2$ adalah sama seperti pencarian f_p hanya saja perbedaannya pada modulusnya, pada f_p nilai modulus dari p sedangkan pada f_q dari q . Berikut tabel hasil perhitungannya :

Tabel 3. 2. Tabel hasil pencarian polinomial f_q dari parameter NTRU dengan nilai $N = 7$, $p = 3$, $q = 32$ dan $df = 2$

k	A	B	Q	R	t1	t2	T
init	$x^7 - 1$	$x^3 - x^2 + x$	-	-	0	1	-
1	$x^7 - 1$	$x^3 - x^2 + x$	$x^4 + x^3 + 31x + 31$	$x + 31$	0	1	$31x^4 + 31x^3 + x + 1$
2	$x^3 - x^2 + x$	$x + 31$	$x^2 + 1$	1	1	$31x^4 + 31x^3 + x + 1$	$x^6 + x^5 + x^4 + 31x^2 + 31x$

3	$x+3$	1	$x+31$	0	$\frac{31x^4+31}{x^3+x+1}$	$x^6 + x^5 + x^4 + 31x^2 + 31x$	$x^7 - 1$
4	1	0	-	-	$x^6 + x^5 + x^4 + 31x^2 + 31x$	$x^7 - 1$	-

Berdasarkan tabel 3.1 diatas maka didapatkan polinomial $fp = 2x + 2x^2 + x^4 + x^5 + x^6$ dan pada tabel 3.2 didapatkan polinomial $fq = 31x + 31x^2 + x^4 + x^5 + x^6$. Sehingga dapat dihitung kunci enkripsi sebagai berikut:

$$h = (p * fq * g) \bmod q$$

$$h = (3 * (31x + 31x^2 + x^4 + x^5 + x^6)) * (-1 + x^2 - x^3 + x^4) \bmod 32$$

$$= ((93x + 93x^2 + 3x^4 + 3x^5 + 3x^6)) * (-1 + x^2 - x^3 + x^4) \bmod 32$$

$= -93x - 93x^2 + 93x^3 - 3x^4 - 3x^5 + 93x^6 + 3x^8 + 3x^{10}$, karena hasil perkalian polinomial terdapat $3x^8$ dan $3x^{10}$ (melebihi nilai $N - 1$) sehingga perlu di lakukan *truncated* terhadap hasil perkalian menjadi:

$$3x^8 = (3x) * (x^7) = 3x$$

$$3x^{10} = (3x^3) * (x^7) = 3x^3, \text{ sehingga hasil dari perkalian menjadi:}$$

$= -93x - 93x^2 + 93x^3 - 3x^4 - 3x^5 + 93x^6 + 3x + 3x^3$, lalu hitung pangkat yang sama pada polinomial sehingga menghasilkan:

$$= (-90x - 93x^2 + 96x^3 - 3x^4 - 3x^5 + 93x^6 + 3x^8 + 3x^{10}) \bmod 32$$

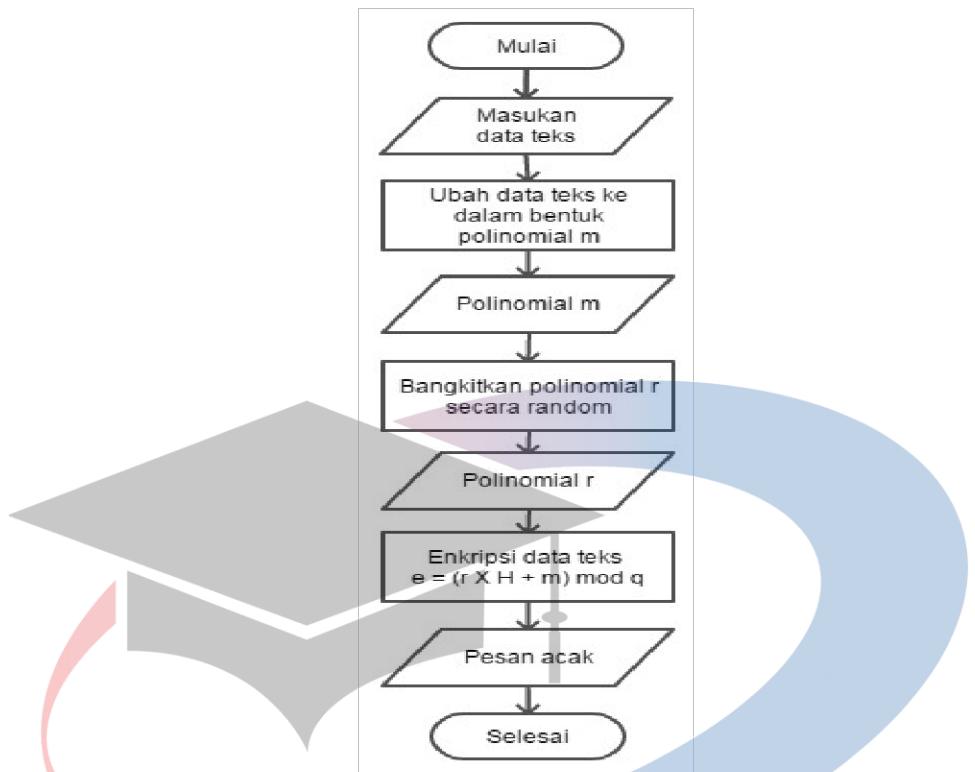
$$= (-26x - 29x^2 + 93x^3 + 29x^4 + 29x^5 + 29x^6) \bmod 32$$

$$h = 6x + 3x^2 + 29x^4 + 29x^5 + 29x^6$$

Sehingga diperoleh kunci enkripsi $h = 6x + 3x^2 + 29x^4 + 29x^5 + 29x^6$ dan kunci dekripsi $f = x - x^2 + x^3$.

b. Enkripsi Data Teks Dengan NTRU

Setelah melakukan proses pembangkitan kunci, langkah selanjutnya adalah melakukan proses enkripsi dengan perincian proses yang dijelaskan pada gambar *flowchart* di bawah ini:



Gambar 3.3. Flowchart enkripsi data teks dengan NTRU

Dalam proses ini dilakukan perhitungan enkripsi data teks dengan menggunakan rumus enkripsi dengan *NTRU*. Sebelum melakukan proses perhitungan enkripsi data teks, kita perlu mengubah pesan yang dimasukan menjadi polinomial m . Misalkan diketahui data teks (m) = a dan polinomial acak $r = 1 + x - x^2$, maka perhitungan dari proses mengubah pesan yang dimasukkan menjadi polinomial m adalah sebagai berikut sebagai berikut:

Representasikan pesan m sebagai sebuah polinomial dengan koefisiennya berada diantara $[-p/2, p/2]$. Jika $p = 3$, maka koefisien polinomial adalah $[-1, 0, 1]$.

- Pesan string “awal” diubah dalam bentuk *polynomial* Nilai ASCII dari “a” adalah 97.

$$97 : 3 = 32 \text{ sisa bagi } 1$$

$$32 : 3 = 10 \text{ sisa bagi } 2$$

$$10 : 3 = 3 \text{ sisa bagi } 1$$

$$3 : 3 = 1 \text{ sisa bagi } 0$$

- Maka array dari $m = [1, 2, 1, 0, 1]$, karena $N = 7$ maka nilai $m = [1, 2, 1, 0, 1, 0, 0]$, koefisien *polynomial* m harus diantara $-1, 0, 1$, maka nilai m

dikurangi 1 menjadi $m = [0, 1, 0, -1, 0, -1, -1]$, sehingga polinomial $m = x - x^3 - x^5 - x^6$

- Setelah polinomial dari m telah ditemukan maka lakukan proses enkripsi dengan persamaan $e = r * h + m \pmod{q}$. Proses perhitungan dari polinomial pesan acak (e) adalah sebagai berikut:

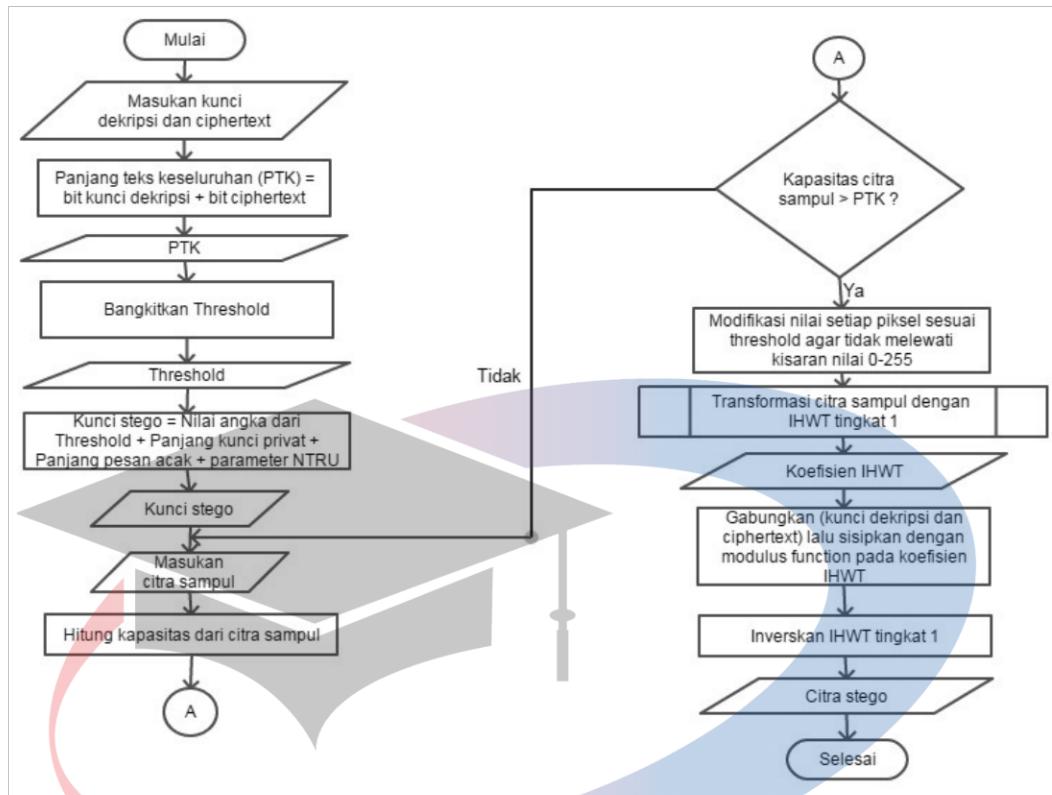
$$\begin{aligned} e &= ((1 + x - x^2) * (6x + 3x^2 + 29x^4 + 29x^5 + 29x^6) + (x - x^3 - x^5 - x^6)) \pmod{32} \\ &= 6x + 9x^2 - 3x^3 + 26x^4 + 58x^5 + 29x^6 - 29x^8, \text{ lakukan } truncated \text{ terhadap} \\ &\quad - 29x^8 \text{ menjadi: } -29x^8 = (-29x) * (x^7) = -29x, \text{ lalu} \\ &= 6x + 9x^2 - 3x^3 + 26x^4 + 58x^5 + 29x^6 - 29x \\ &= -23x + 9x^2 - 3x^3 + 26x^4 + 58x^5 + 29x^6 \pmod{32} \\ &= 9x + 9x^2 + 29x^3 + 26x^4 + 26x^5 + 29x^6 \\ &= (9x + 9x^2 + 29x^3 + 26x^4 + 26x^5 + 29x^6) + (x - x^3 - x^5 - x^6) \\ e &= 10x + 9x^2 + 28x^3 + 26x^4 + 25x^5 + 28x^6 \end{aligned}$$

Pada string “wal” adalah memiliki langkah yang sama seperti proses enkripsi pada string “a”.

c. Penyisipan Data Teks Dengan Modulus Function

Setelah melakukan proses enkripsi, langkah selanjutnya adalah proses penyisipan. Proses penyisipan dapat dilihat dari *flowchart* di bawah ini:





Gambar 3.4. Flowchart penyisipan data teks dengan *modulus function*

- Sebelum melakukan proses penyisipan data teks dengan *modulus function*, terlebih dahulu kita memasukkan kunci dekripsi dan pesan acak
- Lalu hitung panjang bit teks keseluruhan dengan persamaan : $PTK = \text{bit kunci dekripsi} + \text{bit sisip acak}$.
- $PTK = 13 + 14 = 27 \text{ bit}$
- Kemudian bangkitkan *threshold* (T) dengan cara menghitung panjang bitstream dari pesan dan dimodulokan 3 serta ditambah 1, berikut perhitungannya:

$$T = (\text{Panjang-bitstream \% } 3) + 1 = (32 \bmod 3) + 1 = 3$$

- Lalu membangkitkan kunci stego dengan melakukan penggabungan pada bit parameter yang diketahui sebagai berikut :

$$T = 2 \text{ bit};$$

$$N = 11 \text{ bit};$$

$q = 12$ bit;

$df = 8$ bit;

Jumlah karakter kunci dekripsi = 13 bit;

Jumlah karakter pesan acak = 14 bit;

$maxMsgLenBytes = 8$ bit;

$Padding = 2$ bit.

Kunci stego = 2 11 12 8 13 14 8 2

- Setelah kunci stego didapatkan, maka hitung biner dari *ciphertext*, sebagai contoh kita ambil “8 10”, untuk proses penyisipan terlebih dahulu dilakukan konversi data teks ke dalam ASCII dan kemudian di representasikan dalam biner 8 bit. Berikut proses perhitungannya:

ASCII dari 8 : 56, biner 8 bit : 00111000

ASCII dari : 32, biner 8 bit : 00100000

ASCII dari 1 : 49, biner 8 bit : 00110001

ASCII dari 0 : 48, biner 8 bit : 00110000

Sehingga *bitstream* dari pesan adalah sebagai berikut
“00111000001000000011000100110000”.

- Masukkan sebuah citra sampul RGB ukuran 4X4 dengan nilai piksel citra yang diketahui pada tabel berikut:

Tabel 3.3. Nilai piksel pada citra sampul ukuran 4X4

7	165	74	221	19	141	86	70	21	184	12	50
251	81	28	11	100	148	85	251	200	75	123	173
123	91	22	151	7	75	123	173	100	148	85	251
72	287	241	30	246	165	8	221	19	141	86	70
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

- Kapasitas penampungan untuk citra RGB 4X4 dengan nilai $T = 3$ adalah 54 bit, karena $T = 3$ maka padding (penambahan) dilakukan terhadap bitstream pesan dengan panjang pesan = 32, 32 modulo 3 adalah 2, 3 - 2 adalah 1. Bit '0' ditambahkan sebanyak 1 pada ujung *bitstream* pesan sehingga *bitstream* pesan menjadi = 001110000010000000110001001100000.
- Untuk mencegah nilai piksel keluar dari kisaran 0-255, maka dilakukan modifikasi pada piksel citra dengan faktor bobot = 2 dan $T = 3$ seperti berikut:

$$\text{Batas bawah} = 2 * 3 = 6$$

$$\text{Batas atas} = 255 - 6 = 249$$

- Saluran merah baris-1, kolom-0 = 251, karena $251 > 249$, maka saluran merah baris-1, kolom-0 = 249. Saluran merah baris-3, kolom-1 = 287, karena $287 > 249$, maka saluran merah baris-3, kolom-1 = 249. Saluran hijau baris-1, kolom-3 = 251, $251 > 249$, maka saluran hijau baris-1, kolom-3 = 249. Saluran biru baris-2, kolom-3 = 251, $251 > 249$, maka saluran biru baris-2, kolom-3 = 249. Sehingga nilai citra setelah modifikasi nilai piksel adalah sebagai berikut:

Tabel 3.4. Nilai piksel citra pada setiap saluran setelah di modifikasi nilai piksel

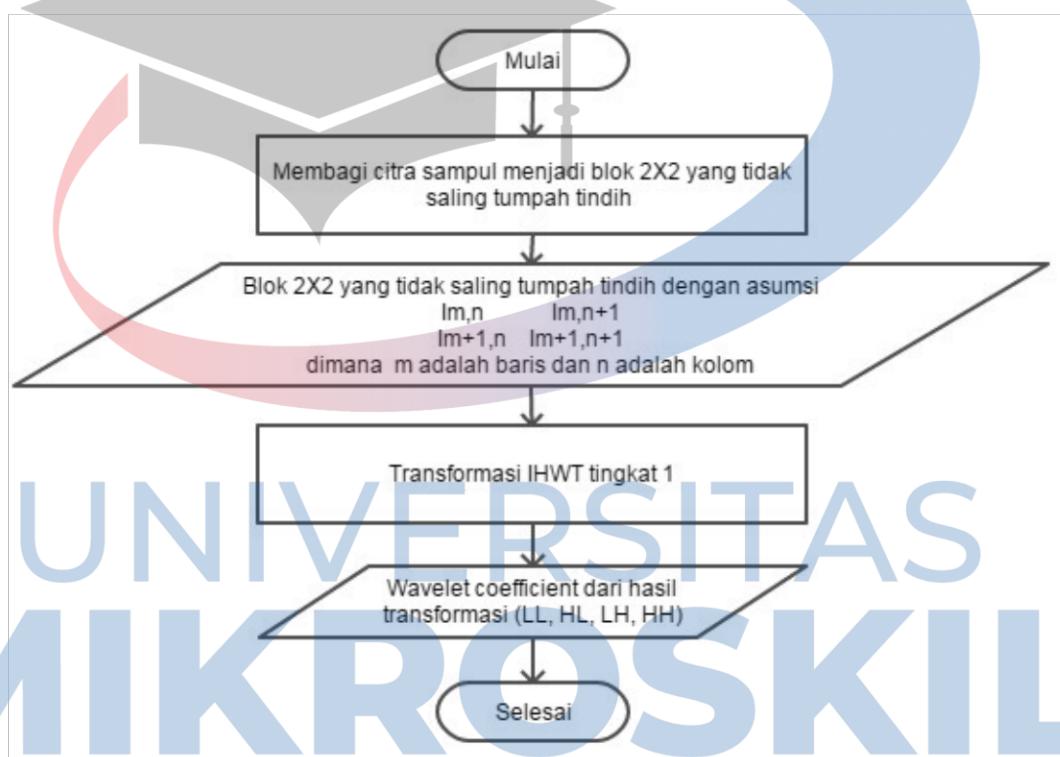
7	165	74	221	19	141	86	70	21	184	12	50
249	81	28	11	100	148	85	249	200	75	123	173
123	91	22	151	7	75	123	73	100	148	85	249
72	249	241	30	246	165	8	221	19	141	86	70
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

Setelah nilai piksel citra di modifikasi kemudian lakukan proses transformasi tingkat 1 menggunakan *IHWHT* pada setiap saluran. Hasil transformasi dapat dilihat pada tabel berikut:

Tabel 3.5. Nilai piksel citra pada setiap saluran setelah di modifikasi nilai piksel

7	165	74	221
249	81	28	11
123	91	22	151
72	249	241	30
Saluran merah (R)			

Proses transformasi dilakukan sebanyak 1 kali transformasi dengan menggunakan *IHWWT*. Berikut ini adalah *flowchart* dari transformasi *IHWWT* tingkat



Gambar 3.5. Proses Transformasi IHWT tingkat 1

Proses transformasi dimulai dengan membagi citra menjadi blok 2X2 yang tidak saling tumpang tindih, dimana blok tersebut berisi sebuah piksel citra pada posisi baris dan kolom sehingga didapatkan *subbands wavelet* sebagai berikut:

Tabel 3.6. Nilai piksel pada citra persubband

LL=	7	74	LH=	165	221
	123	22		91	151
HL=	249	28	HH=	81	11
	72	241		249	30

- Lalu, *IHWWT* diterapkan menggunakan operasi pembulatan ke bawah pada setiap blok untuk mendapatkan *wavelet coefficient* pada *subbands* (LL, HL, LH, HH), berikut perhitungannya :

Iterasi pertama :

$$LL = \left\lfloor \frac{\left\lfloor \frac{7+165}{2} \right\rfloor + \left\lfloor \frac{249+81}{2} \right\rfloor}{2} \right\rfloor = 125$$

$$LH = \left\lfloor \left\lfloor \frac{7+165}{2} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{249+81}{2} \right\rfloor \right\rfloor = -79$$

$$HL = \left\lfloor \frac{7 - 165 + 249 - 81}{2} \right\rfloor = 5$$

$$HH = 7 - 165 - 249 + 81 = -326$$

Iterasi kedua :

$$LL = \left\lfloor \frac{\left\lfloor \frac{74+221}{2} \right\rfloor + \left\lfloor \frac{28+11}{2} \right\rfloor}{2} \right\rfloor = 83$$

$$LH = \left\lfloor \left\lfloor \frac{74+221}{2} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{28+11}{2} \right\rfloor \right\rfloor = 128$$

$$HL = \left\lfloor \frac{74 - 221 + 28 - 11}{2} \right\rfloor = -65$$

$$HH = 74 - 221 - 28 + 11 = -164$$

Iterasi ketiga :

$$LL = \left\lfloor \frac{\left\lfloor \frac{123+91}{2} \right\rfloor + \left\lfloor \frac{72+249}{2} \right\rfloor}{2} \right\rfloor = 133$$

$$LH = \left\lfloor \left\lfloor \frac{123+91}{2} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{72+249}{2} \right\rfloor \right\rfloor = -53$$

$$HL = \left\lfloor \frac{123 - 91 + 72 - 249}{2} \right\rfloor = -73$$

$$HH = 123 - 91 - 72 + 249 = 209$$

Iterasi keempat :

$$LL = \left\lfloor \frac{\left\lceil \frac{22+151}{2} \right\rceil + \left\lceil \frac{241+30}{2} \right\rceil}{2} \right\rfloor = 110$$

$$LH = \left\lfloor \left\lceil \frac{22+151}{2} \right\rceil \right\rfloor - \left\lfloor \left\lceil \frac{241+30}{2} \right\rceil \right\rfloor = -49$$

$$HL = \left\lfloor \frac{22 - 151 + 241 - 30}{2} \right\rfloor = 41$$

$$HH = 22 - 151 - 241 + 30 = -340$$

Untuk saluran hijau dan biru sama prosesnya, sehingga hasil dari transformasi IHWT tingkat 1 pada *subbands wavelet* adalah seperti tabel berikut:

Tabel 3.7. Nilai piksel citra sampul setelah transformasi

125	83	-79	128	102	122	-44	-89	119	89	-35	-117
133	110	-53	-49	123	131	-164	34	102	122	44	89
5	-65	-326	-164	-85	-74	-74	180	-19	-44	-288	12
-73	41	209	-340	6	-132	-149	163	-85	-74	74	-180
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

- Setelah nilai piksel di transformasikan maka lakukan perhitungan penyisipan pada saluran merah pada setiap *subbands LH*, *HL*, *HH* seperti berikut:

Penyisipan pada *subband LH*;

$$p0,2 = -79 \text{ dan } p0,3 = 128$$

$t_k = 1$ karena desimal bit yang akan disisipkan = "001"

$$2^T = 2^3 = 8$$

$$r_k = ((-79) + 128) \bmod 8 = 1$$

$$m = 1 - 1 = 0; m' = 8 - 0 = 8$$

$r_k \leq t_k$ dan $m \leq 2^T$ & $p0,2 < p0,3$. Maka nilai piksel $p0,2' = -79 + 0 = -79$; $p0,3' = 128 + 0 = 128$.

$p_{1,2} = -53$ dan $p_{1,3} = -49$

$t_k = 6$ karena desimal bit yang akan disisipkan = "110"

$$2^T = 2^3 = 8$$

$$r_k = ((-53) + (-49)) \bmod 8 = 2$$

$$m = 2 - 6 = 4 \text{ dan } m' = 8 - 4 = 4$$

$r_k \leq t_k$ dan $m \leq 2^T$ & $p_{1,2} < p_{1,3}$. Maka nilai piksel $p_{1,2}' = (-53) + 2 = -51$; $p_{1,3}' = (-49) + 2 = -47$.

Penyisipan pada *subband HL*;

$$p_{2,0} = 5 \text{ dan } p_{2,1} = -65$$

$t_k = 0$ karena desimal bit yang akan disisipkan = "000"

$$2^T = 2^3 = 8;$$

$$r_k = ((5) + (-65)) \bmod 8 = 4$$

$$m = 4 - 0 = 4 \text{ dan } m' = 8 - 4 = 4$$

$r_k > t_k$ dan $m \leq 2^T$ & $p_{2,0} >= p_{2,1}$, Maka nilai piksel $p_{2,0}' = 5 - 2 = 3$; $p_{2,1}' = (-65) - 2 = -67$

$$p_{3,0} = -73 \text{ dan } p_{3,1} = 41$$

$t_k = 2$ karena desimal bit yang akan disisipkan = "010"

$$2^T = 2^3 = 8$$

$$r_k = ((-73) + (41)) \bmod 8 = 0$$

$$m = 0 - 2 = 2 \text{ dan } m' = 8 - 2 = 6$$

$r_k \leq t_k$ dan $m \leq 2^T$ & $p_{3,0} < p_{3,1}$, Maka nilai piksel $p_{3,0}' = (-73) + 1 = -72$; $p_{3,1}' = 41 + 1 = 42$.

Penyisipan pada *subband* HH;

$$p_{2,2} = -326 \text{ dan } p_{2,3} = -164$$

$t_k = 0$ karena desimal bit yang akan disisipkan = “000”

$$2^T = 2^3 = 8;$$

$$r_k = ((-326) + (-164)) \bmod 8 = 6$$

$$m = 6 - 0 = 6 \text{ dan } m' = 8 - 6 = 2$$

$r_k > t_k$ dan $m \leq 2^T$ & $p_{2,2} < p_{2,3}$. Maka nilai piksel $p_{2,2}' = (-326) - 3 = -329$; $p_{2,3}' = (-164) - 3 = -167$.

$$p_{3,2} = 209 \text{ dan } p_{3,3} = -340$$

$t_k = 0$ karena desimal dari bit yang akan disisipkan = “000”

$$2^T = 2^3 = 8;$$

$$r_k = (209 + (-340)) \bmod 8 = 5$$

$$m = 5 - 0 = 5 \text{ dan } m' = 8 - 5 = 3$$

$r_k > t_k$ dan $m \leq 2^T$ & $p_{3,2} \geq p_{3,3}$. Maka nilai piksel $p_{3,2}' = 209 - 3 = 206$; $p_{3,3}' = (-340) - 2 = -342$.

Perhitungan penyisipan pada saluran hijau pada setiap *subbands* LH, HL, HH seperti berikut:

Penyisipan pada *subband* LH;

$$p_{0,2} = -44 \text{ dan } p_{0,3} = -89$$

$t_k = 6$ karena desimal bit yang akan disisip = “110”

$$2^T = 2^3 = 8;$$

$$r_k = ((-44) + (-89)) \bmod 8 = 3$$

$$m = 3 - 6 = 3 \text{ dan } m' = 8 - 3 = 5$$

$r_k \leq t_k$ dan $m \leq 2^T$ & $p_{0,2} \geq p_{0,3}$. Maka nilai piksel $p_{0,2}' = (-44) + 1 = -43$; $p_{0,3}' = (-89) - 2 = -87$

$p_{1,2} = -164$ dan $p_{1,3} = 34$

$t_k = 1$ karena bit yang akan disisipkan = "001"

$2^T = 2^3 = 8$;

$r_k = ((-164) + 34) \bmod 8 = 6$

$m = 6 - 1 = 5$ dan $m' = 8 - 5 = 3$

$r_k > t_k$ & $m \leq 2^T$ & $p_{1,2} < p_{1,3}$. Maka nilai piksel $p_{1,2}' = (-164) - 2 = -166$; $p_{1,3}' = 34 - 3 = 31$

Penyisipan pada subband HL;

$p_{2,0} = -85$ dan $p_{2,1} = -74$

$t_k = 1$ karena desimal bit yang akan dsisisip = "001"

$2^T = 2^3 = 8$

$r_k = ((-85) + (-74)) \bmod 8 = 1$

$m = 1 - 1 = 0$ dan $m' = 8 - 0 = 8$

$r_k \leq t_k$ & $m \leq 2^T$ & $p_{2,0} < p_{2,1}$. Maka nilai piksel $p_{2,0}' = (-85) + 0 = -85$; $p_{2,1}' = (-74) + 0 = -74$.

$p_{3,0} = 6$ dan $p_{3,1} = -132$

$t_k = 4$ karena desimal bit yang akan disisip = "100"

$2^T = 2^3 = 8$

$r_k = (6 + (-132)) \bmod 8 = 2$

$m = 2 - 4 = 2$ dan $m' = 8 - 2 = 6$

$r_k \leq t_k$ & $m \leq 2^T$ & $p_{3,0} \geq p_{3,1}$. Maka nilai piksel $p_{3,0}' = 6 + 1 = 7$; $p_{3,1}' (-132) + 1 = -131$.

Penyisipan pada subband HH;

$p_{2,2} = -74$ dan $p_{2,3} = 180$

$t_k = 0$ karena desimal bit yang akan disisip = “000”

$$2^T = 2^3 = 8;$$

$$r_k = ((-74) + 180) \bmod 8 = 2$$

$$m = 2 - 0 = 2 \text{ dan } m' = 8 - 2 = 6$$

$r_k > t_k$ dan $m \leq 2^T$ & $p_{2,2} < p_{2,3}$. Maka nilai piksel $p_{2,2} = (-74) - 1 = -75$; $p_{2,3} = 180 - 1 = 179$.

Hasil dari bitstream data teks yang disisipkan dapat dilihat pada tabel berikut ini:

Tabel 3.8. Nilai piksel citra sampul setelah proses penyisipan

125	83	-79	128	102	122	-43	-87	119	89	-35	-117
133	110	-51	-47	123	131	-166	31	102	122	44	89
3	-67	-329	-167	-85	-74	-75	179	-19	-44	-288	12
-72	42	206	-342	7	-131	-149	163	-85	-74	74	-180
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

- Setelah semua bitstream pesan disisipkan, dilakukan IHWT *Invers* tingkat 1 pada nilai piksel saluran seperti berikut:

Iterasi pertama :

$$LL' = \left\lfloor 125 + \left\lfloor \frac{-79+1}{2} \right\rfloor + \left\lfloor \frac{3 + \left\lfloor \frac{-329+1}{2} \right\rfloor + 1}{2} \right\rfloor \right\rfloor = 6$$

$$LH' = 6 - \left\lfloor 3 + \left\lfloor \frac{-329+1}{2} \right\rfloor \right\rfloor = 167$$

$$HL' = 125 + \left\lfloor \frac{-79+1}{2} \right\rfloor - (-79) + \left\lfloor \frac{3 + \left\lfloor \frac{-329+1}{2} \right\rfloor - (-329) + 1}{2} \right\rfloor = 249$$

$$HH' = 249 - \left\lfloor 3 + \left\lfloor \frac{-329+1}{2} \right\rfloor - (-329) \right\rfloor = 81$$

Iterasi kedua :

$$LL' = \left\lfloor 83 + \left\lfloor \frac{128+1}{2} \right\rfloor + \left\lfloor \frac{-67 + \left\lfloor \frac{-167+1}{2} \right\rfloor + 1}{2} \right\rfloor \right\rfloor = 72$$

$$LH' = 72 - \left\lfloor -67 + \left\lfloor \frac{-167+1}{2} \right\rfloor \right\rfloor = 222$$

$$HL' = 83 + \left\lfloor \frac{128+1}{2} \right\rfloor - (128) + \left\lfloor \frac{-67 + \left\lfloor \frac{-167+1}{2} \right\rfloor - (-167) + 1}{2} \right\rfloor = 28$$

$$HH' = 28 - \left\lfloor -67 + \left\lfloor \frac{-167+1}{2} \right\rfloor - (-167) \right\rfloor = 11$$

Iterasi ketiga :

The diagram illustrates the iterative process for calculating pixel values. It shows four equations arranged in a diamond shape, each with a shaded background corresponding to its row:

- Row 1 (Red):** $LL' = \left\lfloor 133 + \left\lfloor \frac{-51+1}{2} \right\rfloor + \left\lfloor \frac{-72 + \left\lfloor \frac{206+1}{2} \right\rfloor + 1}{2} \right\rfloor \right\rfloor = 124$
- Row 2 (Green):** $LH' = 124 - \left\lfloor -72 + \left\lfloor \frac{206+1}{2} \right\rfloor \right\rfloor = 93$
- Row 3 (Blue):** $HL' = 133 + \left\lfloor \frac{-51+1}{2} \right\rfloor - (-51) + \left\lfloor \frac{-72 + \left\lfloor \frac{206+1}{2} \right\rfloor - (206) + 1}{2} \right\rfloor = 72$
- Row 4 (Yellow):** $HH' = 72 - \left\lfloor -72 + \left\lfloor \frac{206+1}{2} \right\rfloor - (206) \right\rfloor = 247$

Iterasi keempat :

The diagram illustrates the iterative process for calculating pixel values. It shows four equations arranged in a diamond shape, each with a shaded background corresponding to its row:

- Row 1 (Red):** $LL' = \left\lfloor 110 + \left\lfloor \frac{-47+1}{2} \right\rfloor + \left\lfloor \frac{42 + \left\lfloor \frac{-342+1}{2} \right\rfloor + 1}{2} \right\rfloor \right\rfloor = 23$
- Row 2 (Green):** $LH' = 23 - \left\lfloor 42 + \left\lfloor \frac{-342+1}{2} \right\rfloor \right\rfloor = 152$
- Row 3 (Blue):** $HL' = 110 + \left\lfloor \frac{-47+1}{2} \right\rfloor - (-47) + \left\lfloor \frac{42 + \left\lfloor \frac{-342+1}{2} \right\rfloor - (-342) + 1}{2} \right\rfloor = 241$
- Row 4 (Yellow):** $HH' = 241 - \left\lfloor 42 + \left\lfloor \frac{-342+1}{2} \right\rfloor - (-342) \right\rfloor = 28$

Begitu juga pada proses perhitungan di saluran hijau dan biru sehingga

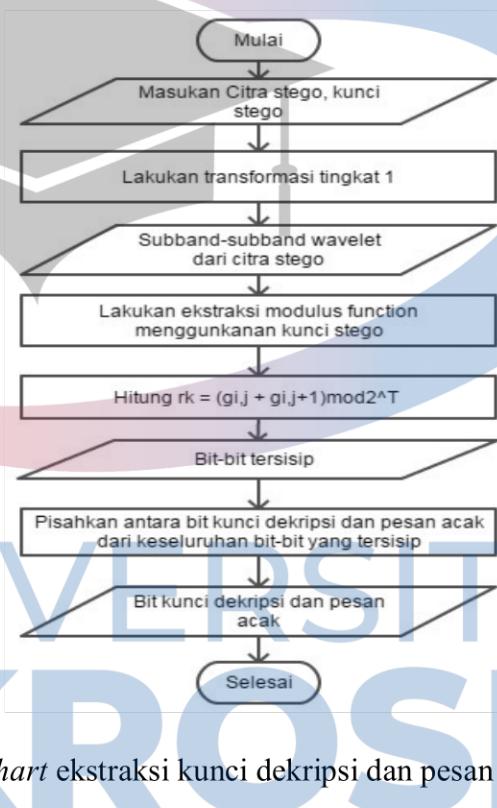
hasil akhir dari IHWT *Invers* tingkat 1 pada nilai piksel di setiap saluran adalah sebagai berikut :

Tabel 3.9. Nilai piksel citra sampul setelah penyisipan dan IHWT *invers*

6	167	72	222	20	142	87	71	21	184	12	50
249	81	28	11	101	148	85	248	200	75	123	173
124	93	23	152	7	74	123	172	100	148	85	249
72	247	241	28	247	165	10	222	19	141	86	70
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

d. Proses Ekstraksi Kunci Dekripsi Dan Pesan Acak Dengan Modulus Function

Pada proses ekstraksi dimulai dengan mentrasformasikan citra stego supaya menghasilkan *subbands wavelet*, setelah itu terapkan *IHWHT* untuk mendapatkan *wavelet coefficient* pada *subbands*. Lakukan ekstraksi menggunakan kunci stego pada seluruh bit-bit tersisip dan hitung $r_k = (g_{ij} + g_{ij+1}) \bmod 2^T$ untuk mendapatkan nilai desimal dari bit-bit tersisip. Proses ekstraksi dapat dilihat dari *flowchart* di bawah ini:



Gambar 3. 6. Flowchart ekstraksi kunci dekripsi dan pesan acak dengan *modulus function*

- Pada proses ekstraksi data teks, dilakukan transformasi sama seperti proses transformasi pada penyisipan dengan menggunakan *IHWHT* pada nilai piksel dari citra stego. Hasil dari transformasi *IHWHT* tingkat 1 pada *subbands wavelet* dari citra stego adalah seperti tabel berikut:

Tabel 3. 10. Nilai piksel citra stego setelah proses transformasi

125	83	-79	128	102	122	-43	-87	119	89	-35	-117
133	110	-51	-47	123	131	-166	31	102	122	44	89
3	-67	-329	-167	-85	-74	-75	179	-19	-44	-288	12
-72	42	206	-342	7	-131	-149	163	-85	-74	74	-180
Saluran merah (R)				Saluran Hijau (G)				Saluran Biru (B)			

- Setelah nilai piksel dari citra stego di transformasikan maka lakukan perhitungan ekstraksi pada saluran merah pada setiap *subbands* LH, HL, HH seperti berikut:

Ekstraksi pada *subband* LH;

$$p_{0,2} = -79 \text{ dan } p_{0,3} = 128$$

$$2^T = 2^3 = 8$$

$$r_k = ((-79) + 128) \bmod 8 = 1 \rightarrow 001$$

$$p_{1,2} = -51 \text{ dan } p_{1,3} = -47$$

$$2^T = 2^3 = 8$$

$$r_k = ((-51) + (-47)) \bmod 8 = 6 \rightarrow 110$$

Ekstraksi pada *subband* HL;

$$p_{2,0} = 3 \text{ dan } p_{2,1} = -67$$

$$2^T = 2^3 = 8;$$

$$r_k = ((3) + (-67)) \bmod 8 = 0 \rightarrow 000$$

$$p_{3,0} = -72 \text{ dan } p_{3,1} = 42$$

$$2^T = 2^3 = 8$$

$$r_k = ((-72) + (42)) \bmod 8 = 2 \rightarrow 010$$

Ekstraksi pada *subband* HH;

$$p_{2,2} = -329 \text{ dan } p_{2,3} = -167$$

$$2^T = 2^3 = 8;$$

$$r_k = ((-329) + (-167)) \bmod 8 = 0 \rightarrow 000$$

$$p_{3,2} = 206 \text{ dan } p_{3,3} = -342$$

$$2^T = 2^3 = 8;$$

$$r_k = (206 + (-342)) \bmod 8 = 0 \rightarrow 000$$

Perhitungan ekstraksi pada saluran hijau pada setiap *subbands* LH, HL, HH seperti berikut:

Ekstraksi pada *subband* LH;

$$p_{0,2} = -43 \text{ dan } p_{0,3} = -87$$

$$2^T = 2^3 = 8;$$

$$r_k = ((-43) + (-87)) \bmod 8 = 6 \rightarrow 110$$

$$p_{1,2} = -166 \text{ dan } p_{1,3} = 31$$

$$2^T = 2^3 = 8;$$

$$r_k = ((-166) + 31) \bmod 8 = 1 \rightarrow 001$$

Ekstraksi pada *subband* HL;

$$p_{2,0} = -85 \text{ dan } p_{2,1} = -74$$

$$2^T = 2^3 = 8$$

$$r_k = ((-85) + (-74)) \bmod 8 = 1 \rightarrow 001$$

$$p_{3,0} = 7 \text{ dan } p_{3,1} = -131$$

$$2^T = 2^3 = 8$$

$$r_k = (7 + (-131)) \bmod 8 = 4 \rightarrow 100$$

Ekstraksi pada *subband* HH;

$$p_{2,2} = -75 \text{ dan } p_{2,3} = 179$$

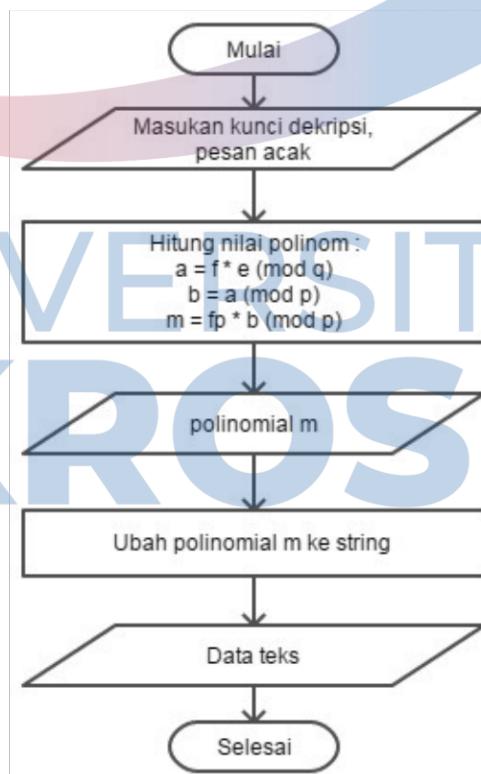
$$2^T = 2^3 = 8;$$

$$r_k = ((-75) + 179) \bmod 8 = 0 \rightarrow 000$$

Hasil ekstraksi dari nilai piksel citra stego menghasilkan *bitstream* = 001110000010000000110001001100000 dimana ini adalah sama dengan *bitstream* dari data teks yang disisip.

e. Proses Dekripsi Pesan Acak Dengan NTRU

Pada proses dekripsi, pesan acak tersebut akan dienkripsi dengan mencari nilai polinomial $a = f * e \pmod{q}$, $b = a \pmod{p}$ dan $c = fp * b \pmod{q}$. Polinomial c merupakan hasil dekripsi yaitu data teks. Proses dekripsi dapat dilihat dari *flowchart* di bawah ini:



Gambar 3.7. *Flowchart* dekripsi pesan acak dengan NTRU

Setelah melakukan proses enkripsi, langkah selanjutnya adalah mendekripsi pesan acak menggunakan kunci dekripsi. Proses dekripsi adalah sebagai berikut:

- Langkah awal ialah memasukkan kunci dekripsi dan pesan acak
- Menghitung polinomial a, b dan c seperti berikut;

$$a = (f * e) \bmod q$$

$$= ((x - x^2 + x^3) * (10x + 9x^2 + 28x^3 + 26x^4 + 25x^5 + 28x^6)) \bmod 32$$

$$= 10x^2 - x^3 + 29x^4 + 7x^5 + 27x^6 + 29x^7 - 3x^8 + 28x^9, \text{ lakukan } truncated \\ \text{terhadap } 29x^7, -3x^8 \text{ dan } 28x^9 \text{ menjadi:}$$

$$29x^7 = (29) * (x^7) = 29$$

$$-3x^8 = (-3x) * (x^7) = -3x$$

$$28x^9 = (28x^2) * (x^7) = 28x^2$$

$$= 10x^2 - x^3 + 29x^4 + 7x^5 + 27x^6 + 29 - 3x + 28x^2$$

$$= (29 - 3x + 38x^2 - x^3 + 29x^4 + 7x^5 + 27x^6) \bmod 32$$

$$= 29 + 29x + 6x^2 + 31x^3 + 29x^4 + 7x^5 + 27x^6, \text{ hasil } a \text{ harus berada pada} \\ \text{interval } -16 \text{ s/d } 16. 29 \text{ dan } 31 \text{ adalah diluar dari interval sehingga} \\ \text{perlu dilakukan pengurangan koefisien polinomial terhadap nilai } q, \\ \text{maka hasilnya adalah sebagai berikut:}$$

$$a = -3 - 3x + 6x^2 - x^3 - 3x^4 + 7x^5 - 5x^6$$

Kemudian cari hitung $b = a \bmod p$ dengan langkah sebagai berikut :

$$b = (-3 - 3x + 6x^2 - x^3 - 3x^4 + 7x^5 - 5x^6) \bmod 3$$

$$= -x^3 + x^5 - 2x^6, \text{ hasil } b \text{ harus berada pada interval } -1 \text{ s/d } 1. 2 \text{ adalah diluar} \\ \text{dari interval sehingga perlu dilakukan operasi penjumlahan dan} \\ \text{pengurangan yang menghasilkan sebagai berikut:}$$

$$b = -x^3 + x^5 + x^6$$

Kemudian cari hitung $c = (f_p * b) \bmod p$ dengan langkah sebagai berikut :

$$c = ((2x + 2x^2 + x^4 + x^5 + x^6) * (-x^3 + x^5 + x^6)) \bmod 3$$

$$= (-2x^4 - 2x^5 + 2x^6 + 3x^7 + x^8 + 2x^{10} + 2x^{11} + x^{12}), \text{ lakukan } truncated \\ \text{terhadap } 5x^7, 3x^8, 2x^9, 2x^{10}, 2x^{11} \text{ dan } x^{12} \text{ menjadi:}$$

$$3x^7 = (3) * (x^7) = 3$$

$$x^8 = (x) * (x^7) = x$$

$$2x^{10} = (2x^3) * (x^7) = 2x^3$$

$$\begin{aligned}
 2x^{11} &= (2x^4) * (x^7) = 2x^4 \\
 x^{12} &= (x^5) * (x^7) = x^5 \\
 &= -2x^4 - 2x^5 + 2x^6 + 3 + x + 2x^3 + 2x^4 + x^5 \\
 &= (3 + x + 2x^3 - x^5 + 2x^6) \bmod 3 \\
 &= x + 2x^3 - x^5 - 2x^6, \text{ hasil } c \text{ harus berada pada interval } -1 \text{ s/d } 1. 2 \text{ adalah diluar dari interval sehingga perlu dilakukan operasi pengurangan yang menghasilkan sebagai berikut:} \\
 &= x - x^3 - x^5 - x^6
 \end{aligned}$$

Hasil dekripsi yaitu polinomial $c = x - x^3 - x^5 - x^6$ adalah sama dengan polinomial $m = x - x^3 - x^5 - x^6$ dengan *array* $m = [0, 1, 0, -1, 0, -1, -1]$, sehingga dikatakan polinomial acak kembali menjadi polinomial data teks.

- Untuk mengubah kembali ke dalam bilangan ASCII, tambahkan dengan 1 pada koefisien polinomial m sehingga *array* pada polinomial $m = [1, 2, 1, 0, 1, 0, 0]$, m diubah kembali ke nilai ASCII. Berikut perhitungannya;

$$1 = (1*3) + 0 = 3$$

$$0 = (3*3) + 1 = 10$$

$$1 = (10*3) + 2 = 32$$

$$2 = (32*3) + 1 = 97$$

$$1 = 97.$$

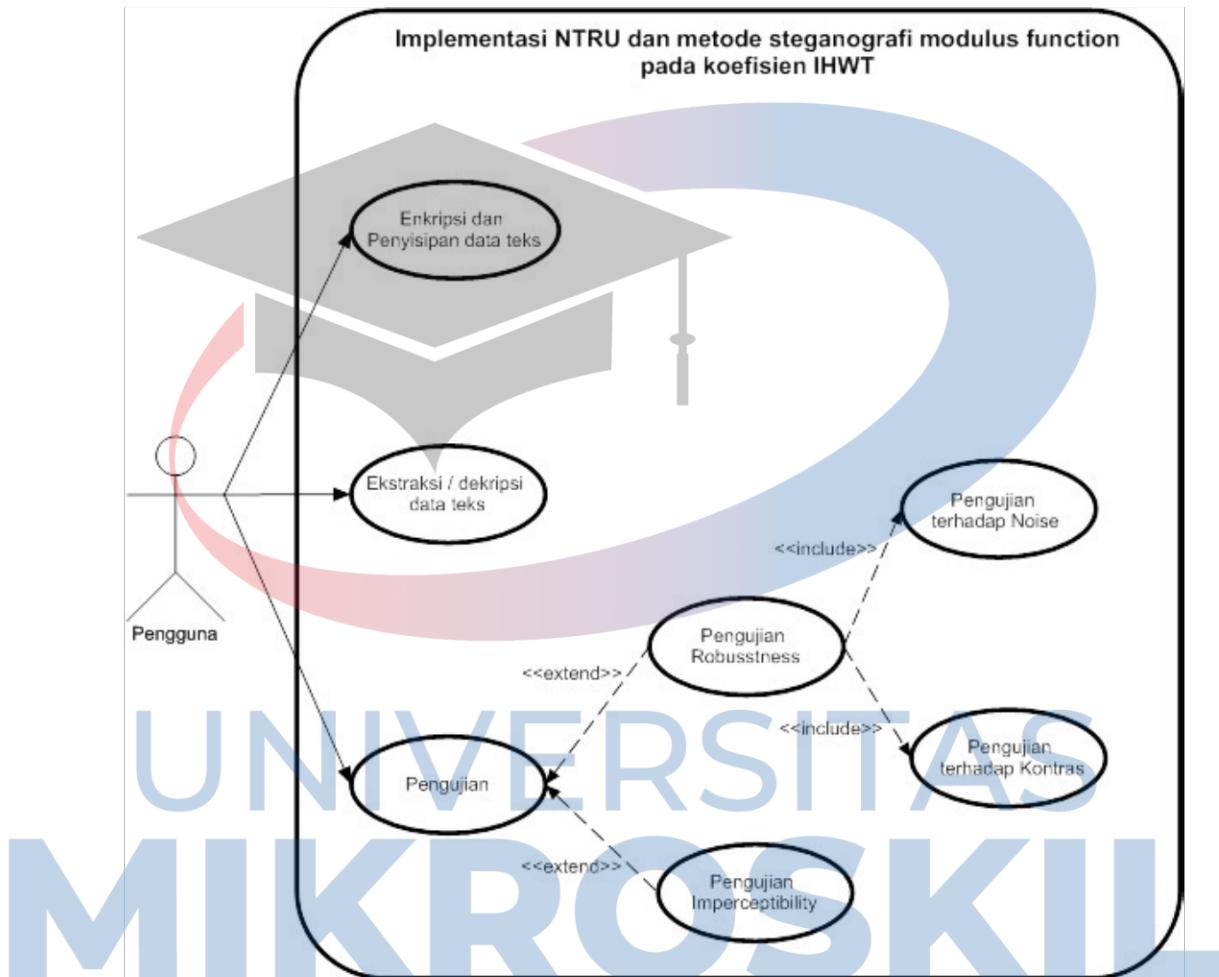
Hasil dari konversi biner ke ASCII adalah 97, dimana 97 merupakan nilai ASCII dari "a". Untuk string "wal" proses dekripsi dilakukan sama seperti string "a".

3.1.1.2. Analisis Kebutuhan

Analisis kebutuhan merupakan tahapan penting dalam pengembangan sistem untuk mengetahui secara detail sistem yang akan dikembangkan. Analisis kebutuhan dibagi menjadi dua, yaitu analisis kebutuhan fungsional dan kebutuhan non fungsional.

a. Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional adalah suatu gambaran dari informasi yang merupakan spesifikasi inti mengenai hal-hal yang bisa dilakukan oleh sistem. Analisis kebutuhan fungsional di implementasikan menggunakan *use case* seperti berikut :



Gambar 3.8. Use case diagram

Berikut narasi dari *use case* di atas:

Tabel 3. 11. Tabel narasi dari *use case* enkripsi / penyisipan data teks

Nama <i>use case</i>	Enkripsi dan penyisipan data teks
Case terkait	-
Aktor	Pengguna

Deskripsi	<i>Use case</i> menjelaskan proses penyembunyian data teks yang terjadi, meliputi enkripsi data teks, sisip data teks dan juga menyatukan pesan yang akan disisipkan dengan urutan (kunci dekripsi dan pesan acak).	
Aksi Aktor	Respon Sistem	
Bidang khas suatu kejadian	<p>1. Pengguna menekan tab menu enkripsi / <i>embedding</i> data teks.</p> <p>3. Pengguna memilih parameter set <i>NTRU</i>.</p> <p>4. Pengguna menekan <i>button</i> bangkitkan kunci enkripsi dan kunci dekripsi.</p> <p>7. Pengguna memasukan data teks di <i>richtextbox</i> pesan rahasia dan menekan <i>button</i> enkripsi.</p>	<p>2. Sistem akan masuk ke jendela enkripsi / <i>embedding</i>.</p> <p>5. Sistem membangkitkan kunci enkripsi.</p> <p>6. Sistem membangkitkan kunci dekripsi.</p> <p>8. Sistem akan menampilkan <i>ciphertext</i> di <i>richtextbox</i> pesan acak dan menampilkan waktu dari proses enkripsi.</p>

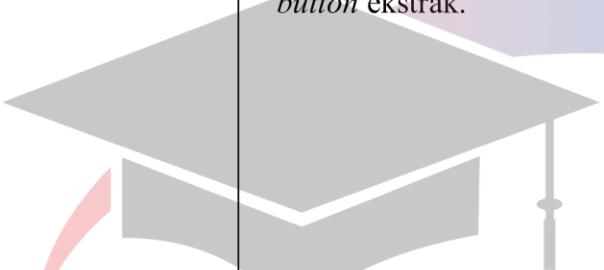
UNIVERSITAS MIKROSKIL

	<p>9. Pengguna menekan button satukan kunci dekripsi dan pesan acak.</p> <p>11. Pengguna menekan <i>button</i> bangkitkan T acak.</p> <p>13. Pengguna menekan <i>button</i> bangkitkan kunci stego dan menekan <i>button</i> simpan.</p> <p>15. Pengguna mencari citra sampul dengan menekan <i>button</i> cari dan melakukan penyisipan dengan menekan <i>button</i> sisip.</p>	<p>10. Sistem akan menggabungkan kunci dekripsi dan pesan acak dengan urutan (kunci dekripsi, pesan acak) dan menampilkan hasil penggabungannya juga hasil perhitungan bitnya.</p> <p>12. Sistem membangkitkan T acak.</p> <p>14. Sistem membangkitkan kunci stego dan menyimpan kunci stego.</p> <p>16. Sistem akan melakukan proses penyisipan dan menampilkan citra di <i>picturebox</i> citra stego.</p>
--	---	---

	17. Pengguna menekan <i>button</i> simpan dan memilih lokasi penyimpanan.	18. Sistem akan menyimpan citra stego di lokasi yang dipilih oleh pengguna.
<i>Error</i>	1. Citra sampul tidak dapat menampung pesan tersisip.	

Tabel 3.12. Tabel narasi dari *use case* ekstraksi / dekripsi data teks

Nama <i>use case</i>	Ekstraksi / dekripsi data teks	
Case terkait	-	
Aktor	Pengguna	
Deskripsi	<i>Use case</i> menjelaskan proses ekstraksi dan dekripsi data teks yang terjadi, meliputi ekstraksi data teks dan dekripsi data teks.	
Bidang khas suatu kejadian	<p>Aksi Aktor</p> <p>1. Pengguna menekan tab menu ekstraksi / dekripsi.</p> <p>3. Pengguna memasukkan citra stego dengan menekan <i>button</i> cari citra stego.</p> <p>5. Pengguna memasukkan kunci ekstraksi dengan menekan <i>button</i> cari kunci ekstrak dan bisa di masukkan</p>	<p>Respon Sistem</p> <p>2. Sistem akan masuk ke jendela ekstraksi dan dekripsi.</p> <p>4. Sistem menampilkan citra stego di <i>picture box</i>.</p>

	<p>manual langsung di <i>textbox</i> kunci ekstraksi.</p> <p>7. Pengguna melakukan ekstraksi dengan menekan <i>button</i> ekstrak.</p>  <p>9. Pengguna memasukkan kunci dekripsi dengan menekan <i>button</i> ambil <i>cipherkey</i>.</p> <p>11. Pengguna memasukkan pesan acak dengan menekan <i>button</i> ambil pesan acak.</p> <p>13. Pengguna melakukan dekripsi pesan acak dengan menekan <i>button</i> dekripsi.</p>	<p>6. Sistem akan menampilkan kunci ekstraksi di <i>textbox</i> kunci ekstraksi.</p> <p>8. Sistem akan mengambil pesan yang disisipkan dari citra stego dan menampilkannya di <i>richtextbox</i> pesan tersisip.</p> <p>10. Sistem menampilkan kunci dekripsi di <i>richtextbox</i> <i>cipherkey</i>.</p> <p>12. Sistem akan menampilkan pesan acak di <i>richtextbox</i> pesan acak.</p>
--	--	---

		14. Sistem akan menampilkan data teks di <i>richtextbox</i> pesan rahasia.
<i>Error</i>	1. Kunci ekstraksi salah. 2. Citra stego salah.	

Tabel 3. 13. Tabel narasi dari *use case* pengujian *imperceptibility*

Nama <i>use case</i>	Pengujian <i>Imperceptibility</i>	
Case terkait	Pengujian	
Aktor	Pengguna	
Deskripsi	<i>Use case</i> menjelaskan proses pengujian yang terjadi, meliputi aspek pengujian <i>imperceptibility</i> .	
	Aksi Aktor	Respon Sistem
Bidang khas suatu kejadian	1. Pengguna memilih pengujian <i>imperceptibility</i> pada <i>tab menu</i> . 3. Pengguna memilih citra sampul dan citra stego yang akan diuji dengan menekan <i>button</i> cari citra sampul dan cari citra stego. 5. Pengguna menghitung nilai <i>PSNR</i> dan <i>MSE</i> dengan	2. Sistem akan menampilkan pengujian <i>imperceptibility</i> . 4. Sistem akan menampilkan citra sampul dan citra stego yang telah dipilih dan ditentukan oleh pengguna.

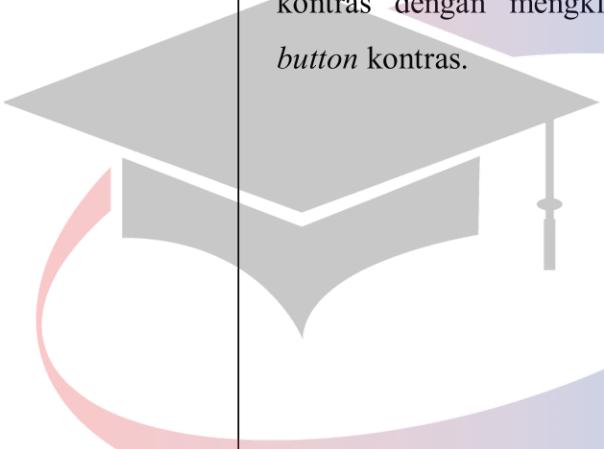
	menekan <i>button</i> hitung <i>PSNR</i> dan <i>MSE</i> .	
	7. Pengguna menekan <i>button</i> ekspor tabel ke excel.	6. Sistem akan menampilkan nilai <i>PSNR</i> dan <i>MSE</i> dari kedua citra. 8. Sistem akan menampilkan data dari tabel di program ke dalam <i>ms.excel</i> .
<i>Error</i>	1. Citra stego tidak ada.	

Tabel 3. 14. Tabel narasi dari *use case* pengujian *robustness*

Nama <i>use case</i>	Pengujian <i>Robustness</i>	
Case terkait	Pengujian terhadap <i>noise salt and pepper</i> dan kontras	
Aktor	Pengguna	
Deskripsi	<i>Use case</i> menjelaskan proses pengujian <i>robustness</i> yang terjadi meliputi pengujian terhadap <i>noise</i> dan kontras.	
	Aksi Aktor	Respon Sistem
Bidang khas suatu kejadian	1. Pengguna memilih pengujian <i>robustness</i> pada tab menu. 3. Pengguna melakukan pengujian terhadap <i>noise</i>	2. Sistem akan menampilkan pengujian <i>robustness</i> dimana terdapat dua variasi yaitu pengujian <i>noise</i> dan kontras.

	<p>dengan memasukan citra stego yang akan diuji dengan menekan <i>button</i> cari citra stego.</p> <p>5. Pengguna memasukan kunci stego dengan menekan <i>button</i> ambil kunci stego.</p> <p>7. Pengguna memasukkan persentase <i>noise salt and pepper</i> dan menekan <i>button</i> tambah noise.</p> <p>9. Pengguna mengklik <i>button</i> simpan lalu menentukan lokasi penyimpanan.</p>	<p>4. Sistem akan menampilkan citra stego yang ditentukan oleh pengguna di <i>picturebox</i> citra stego.</p> <p>6. Sistem akan menampilkan kunci stego di <i>textbox</i> kunci stego</p> <p>8. Sistem akan menampilkan citra stego yang sudah ditambah <i>noise salt and pepper</i>.</p> <p>10. Sistem akan menampilkan <i>form dialog</i> untuk lokasi penyimpanan dan menampilkan <i>messagebox</i> saat pengguna sudah</p>
--	--	--

	<p>11. Pengguna menekan <i>button ekstrak</i>.</p> <p>13. Pengguna menekan <i>button ekspor tabel ke excel</i>.</p> <p>15. Pengguna dapat melihat nilai piksel yang diberi serangan terhadap <i>noise</i> dengan mengklik <i>button bandingkan kedua citra</i>.</p> <p>17. Selanjutnya pengguna pindah pengujian terhadap kontras dengan mengklik pengujian kontras pada <i>tab menu</i> di <i>form pengujian robustness</i></p>	<p>menentukan lokasi penyimpanan.</p> <p>12. Sistem akan menampilkan hasil ekstrak di <i>textbox</i> hasil ekstraksi citra stego dan <i>textbox</i> hasil ekstraksi citra <i>noise</i> serta menampilkannya pada tabel dalam programnya.</p> <p>14. Sistem akan menampilkan data dari tabel di program ke dalam <i>ms.excel</i>.</p> <p>16. Lalu sistem akan menampilkan sebuah <i>form matrix value viewer</i>.</p>
--	--	--

	<p>18.Sistem akan menampilkan pengujian <i>robustness</i> terhadap kontras.</p> <p>19.Lalu pengguna memasukkan citra stego dan memasukkan nilai kontras lalu menambah kontras dengan mengklik <i>button</i> kontras.</p> 	<p>20.Sistem akan menampilkan citra stego di <i>picturebox</i> citra stego lalu menampilkan citra hasil penambahan kontras di <i>picturebox</i> citra stego setelah diberikan kontras.</p>
	<p>21.Pengguna menyimpan citra kontras dengan mengklik <i>button</i> simpan citra kontras dan memilih lokasi penyimpanan.</p>	<p>22.Lalu sistem akan menampilkan <i>form dialog</i> untuk pengguna menentukan lokasi penyimpanan dan menampilkan <i>messagebox</i> saat pengguna sudah menentukan lokasi penyimpanan.</p>

	<p>23.Selanjutnya pengguna mencari kunci ekstrasi dengan mengklik <i>button</i> cari kunci ekstraksi dan menekan <i>button</i> ekstraksi pesan.</p>	
	<p>25.Selanjutnya pengguna menghitung persentase dengan mengklik <i>button</i> hitung persentase pesan kembali.</p>	<p>24. Sistem akan menampilkan hasil ekstraksi pesan dari citra stego di <i>richtextbox</i> citra stego dan <i>richtextbox</i> citra kontras pada citra kontras.</p>
	<p>27.Selanjutnya pengguna memasukkan data ke tabel dengan mengklik <i>button</i> tambah ke tabel lalu mengekspro ke <i>excel</i> dengan mengklik <i>button</i> ekspor ke <i>excel</i>.</p>	<p>26.Selanjutnya sistem akan menampilkan persentase pesan kembali di <i>textbox</i> pesan sisip kembali.</p>
		<p>28.Selanjutnya sistem akan menampilkan tabel yang berisi <i>field</i> pengujian dan menampilkan <i>ms.excel</i> yang</p>

	<p>29. Pengguna dapat melihat nilai piksel yang diberi serangan terhadap kontras dengan mengklik <i>button</i> bandingkan kedua citra.</p>	<p>berisi data pengujian dari tabel apikasi tersebut.</p>
		<p>30. Lalu sistem akan menampilkan sebuah <i>form matrix value viewer</i>.</p>
Error	<ol style="list-style-type: none"> 1. Citra stego tidak ada. 2. Masukkan dari persentase <i>noise</i> menggunakan karakter titik sebagai masukkan nilai pecahan pada persentase <i>noise</i>. 3. Masukkan dari nilai kontras menggunakan nilai pecahan. 	

b. Analisis Kebutuhan Non Fungsional

Analisis kebutuhan *non fungsional* dilakukan untuk mengetahui spesifikasi terhadap kinerja, informasi, ekonomi, pengendalian, efisiensi dan pelayanan yang dikenal PIECES. Kepanjangan dari PIECES adalah P = *Performance*, I = *Information*, E = *Economic*, C = *Control*, E = *Efficiency* dan S = *Service*. Berikut merupakan kerangka dari PIECES.

1. Performance

Program dapat melakukan proses penyisipan dan ekstraksi data teks pada citra sampul tanpa ada batas maksimalnya terkecuali pada perhitungan persentase pesan kembali di proses pengujian *robustness*, apabila semakin besar parameter set yang digunakan saat penyisipan maka semakin lama proses perhitungan persentase pesan kembali dari citra stego yang telah ditambahkan *noise*.

2. Information

- i. Perangkat lunak dapat memberikan informasi berupa *listview* hasil pengujian *imperceptibility* yang berisi ukuran citra, nilai *PSNR* dan *MSE*.
- ii. Perangkat lunak dapat memberikan informasi berupa *listview* hasil pengujian *robustness* yang berisi ukuran citra, persentase noise dan persentase kembali.
- iii. Perangkat lunak dapat memberikan informasi berupa *message box* ketika ukuran citra sampul tidak dapat menampung pesan teks yang diberikan.
- iv. Perangkat lunak dapat menampilkan informasi waktu saat proses penyembunyian dan ekstraksi dalam bentuk berupa *message box*.
- v. Perangkat lunak dapat menampilkan *progress bar* saat proses penyembunyian dan ekstraksi sedang berjalan.

3. Economic

Perangkat lunak tidak memerlukan perangkat pendukung lainnya dalam proses eksekusi dengan adanya *.NET Framework* sehingga perangkat tidak memerlukan banyak biaya biaya dalam proses perancangannya.

4. Control

- i. Perangkat lunak melakukan validasi terhadap polinomial acak dari *NTRU* dalam melakukan proses pembangkitan kunci enkripsi dan dekripsi.
- ii. Perangkat lunak melakukan validasi terhadap ekstensi dari citra .bitmap 24 bit.
- iii. Perangkat lunak melakukan validasi masukan dari ukuran citra sampul terhadapa pesan acak yang akan disisipkan.

5. Efficiency

User dapat melakukan proses pengujian terhadap banyak citra stego dan citra sampul dengan menyimpan laporannya ke dalam *excel*.

6. Service

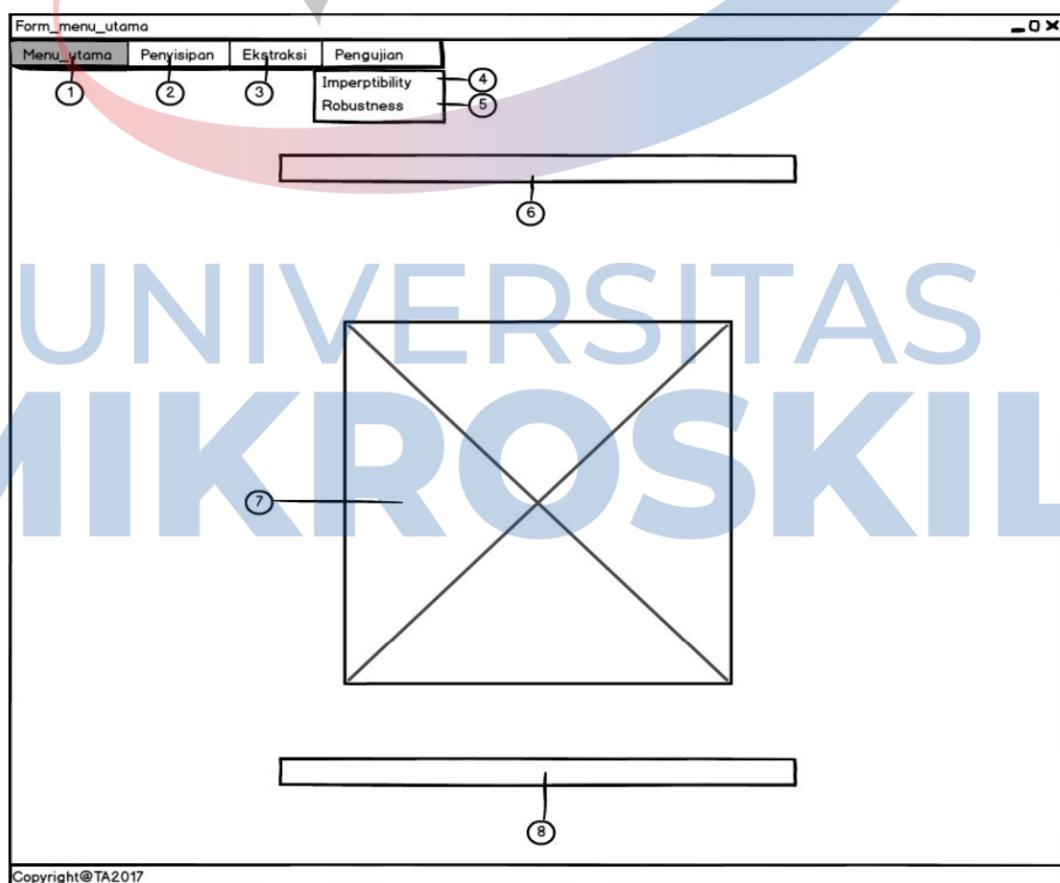
User dapat melakukan pengamanan data teks dengan menggunakan sistem dan juga mengetahui lama waktu dari masing-masing proses.

3.2. Perancangan Sistem

Pada tahap ini dilakukan perancangan dari aplikasi yang akan dibangun, seperti perancangan *interface* dengan *Balsamiq Mockups*.

3.2.1. Perancangan Form Menu Utama

Perancangan *form* menu utama merupakan *form* yang pertama muncul saat perangkat lunak dijalankan yang berfungsi menyediakan informasi identitas penulis serta menyediakan *link* yang memanggil *form* yang ada pada aplikasi. Berikut ini tampilan *form* menu utama.



Gambar 3.9. Perancangan menu utama

Keterangan:

1. *Tab control* yang berfungsi untuk menampilkan *tab page menu utama*.
2. *Tab control* yang berfungsi untuk menampilkan *tab page pengirim*.
3. *Tab control* yang berfungsi untuk menampilkan *tab page penerima*.
4. *Tab control* yang berfungsi untuk menampilkan *tab page pengujian imperceptibility* pada citra stego.
5. *Tab control* yang berfungsi untuk menampilkan *tab page pengujian robustness* pada citra stego.
6. *Label* yang berisi judul skripsi penulis.
7. *Label* yang berisi logo.
8. *Label* yang berisi identitas penulis.

3.2.2. Perancangan Form Penyisipan

Perancangan *form* penyisipan untuk menyembunyikan data teks ke dalam citra sampul yang terdiri dari enkripsi data teks yang akan menghasilkan *ciphertext*, penyembunyian *ciphertext* ke dalam citra sampul serta menyimpan *ciphertext* dan citra stego. Berikut ini tampilan *form* penyisipan:

The screenshot shows the 'Form Penyisipan' application window divided into two main sections:

- Left Panel (Kriptografi (NTRU)):** Contains fields for parameter sets (p, q, N, dt), message inputs (Pesron rahasia, Pesan acak), and encryption/decryption buttons (Enkripsi, Hopus).
- Right Panel (Steganografi (IHWTF+Modulus Function)):** Contains fields for alpha, T Acak, and various Steganography functions like Bangkitkan T acak, Simpan, Cari, Sisip, and PSNR/MSE calculations.

Gambar 3.10. Perancangan *form* penyisipan

Keterangan:

1. *Combobox* yang berfungsi untuk mengambil dan menampilkan parameter *set* sesuai standar *security level* yang direkomendasi oleh *IEEE P1363.1TM/D10*.
2. *Textbox* yang berfungsi untuk menampilkan nilai parameter dari *p*.
3. *Textbox* yang berfungsi untuk menampilkan nilai parameter dari *q*.
4. *Textbox* yang berfungsi untuk menampilkan nilai parameter dari *N*.
5. *Textbox* yang berfungsi untuk menampilkan nilai parameter dari *df*.
6. *Richtextbox* yang berfungsi untuk menampilkan kunci dekripsi.
7. *Richtextbox* yang berfungsi untuk menampilkan kunci enkripsi.
8. *Button* yang berfungsi untuk membangkitkan kunci dekripsi.
9. *Label* yang berfungsi untuk menampilkan waktu membangkitkan kunci dekripsi.
10. *Button* yang berfungsi untuk membangkitkan kunci enkripsi.
11. *Label* yang berfungsi untuk menampilkan waktu membangkitkan kunci enkripsi.
12. *Richtextbox* yang berfungsi untuk tempat mengetikkan isi pesan rahasia.
13. *Button* yang berfungsi untuk mengenkripsi pesan rahasia.
14. *Button* yang berfungsi untuk menghapus isi pesan rahasia.
15. *Richtextbox* yang berfungsi untuk menampilkan pesan acak.
16. *Label* yang berfungsi untuk menampilkan waktu mengenkripsi pesan rahasia menjadi pesan acak.
17. *Richtextbox* yang berfungsi untuk menampilkan pesan yang akan disisip.
18. *Button* yang berfungsi untuk menyatukan pesan yang akan disisip.
19. *Label* yang berfungsi untuk menampilkan panjang bit yang akan disisip.
20. *Textbox* yang berfungsi untuk menampilkan parameter *a*
21. *Textbox* yang berfungsi untuk menampilkan parameter *T* yang telah diacak.
22. *Button* yang berfungsi untuk menampilkan hasil dari nilai *T* acak.
23. *Richtextbox* yang berfungsi untuk menampilkan kunci steganografi.
24. *Button* yang berfungsi untuk membangkitkan kunci stego.
25. *Button* yang berfungsi untuk menyimpan kunci stego.

26. Picturebox yang berfungsi untuk menampilkan citra sampul.
27. Picturebox yang berfungsi untuk menampilkan citra stego.
28. Button yang berfungsi untuk mengambil citra yang akan disisip pesan acak.
29. Button yang berfungsi untuk menyisipkan pesan acak ke citra.
30. Progressbar yang berfungsi untuk menampilkan proses sedang berjalan saat pesan acak disisipkan ke dalam citra sampul.
31. Button yang berfungsi untuk menyimpan citra stego (citra yang telah disisip pesan acak).
32. Label yang berfungsi untuk menampilkan waktu pada proses penyisipan.
33. Textbox yang berfungsi untuk menampilkan nilai MSE dari citra stego.
34. Textbox yang berfungsi untuk menampilkan nilai PSNR dari citra stego.

3.2.3. Perancangan Form Ekstraksi

Perancangan *form* ekstraksi untuk mengekstraksi data teks dari dalam citra stego yang terdiri dari dekripsi *ciphertext* yang akan menghasilkan *plaintext*, mengeskstraksi *ciphertext* dari dalam citra stego. Berikut ini tampilan *form* ekstraksi.

The screenshot shows a Windows-style application window titled "Form_ekstraksi". The window has a menu bar with "Menu_utama", "Penyisipan", "Ekstraksi", and "Pengujian".

Left Panel (Steganografi):

- Contains a "Citra stego" input field with a crossed-out image (labeled 1).
- A "Cari" button (labeled 2).
- A "Kunci Ekstraksi" input field (labeled 3).
- A "Cari" button (labeled 4).
- An "Ekstraksi" button (labeled 5).
- A "Pesanan Tersisip (Cipherkey + Pesan Acak)" output area (labeled 6).
- A "Pesan Acak" output area (labeled 7).

Right Panel (Kriptografi):

- A "Cipherkey (h)" input field with a dropdown arrow (labeled 8).
- A "Ambil Cipherkey" button (labeled 9).
- A "Pesanan Acak" input field (labeled 10).
- A "Ambil Pesan Acak" button (labeled 11).
- A "Dekripsi" button (labeled 12).
- A "Pesanan Rahasia" output area (labeled 13).
- A "Pesan Acak" output area (labeled 14).

At the bottom left of the window is the text "Copyright@TA2017".

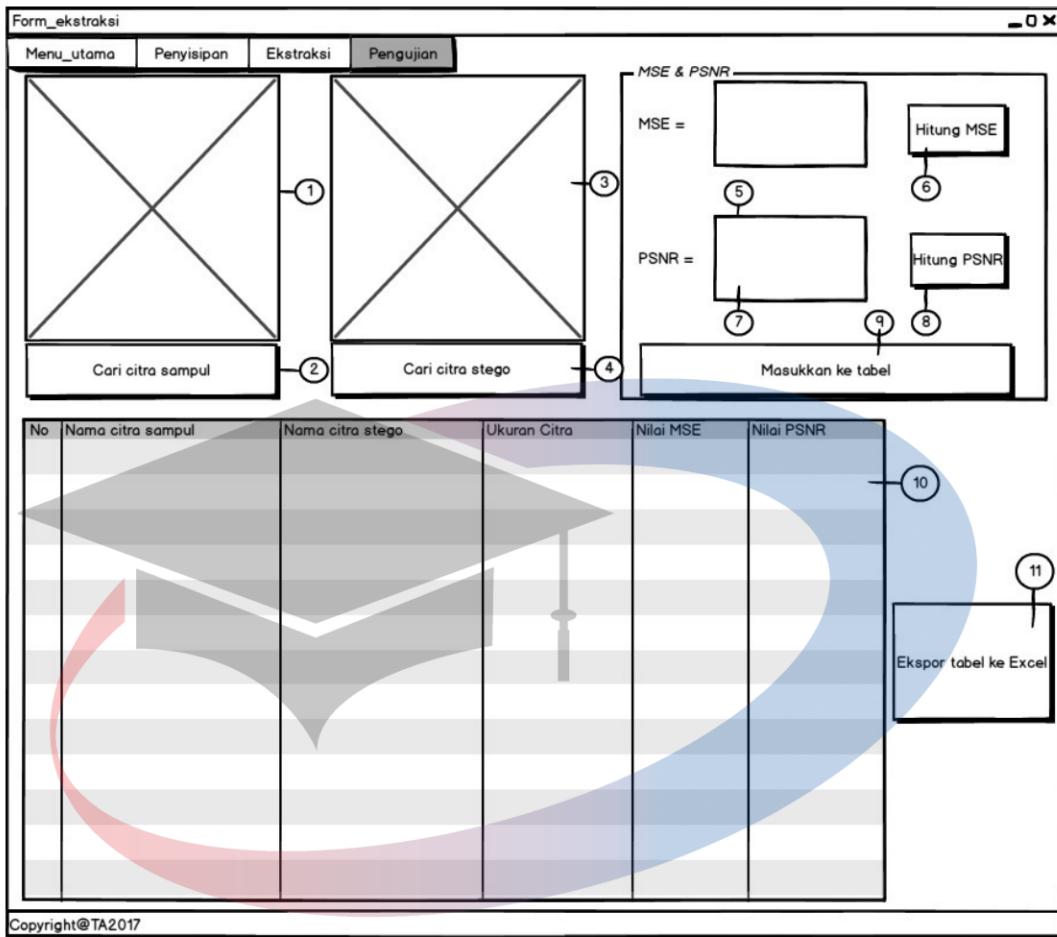
Gambar 3.11. Perancangan *form* ekstraksi

Keterangan:

1. *Picture box* yang berfungsi untuk menampilkan citra stego.
2. *Button* yang berfungsi untuk mengambil citra stego yang telah disimpan.
3. *Textbox* yang berfungsi untuk menampilkan kunci ekstraksi atau sebagai tempat pengetikan kunci ekstraksi.
4. *Button* yang berfungsi untuk mengambil kunci stego.
5. *Progressbar* yang berfungsi untuk menampilkan proses sedang berjalan saat pesan acak di ekstraksi dari dalam citra stego.
6. *Button* yang berfungsi untuk mengekstrak pesan acak dari citra stego.
7. *Richtextbox* yang berfungsi untuk menampilkan pesan yang tersisip.
8. *Richtextbox* yang berfungsi untuk menampilkan kunci rahasia (kunci dekripsi).
9. *Button* yang berfungsi untuk mengambil kunci rahasia (kunci dekripsi) yang telah disimpan.
10. *Richtextbox* yang berfungsi untuk menampilkan pesan acak.
11. *Button* yang berfungsi untuk mengambil pesan acak.
12. *Button* yang berfungsi untuk mendekripsi pesan acak.
13. *Progressbar* yang berfungsi untuk menampilkan proses dekripsi sedang berjalan.
14. *Richtextbox* yang berfungsi untuk menampilkan pesan rahasia hasil proses dekripsi.

3.2.4. Perancangan Form Pengujian Imperceptibility

Perancangan *form* pengujian *imperceptibility* untuk menguji citra stego menggunakan metode mengukur *MSE* dan *PSNR* yang akan dibandingkan dengan citra sampul. Berikut ini tampilan *form* pengujian *imperceptibility*.



Gambar 3.12. Perancangan form pengujian *imperceptibility*

Keterangan :

1. Picturebox yang berfungsi untuk menampilkan citra sampul.
2. Button yang berfungsi untuk mengambil citra sampul.
3. Picturebox yang berfungsi untuk menampilkan citra steganografi.
4. Button yang berfungsi untuk mengambil citra steganografi.
5. RichTextbox yang berfungsi untuk menampilkan nilai *MSE* pada pengujian *imperceptibility*.
6. Button yang berfungsi untuk menghitung nilai *MSE* pada pengujian *imperceptibility*.
7. RichTextbox yang berfungsi untuk menampilkan nilai *PSNR* pada pengujian *imperceptibility*.
8. Button yang berfungsi untuk menghitung nilai *PSNR* pada pengujian *imperceptibility*.
9. RichTextbox yang berfungsi untuk menampilkan nilai *MSE* pada pengujian *imperceptibility*.
10. RichTextbox yang berfungsi untuk menampilkan nilai *PSNR* pada pengujian *imperceptibility*.
11. RichTextbox yang berfungsi untuk menghitung nilai *PSNR* pada pengujian *imperceptibility*.

9. *Button* yang berfungsi untuk memasukan nilai dari perhitungan *PSNR* dan *MSE* ke dalam tabel.
10. *Table* yang berfungsi untuk menampilkan nilai *PSNR* dan *MSE* dari pengujian *imperceptibility*
11. *Button* yang berfungsi untuk mengekspor tabel dari sistem ke *microsoft excel*.

3.2.5. Perancangan Form Pengujian Robustness

Perancangan *form* pengujian *robustness* untuk menguji citra stego menggunakan serangan pemberian *noise salt and pepper* yang akan diberikan persentase noisenya. Berikut ini tampilan *form* pengujian *robustness*.

No	Nama citra stego	Nama citra noise	Ukuran Citra	Persentase noise	Persentase kembali
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Gambar 3.13. Perancangan *form* pengujian *robustness* terhadap *noise*

Keterangan :

1. *Button* yang berfungsi untuk mencari citra stego.
2. *Picturebox* yang berfungsi untuk menampilkan citra stego
3. *Textbox* yang berfungsi untuk mengisi nilai persentase dari noise *salt and pepper*.
4. *Button* yang berfungsi untuk menambah *noise* pada citra stego.
5. *Progress bar* yang berfungsi untuk menampilkan proses menambah *noise* pada citra stego sedang berjalan.
6. *Picturebox* yang berfungsi untuk menampilkan citra *noise*.
7. *Textbox* yang berfungsi untuk menampilkan atau mengisi kunci stego.
8. *Button* yang berfungsi untuk mengambil kunci stego.
9. *Button* yang berfungsi untuk menyimpan citra stego.
10. *Button* yang berfungsi untuk menampilkan titik kordinat pada setiap piksel dari citra stego dan citra modifikasi.
11. *Button* yang berfungsi untuk mengekstrak citra stego dan citra yang telah ditambah *noise*.
12. *Progress bar* yang berfungsi untuk menampilkan proses ekstraksi sedang berjalan.
13. *Richtextbox* yang berfungsi untuk menampilkan hasil ekstraksi (kunci dekripsi dan pesan acak) dari pada citra stego.
14. *Richtextbox* yang berfungsi untuk menampilkan hasil ekstraksi (kunci dekripsi dan pesan acak) dari citra stego yang telah ditambahkan *noise salt and pepper*.
15. *Button* yang berfungsi untuk menghitung persentase pesan kembali.
16. *Progress bar* yang berfungsi untuk menampilkan proses perhitungan persentase pesan kembali sedang berjalan.
17. *Textbox* yang berfungsi untuk menampilkan proses perhitungan persentase pesan kembali.
18. *Button* yang berfungsi untuk menambahkan nilai persentase pesan kembali ke tabel.

19. *Table* yang berfungsi untuk menampilkan hasil pengujian dari *robustness* terhadap *noise salt and pepper*.
20. *Button* yang berfungsi untuk mengekspor tabel dari sistem ke *microsoft excel*.

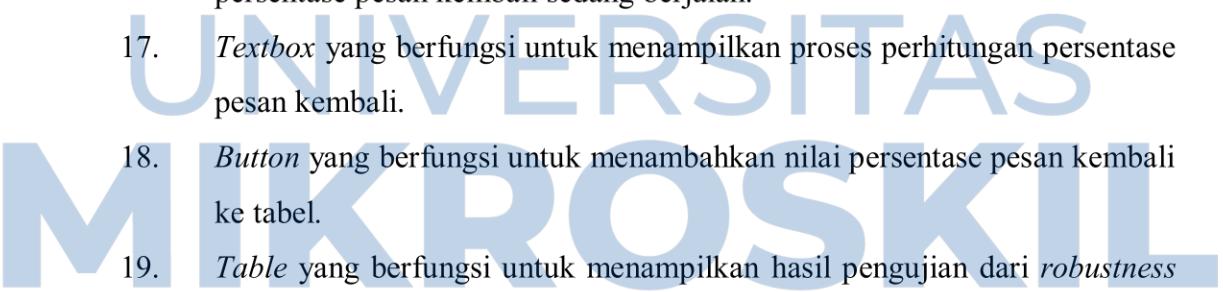
No	Nama citra stego	Nama citra kontras	Ukuran Citra	Persentase noise	Persentase kembali

Copyright@TA2017

Gambar 3.14. Perancangan *form* pengujian *robustness* terhadap kontras

Keterangan :

1. *Button* yang berfungsi untuk mencari citra stego.
2. *Picturebox* yang berfungsi untuk menampilkan citra stego
3. *Textbox* yang berfungsi untuk mengisi nilai kontras yang ingin ditambahkan.
4. *Button* yang berfungsi untuk menambah kontras pada citra stego.
5. *Progress bar* yang berfungsi untuk menampilkan proses menambah kontras pada citra stego sedang berjalan.

- 
6. *Picturebox* yang berfungsi untuk menampilkan citra kontras.
 7. *Textbox* yang berfungsi untuk menampilkan atau mengisi kunci stego.
 8. *Button* yang berfungsi untuk mengambil kunci stego.
 9. *Button* yang berfungsi untuk menyimpan citra stego setelah diberi kontras.
 10. *Button* yang berfungsi untuk menampilkan titik kordinat pada setiap piksel dari citra stego dan citra modifikasi.
 11. *Button* yang berfungsi untuk mengekstrak citra stego dan citra yang telah ditambah kontras.
 12. *Progress bar* yang berfungsi untuk menampilkan proses ekstraksi sedang berjalan.
 13. *Richtextbox* yang berfungsi untuk menampilkan hasil ekstraksi (kunci dekripsi dan pesan acak) dari citra stego.
 14. *Richtextbox* yang berfungsi untuk menampilkan hasil ekstraksi (kunci dekripsi dan pesan acak) dari citra stego yang telah ditambahkan nilai kontras.
 15. *Button* yang berfungsi untuk menghitung persentase pesan kembali.
 16. *Progress bar* yang berfungsi untuk menampilkan proses perhitungan persentase pesan kembali sedang berjalan.
 17. *Textbox* yang berfungsi untuk menampilkan proses perhitungan persentase pesan kembali.
 18. *Button* yang berfungsi untuk menambahkan nilai persentase pesan kembali ke tabel.
 19. *Table* yang berfungsi untuk menampilkan hasil pengujian dari *robustness* terhadap kontras..
 20. *Button* yang berfungsi untuk mengeksport tabel dari sistem ke *microsoft excel*.