BAB 4 PEMBAHASAN

Pada bab ini, akan dijelaskan pembahasan mengenai tentang hasil analisis dari kombinasi penggunaan antara algoritma enkripsi *AES* (*Advanced Encryption Standart*) dan juga algoritma kompresi *LZW* (Lempel-Ziv-Welch) untuk pengamanan file berjenis citra gambar. Penelitian akan melakukan proses enkripsi dan kemudian dikombinasikan dengan proses kompresi pada saat proses pengamanan citra gambar.

4.1. Sumber Data

Data yang digunakan pada penelitian adalah bersumber dari data bertipe citra atau gambar yang diperoleh dari internet dengan memiliki file citra yang sesuai. Citra yang digunakan disimpan kedalam bentuk format sebagai berikut:

4.1.1. Sumber Data

Data yang diapakai atau digunakan pada penelitian adalah bersumber dari data bertipe citra yang diperoleh dari internet dan juga ada beberapa dokumen disimpan kedalam format berikut ni :

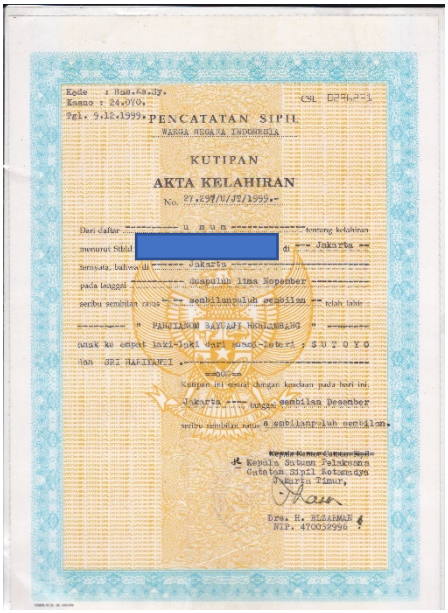
Tabel 4.1 Sumber Data

No	Tipe File	Keterangan
1	.jpg	JPG (*Joint Photographic Group*) merupakan skema kompresi file bitmap
2	.png	PNG *(Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut.

Berikut merupakan sampel gambar yang diambil dari beberapa sumber internet terdapat 4 gambar citra dengan format jpg dan png jadi untuk ditotal menjadi sebanyak 8 citra karena masing – masing dari citra mewakili 2 format, yaitu jpg dan png.

Gambar 1 Sampel Gambar Lenna

Gambar *2* Sampel Sertifikat Seminar Gambar



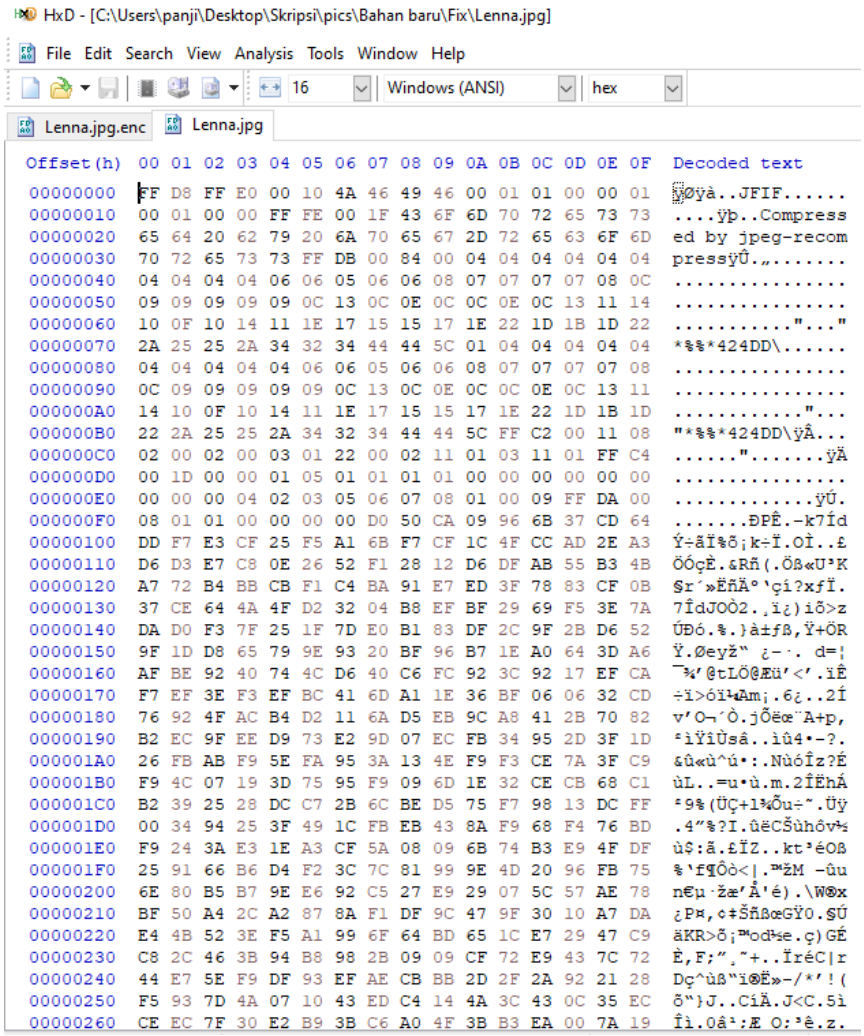
Gambar *3* Sampel Surat Dokumen Gambar

Gambar 4 Sampel Gambar Tiger

4.2. Perhitungan AES dan LZW

Analisis bagaimana cara kerja enkripsi AES adalah sebagai berikut :

1. Citra diubah ke dalam bentuk byte stream.
2. Kemudian kalau 16 byte akhir tidak sampai 16, si dengan padding atau null.
3. Byte stream dipecah 16 byte setiap bloknya.
4. Jalankan proses enkripsi berdasarkan blok pertama yang diubah menjadi array state.
5. Proses AES :
    a. *AddRoundKey*, yaitu XOR dengan key dan *plaintext*
    b. *SubBytes, subtitusi byte pada tabel S-Box*
    c. *ShiftRow, penggeseran byte pada array*
    d. *MixColumns, transformasi kolom state*
    e. *AddRoundKey, yaitu XOR state dengan roundkey*
    f. *Lakukan proses dari a sampai e selama Nr-1 kali*
    g. *Pada round terakhir lakukan proses a sampai d tanpa langkah MixColumn.*
6. Setelah langkah enkripsi 16 byte selesai, maka lakukan 16 byte setelahnya hingga semua blok byte terenkripsi.



Gambar 5 Barisan Hexadecimal

Sekarang akan diambill contoh perhitungan AES 256 bit yaitu dengan pada awal baris hexadecimal gambar tersebut dimana untuk mengetahui barisan hexadecimal menggunakan aplikasi HxD yang tersedia di nternet. Berikut adalah langkah – langkah dan perhitungan yang dilakukan sebagai berikut :

Contoh barisan hexadecimal yang diambil adalah barisan awal dari gambar 4.5 sehingga didapatkan matriks hexadecimal sebagai berikut :

Plainteks :

FF	10	46	01
D8	4A	00	00
FF	46	01	00

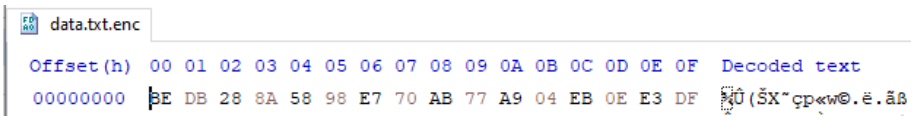
E0	49	01	01

Kunci :

BE	58	AB	EB
DB	98	77	0E
28	E7	A9	E3
8A	70	04	DF

Key Schedule :

Chiperkey di eksp ansi untuk menghasilkan subkey yang akan digunakan untuk setiap putaran sampai Nr – 1 kali putaran



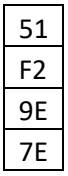
Gambar 6 Gambar Barisan Hexadecimal Key

Kunci Awal

BE	58	AB	EB
DB	98	77	0E
28	E7	A9	E3
8A	70	04	DF

Kolom terakhir chiperkey dirotasi pada baris 1 menjadi baris 4 (rot word)

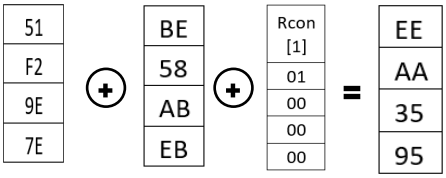
Kemudian kolom diubah berdasarkan tabel S-Box menjadi :



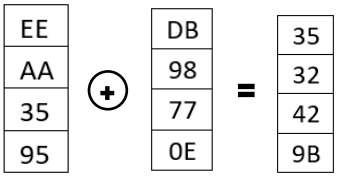
Kemudian kolom dioperasikan XOR dengan kolom ke empat sebelumnya (W_{i-1} sampai dengan W_{i-4}). Dibutuhkan tabel Rcon yang bersifat baku.

Tabel 4.2 RCon (Round Constant)

Rcon [1]	Rcon [2]	Rcon [3]	Rcon [4]	Rcon [5]	Rcon [6]	Rcon [7]	Rcon [8]	Rcon [9]	Rcon [10]
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00



Kemudian lakukan proses ulnag XOR hingga 4 kolom ke sebelumnya seperti contoh :



Kemudian dilakukan proses selanjutnya sehingga akan mendapatkan keyschedule yaitu sebagai berikut :

Key Schedule				Round Constant
BE	58	AB	EB	
DB	98	77	0E	
28	E7	A9	E3	
8A	70	04	DF	
00	00	00	00	
00	00	00	00	
00	00	00	00	
00	00	00	00	
DC	84	2F	C4	01
B8	20	57	59	
4B	AC	05	E6	
E9	99	9D	42	
1C	1C	1C	1C	
CB	CB	CB	CB	
8E	8E	8E	8E	
2C	2C	2C	2C	
C1	45	6A	AE	02
A1	81	D6	8F	
3A	96	93	75	
75	EC	71	33	
F8	E4	F8	E4	
B8	73	B8	73	
13	9D	13	9D	
EF	C3	EF	C3	
4A	0F	65	CB	04
FF	7E	A8	27	
14	82	11	64	
1C	F0	81	B2	
E7	03	FB	1F	
74	07	BF	CC	
50	CD	DE	43	
D8	1B	F4	37	
09	06	63	A8	08
E5	9B	33	14	
8E	0C	1D	79	
DC	2C	AD	1F	
25	26	DD	C2	
8E	89	36	FA	

E6	2B	F5	B6	
18	03	F7	C0	
34	32	51	F9	10
AB	30	03	17	
34	38	25	5C	
F9	D5	78	67	
BC	9A	47	85	
7E	F7	C1	3B	
AC	87	72	C4	
9D	9E	69	A9	
F6	C4	95	6C	20
B7	87	84	93	
E7	DF	FA	A6	
6E	BB	C3	A4	
EC	76	31	B4	
A2	55	94	AF	
88	0F	7D	B9	
D4	4A	23	8A	
CF	0B	9E	F2	40
E1	66	E2	71	
99	46	BC	1A	
E3	58	9B	3F	

Setelah melakukan proses key schedule maka proses yang dilakukan adalah sebagai berikut :

A. *AddRoundKey*, yaitu XOR dengan key dan plainteks

83	00	49	01
8D	10	46	00
FF	4A	00	00
E0	46	01	01

⊕

BE	DB	28	8A
58	98	E7	70
AB	77	A9	04
EB	0E	E3	DF

=

41	03	D7	6A
58	88	AD	36
E2	31	A9	05
EA	0E	E3	DE

B. *SubBytes, subtitusi byte pada S-Box*

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x 0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

S-BOX

Gambar 7 Tabel S-Box

41	03	D7	6A
58	88	AD	36
E2	31	A9	05
EA	0E	E3	DE

Subtitusi dengan S-Box

83	7B	0E	02
6A	C4	95	05
98	C7	D3	6B
87	AB	11	1D

C. *ShiftRows, penggeseran byte pada array*

Pada transformasi untuk baris pertama tidak digeser, sedangkan untuk baris kedua digeser ke kiri satu kali, baris ketiga geser ke kiri dua kali, dan baris keempat digeser ke kiri tiga kali.

83	7B	0E	02
C4	95	05	6A
D3	6B	98	C7
11	1D	87	AB

Dilakukan *ShiftRows* →

83	7B	0E	02
6A	C4	95	05
98	C7	D3	6B
87	AB	11	1D

D. *MixColumns, transfomasi kolom state dengan matriks*

Perkalian matriks antara kolom state dengna matriks yaitu sebagai berikut :

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

✖

83	7B	0E	02
6A	C4	95	05
98	C7	D3	6B
87	AB	11	1D

$= (02 \times 83) \odot (03 \times 6a) \odot (01 \times 98) \odot (01 \times 87)$

(02 x 83) = x (10000011)
(02 x 83) = x $(x^7 + x + 1)$
(02 x 83) = $x^8 + x^2 + x$
(02 x 83) = $x^4 + x^3 + x + 1 + x^2 + x$
(02 x 83) = $x^4 + x^3 + x^2 + 1$
= 00011101
(03 x 6a) = $(x + 1)\ (x^6 + x^5 + x^3 + x)$
(03 x 6a) = $(x^7 + x^6 + x^4 + x^2) + (x^6 + x^5 + x^3 + x)$
(03 x 6a) = $x^7 + x^4 + x^3 + x^2 + x$
= 10011110
(01 x 98) = 1 (10011000)
= 10011000
(01 x 87) = 1 (10000111)
= 10000111
= 00011101⊕10011110⊕10011000⊕10000111
= 10011100 atau 9C

E. *AddRoundKey*, yaitu XOR dengan roundkey

F. *Lakukan proses tersebut A sampai E selama Nr-1 kali*

G. *Proses akhir jalankan langkah A sampai E tanpa langkah MixColumns*

Sehingga setelah melakukan proses perhitungan akan menghasilkan sebagai berikut:

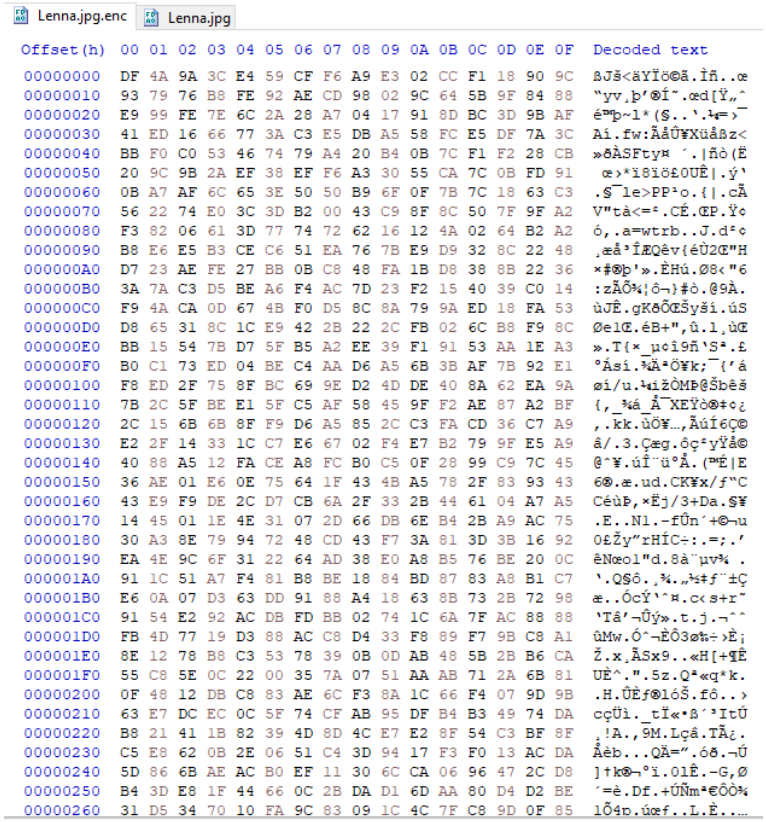
Tabel 4.3 Tabel Hasil Perhitungan Enkripsi AES

Round	SubBytes				ShiftRows				MixColumns				AddRoundKey			
0													A5	02	AF	1A
													45	CE	81	48
													0C	BE	96	F4
													F8	8B	4F	4D
1	27	6A	98	87	27	6A	98	87	D7	95	C6	23	D7	95	C6	23
	B1	C4	C7	AB	C4	C7	AB	AB	C7	CE	C2	31	C7	CE	C2	31
	0E	95	D3	11	D3	11	0E	11	79	89	20	BA	79	89	20	BA
	02	05	6B	1D	1D	02	05	1D	44	6C	1C	60	44	6C	1C	60
2	0E	2A	B4	26	0E	2A	B4	26	FD	D4	C7	26	21	50	E8	E2

	C6	8B	25	C7	8B	25	C7	C6	11	7C	B0	DF	A9	5C	E7	86
	B6	A7	B7	F4	B7	F4	B6	A7	9B	D1	F4	0A	D0	7D	F1	EC
	1B	50	9C	D0	D0	1B	50	9C	95	99	16	28	7C	00	8B	6A
3	FD	53	9B	98	FD	53	9B	98	9C	DF	F2	87	80	C3	EE	9B
	D3	4A	94	44	4A	94	44	D3	93	39	E0	02	58	F2	2B	C9
	70	FF	A1	CE	A1	CE	70	FF	E8	70	9A	E9	66	FE	14	67
	10	63	3D	02	02	10	63	3D	F3	8F	44	E5	DF	A3	68	C9
4	CD	2E	28	14	CD	2E	28	14	26	4F	15	68	E7	0A	7F	C6
	6A	89	F1	DD	89	F1	DD	6A	0C	DD	D6	53	AD	5C	00	DC
	33	BB	FA	85	FA	85	33	BB	D7	77	8D	DC	ED	E1	1E	A9
	9E	0A	45	DD	DD	9E	0A	45	9E	21	82	67	EB	CD	F3	54
5	94	67	D2	B4	94	67	D2	B4	BF	51	C6	22	47	B5	3E	C6
	95	4A	63	86	4A	63	86	95	B6	26	87	9B	0E	55	3F	E8
	44	F8	72	D3	72	D3	55	F8	5A	99	22	DD	49	04	31	40
	E9	BD	0D	20	20	E9	BD	0D	DF	D0	DF	B0	30	13	30	73
6	A0	D5	B2	B4	A0	D5	B2	B4	0C	23	8F	63	46	2C	EA	A8
	AB	FC	75	9B	FC	75	98	AB	9E	20	AF	F0	61	5E	07	D7
	3B	F2	C7	09	C7	09	3B	F2	43	BE	D8	EC	57	3C	C9	88
	04	7D	04	8F	8F	04	7D	04	C5	10	97	96	D9	E0	16	24
7	5A	71	87	C2	5A	71	87	C2	B7	47	BD	19	50	44	46	06
	EF	58	C5	0E	58	C5	0E	EF	A0	82	97	66	D4	85	28	AA
	5B	EB	DD	C4	DD	C4	58	EB	F9	78	07	29	A9	B5	D9	6A
	35	E1	47	36	36	35	E1	47	07	F8	1E	D7	DF	E3	EA	E0
8	53	1B	5A	6F	53	1B	5A	6F	D0	F6	99	54	D9	F0	FA	FC
	48	97	34	AC	97	34	AC	48	D8	EB	66	1C	3D	70	55	08
	D3	D5	35	02	35	02	D3	D5	96	92	78	04	18	9E	65	7D
	9E	11	87	E1	E1	9E	11	87	8E	3C	B3	39	52	10	1E	26
9	35	8C	2D	B0	35	8C	2D	B0	23	E3	6D	6B	06	C5	B0	A9
	27	51	FC	30	51	FC	30	27	B7	75	6B	91	39	FC	BD	6B
	AD	0B	4D	FF	4D	FF	AD	0B	FC	95	19	17	1A	BE	EC	A1
	00	CA	72	F7	F7	00	CA	72	B6	8C	65	03	AE	8F	92	C3
10	6F	A6	E7	D3	6F	A6	E7	D3	F5	55	85	6A	C1	67	D4	93
	12	B0	4C	7F	B0	4C	7F	12	73	8C	97	51	D8	BC	94	46
	A2	AE	CE	32	CE	32	A2	AE	2A	B9	52	57	1E	81	77	0B
	E4	73	4F	2E	2E	E4	73	4F	93	5C	09	4C	6A	89	71	2B
11	6F	A6	E7	D3	6F	A6	E7	D3	F5	55	86	6A	C1	67	D4	93
	12	B0	4C	7F	B0	4C	7F	12	73	8C	97	51	D8	BC	94	46
	A2	AE	CE	32	CE	32	A2	AE	2A	B9	52	57	1E	81	77	0B
	E4	73	4F	2E	2E	E4	73	4F	93	5C	09	4C	6A	89	71	2B
12	94	1C	CE	E5	94	1C	CE	E5	C8	EA	C1	FD	3E	2E	54	91
	12	3B	FE	4F	3B	FE	4F	12	24	9D	63	79	93	1A	E7	EA

	52	51	38	DB	38	DB	52	51	56	7F	71	88	B1	A0	8B	2E
	10	C5	4B	8E	8E	10	C5	4B	A3	21	C5	E1	CD	9A	06	45
13	B2	31	20	81	B2	31	20	81	D1	49	A2	E9	3D	3F	93	5D
	DC	A2	94	87	A2	94	87	DC	C4	EC	CE	76	66	B9	5A	D9
	C8	E0	3D	31	3D	31	C8	E0	D8	1B	FF	37	50	14	82	8E
	BD	B8	6F	6E	6E	BD	B8	6F	8E	97	44	7A	5A	DD	67	F0
14	27	75	DC	4C	27	75	DC	4C					DF	E4	A9	F1
	33	56	BE	35	56	BE	35	33					4A	59	E3	18
	53	FA	13	19	13	19	53	FA					9A	CF	02	90
	BE	C1	85	8C	8C	BE	C1	85					3C	F6	CC	9C

Hasil di atas merupakan perhitungan dari baris pertama hexadecimal yang berdasarkan citra yang digunakan. Kemudian apabila telah berhasil melakukan perhitungan untuk setiap barisnya maka akan diperoleh hasil sebagai berikut:



Gambar *8* Barisan Hexadecimal Hasil Enkripsi

Kemudian setelah dilakukan proses Enkripsi dilaksanakan proses kompresi dengan algoritma LZW. Analisis bagaimana cara kerja dari algoritma kompresi LZW adalah sebagai berikut:

1. Kompresi LZW memakai tabel kode, menggunakan 4096 menjadi pilihan generik buat jemlah entri tabel. Kode 0 hingga 255 pada tabel kode selalu ditugaskan buat mewakili byte tunggal berdasarkan arsip input.
2. Ketika dimulai proses encoding, tabelo kode hanya diisi 256 entri pertama, menggunakan residu tabel yg kosong. Kompresi bisa dicapai menggunakan memakai kode 256 sampai 4095 buat mewakili urutan byte.
3. Ketika proses encoding berlanjut, LZW mengidentifikasi urutan berulang pada data, & menambahkannya ke tabel kode.
4. Proses decoding dicapai menggunakan merogoh setiap kode berdasarkan arsip terkompresi & menerjemahkannya melalui table kode buat menemukan karakter atau karakter yg diwakilinya.

ASCII Code: Character to Binary

0	0011 0000	O	0100 1111	m	0110 1101
1	0011 0001	P	0101 0000	n	0110 1110
2	0011 0010	Q	0101 0001	o	0110 1111
3	0011 0011	R	0101 0010	p	0111 0000
4	0011 0100	S	0101 0011	q	0111 0001
5	0011 0101	T	0101 0100	r	0111 0010
6	0011 0110	U	0101 0101	s	0111 0011
7	0011 0111	V	0101 0110	t	0111 0100
8	0011 1000	W	0101 0111	u	0111 0101
9	0011 1001	X	0101 1000	v	0111 0110
A	0100 0001	Y	0101 1001	w	0111 0111
B	0100 0010	Z	0101 1010	x	0111 1000
C	0100 0011	a	0110 0001	y	0111 1001
D	0100 0100	b	0110 0010	z	0111 1010
E	0100 0101	c	0110 0011	.	0010 1110
F	0100 0110	d	0110 0100	,	0010 0111
G	0100 0111	e	0110 0101	:	0011 1010
H	0100 1000	f	0110 0110	;	0011 1011
I	0100 1001	g	0110 0111	?	0011 1111
J	0100 1010	h	0110 1000	!	0010 0001
K	0100 1011	I	0110 1001	'	0010 1100
L	0100 1100	j	0110 1010	"	0010 0010
M	0100 1101	k	0110 1011	(	0010 1000
N	0100 1110	l	0110 1100	)	0010 1001
				space	0010 0000

Gambar 9 Tabel ASCII 1

ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Gambar 10 Tabel ASCII 2

Sebelum melakukan proses perhitungan, gambar yang ngin dikompresi akan diubah terlebih dahulu ke dalam bentuk Base64 agar dapat menghasilkan string atau text supaya bisa dilakukan perhitungan.

Contoh String Karakter yang diambil dari gambar adalah sebanyak 25 karakter awal yang terdapat di gambar:

9j4AAQSkZJRgABAQAAAQABAAD

Dari karakter diatas apabila dijadikan bilangan biner yang dimana setiap karakter mewakili 8 bit atau 1 byte maka akan menjadi total sebanyak 200 bits

Berikut adalah hasil perhitungan LZW pada string diatas tersebut.

Tabel 4.4 Hasil Perhitungan Kompresi LZW

Contoh String 9j4AAQSkZJRgABAQAAAQABAAD			
Current	Next	Output	Add to Dictionary
9057	j106	9057	9j256
j106	4052	j106	j4257
4052	A065	4052	4A258
A065	A065	A065	AA258
A065	Q081	A065	AQ259
Q081	S083	Q081	QS260
S083	k107	S083	Sk261
k107	Z090	k107	kZ262
Z090	J074	Z090	ZJ263
J074	R082	J074	JR264
R082	g103	R082	Rg265
g103	A065	g103	gA266
A065	B066	A065	AB267
B066	A065	B066	BA268
A065	Q081	sudah ada di dictionary	
AQ259	A065	AQ259	AQA269
A065	A065	sudah ada di dictionary	
AA258	A065	AA258	AAA270
A065	Q081	sudah ada di dictionary	
AQ259	A065	sudah ada di dictionary	
AQA269	B066	AQA269	AQAB271
B066	A065	sudah ada di dictionary	
BA268	A065	BA268	BAA272
A065	D068	A065	AD273
D068	-	D068	-

Pada string awal yang memiliki 200 bits kemudian setelah dilakukan proses kompresi LZW ukuran dari string tersebut sekarang hanya menjadi 164 bits dimana 200 bits dikurang 164 bits adalah sama dengan 36 bits atau mengalami penyusutan sebanyak 18 persen.

Kemudian untuk selanjutnya adalah analisi proses dari decoding atau dekompresi algoritma kompresi LZW. Cara untuk melakukan proses

dekompresi sama dengan proses kompresi hanya proses kebalikan dari kompresi tersebut. Setelah melakukan proses didapat bilangan ASCII yaitu sebagai berikut:

057 106 052 065 065 081 083 107 090 074 082 103 065 066 259 258 269 268 065 068

Setelah mengetahui hasil dari ASCII tersebut maka dapat dilakukan perhitungan LZW untuk decoding yaitu sebagai berikut:

Tabel 4.5 Hasil Perhitungan Dekompresi LZW

Current	Next	Output	Add to Dictionary
057	106	057	057 106 (256)
106	052	106	106 052 (257)
052	065	052	052 065 (258)
065	065	065	065 065 (259)
065	081	065	065 081 (260)
081	083	081	081 083 (261)
083	107	083	083 107 (262)
107	090	107	107 090 (263)
090	074	090	090 074 (264)
074	082	074	074 082 (265)
082	103	082	082 103 (266)
103	065	103	103 065 (267)
065	066	065	065 066 (268)
066	259	066	066 065 081 (269)
259	258	065 081	065 081 065 065 (270)
258	269	065 065	065 065 065 081 065 (271)
269	268	065 081 065	065 081 065 066 065 (272)
268	065	066 065	066 065 065(273)
065	068	065	065 (274)
068	-	068	-

Setelah dilakukan proses decoding maka akan didapatkan deret bilang ASCII yaitu adalah sebagai berikut :

057 106 052 065 065 081 083 107 090 074 082 103 065 066 065 081 065 065 065 081 065 066 065 068

Atau membentuk string karakter:

9j4AAQSkZJRgABAQAAAQABAAD

Kemudian untuk selanjutnya adalah bagaimana cara untuk melakukan Dekripsi dengan menggunakan AES :

1. File diubah ke dalam bentuk byte stream.
2. Kalau 16 byte akhir tidak sampai 16 si dengan null.
3. Byte Stream dipecah 16 byte tiap blok
4. Jalankan proses dekripsi berdasarkan blok pertama yang diubah menjadi array state.
5. Proses :
    a. *InvAddRoundKey*, yaitu XOR dengan key dan cipherteks
    b. InvSubBytes, subtitusi pada tabel reverse S-Box
    c. InvShiftRows, penggeseran lawan arah pada array
    d. InvMixColumns, transfomasi kolom state

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

    e. InvAddRoundKey, yaitu XOR dengan roundkey
    f. Lakukan langka a sampai e selama Nr – 1 kali
    g. Proses akhir jalankan langkah a sampai e tanpa menggunakan MixColumns.
6. Setelah langkah dekripsi 16 byte awal selesai, lakukan 16 byte setelahnya hingga semua blok telah selesai di dekripsi.

Pada proses dekripsi sama seperti halnya dengan enkripsi hanya saja dialkukan proses nvers atau kebalikannya sehingga file hasil enkripsi yang seperti dibawah.

Lenna.jpg.enc Lenna.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  DF 4A 9A 3C E4 59 CF F6 A9 E3 02 CC F1 18 90 9C  ßJš<äYÏö®ã.Ìñ..œ
00000010  93 79 76 B8 FE 92 AE CD 98 02 9C 64 5B 9F 84 88  "yv¸þ'®Í˜.œd[Ÿ„ˆ
00000020  E9 99 FE 7E 6C 2A 28 A7 04 17 91 8D BC 3D 9B AF  é™þ~l*(§..'.¼=›¯
00000030  41 ED 16 66 77 3A C3 E5 DB A5 58 FC E5 DF 7A 3C  Aí.fw:ÃåÛ¥XüåßZ<
00000040  BB F0 C0 53 46 74 79 A4 20 B4 0B 7C F1 F2 28 CB  »ðÀSFty¤ ´.|ñò(Ë
00000050  20 9C 9B 2A EF 38 EF F6 A3 30 55 CA 7C 0B FD 91   œ›*ï8ïö£0UÊ|.ý'
00000060  0B A7 AF 6C 65 3E 50 50 B9 6F 0F 7B 7C 18 63 C3  .§¯le>PP¹o.{|.cÃ
00000070  56 22 74 E0 3C 3D B2 00 43 C9 8F 8C 50 7F 9F A2  V"tà<=².CÉ.ŒP.Ÿ¢
00000080  F3 82 06 61 3D 77 74 72 62 16 12 4A 02 64 B2 A2  ó‚.a=wtrb..J.d²¢
00000090  B8 E6 E5 B3 CE C6 51 EA 76 7B E9 D9 32 8C 22 48  ¸æå³ÎÆQêv{éÙ2Œ"H
000000A0  D7 23 AE FE 27 BB 0B C8 48 FA 1B D8 38 8B 22 36  ×#®þ'».ÈHú.Ø8‹"6
000000B0  3A 7A C3 D5 BE A6 F4 AC 7D 23 F2 15 40 39 C0 14  :zÃÕ¾¦ô¬}#ò.@9À.
000000C0  F9 4A CA 0D 67 4B F0 D5 8C 8A 79 9A ED 18 FA 53  ùJÊ.gKðÕŒŠyší.úS
000000D0  D8 65 31 8C 1C E9 42 2B 22 2C FB 02 6C B8 F9 8C  Øe1Œ.éB+",û.l¸ùŒ
000000E0  BB 15 54 7B D7 5F B5 A2 EE 39 F1 91 53 AA 1E A3  ».T{×_µ¢î9ñ'Sª.£
000000F0  B0 C1 73 ED 04 BE C4 AA D6 A5 6B 3B AF 7B 92 E1  °Ásí.¾ÄªÖ¥k;¯{'á
00000100  F8 ED 2F 75 8F BC 69 9E D2 4D DE 40 8A 62 EA 9A  øí/u.¼ižÒMÞ@Šbêš
00000110  7B 2C 5F BE E1 5F C5 AF 58 45 9F F2 AE 87 A2 BF  {,_¾á_Å¯XEŸò®‡¢¿
00000120  2C 15 6B 6B 8F F9 D6 A5 85 2C C3 FA CD 36 C7 A9  ,.kk.ùÖ¥…,ÃúÍ6Ç©
00000130  E2 2F 14 33 1C C7 E6 67 02 F4 E7 B2 79 9F E5 A9  â/.3.Çæg.ôç²yŸå©
00000140  40 88 A5 12 FA CE A8 FC B0 C5 0F 28 99 C9 7C 45  @ˆ¥.úÎ¨ü°Å.(™É|E
00000150  36 AE 01 E6 0E 75 64 1F 43 4B A5 78 2F 83 93 43  6®.æ.ud.CK¥x/ƒ"C
00000160  43 E9 F9 DE 2C D7 CB 6A 2F 33 2B 44 61 04 A7 A5  CéùÞ,×Ëj/3+Da.§¥
00000170  14 45 01 1E 4E 31 07 2D 66 DB 6E B4 2B A9 AC 75  .E..N1.-fÛn´+©¬u
00000180  30 A3 8E 79 94 72 48 CD 43 F7 3A 81 3D 3B 16 92  0£Ży"rHÍC÷:.=;.'
00000190  EA 4E 9C 6F 31 22 64 AD 38 E0 A8 B5 76 BE 20 0C  êNœo1"d.8à¨µv¾ .
000001A0  91 1C 51 A7 F4 81 B8 BE 18 84 BD 87 83 A8 B1 C7  '.Q§ô.¸¾.„½‡ƒ¨±Ç
000001B0  E6 0A 07 D3 63 DD 91 88 A4 18 63 8B 73 2B 72 98  æ..ÓcÝ'ˆ¤.c‹s+r˜
000001C0  91 54 E2 92 AC DB FD BB 02 74 1C 6A 7F AC 88 88  'Tâ'¬Ûý».t.j.¬ˆˆ
000001D0  FB 4D 77 19 D3 88 AC C8 D4 33 F8 89 F7 9B C8 A1  ûMw.Óˆ¬ÈÔ3ø‰÷›È¡
000001E0  8E 12 78 B8 C3 53 78 39 0B 0D AB 48 5B 2B B6 CA  Ž.x¸ÃSx9..«H[+¶Ê
000001F0  55 C8 5E 0C 22 00 35 7A 07 51 AA AB 71 2A 6B 81  UÈ^.".5z.Qª«q*k.
00000200  0F 48 12 DB C8 83 AE 6C F3 8A 1C 66 F4 07 9D 9B  .H.ÛÈƒ®lóŠ.fô..›
00000210  63 E7 DC EC 0C 5F 74 CF AB 95 DF B4 B3 49 74 DA  cçÜì._tÏ«•ß´³ItÚ
00000220  B8 21 41 1B 82 39 4D 8D 4C E7 E2 8F 54 C3 BF 8F  ¸!A.‚9M.Lçâ.TÃ¿.
00000230  C5 E8 62 0B 2E 06 51 C4 3D 94 17 F3 F0 13 AC DA  Åèb...QÄ=".óð.¬Ú
00000240  5D 86 6B AE AC B0 EF 11 30 6C CA 06 96 47 2C D8  ]†k®¬°ï.0lÊ.–G,Ø
00000250  B4 3D E8 1F 44 66 0C 2B DA D1 6D AA 80 D4 D2 BE  ´=è.Df.+ÚÑmª€ÔÒ¾
00000260  31 D5 34 70 10 FA 9C 83 09 1C 4C 7F C8 9D 0F 85  1Õ4p.úœƒ..L.È.…
```

Gambar 11 Bilangan Hexadecimal yang akan DiDekripsi

DF	E4	A9	F1
4A	59	E3	18
9A	CF	02	90
3C	F6	CC	9C

⊕

BE	DB	28	8A
58	98	E7	70
AB	77	A9	04
EB	0E	E3	DF

=

61	3F	81	7B
12	C1	04	68
31	B8	AB	94
D7	F8	2F	43

Setelah tu akan diubah kembali menjadi ke file aslinya dengan cara yang dijelaskan sebelumnya untuk prosesnya maka perhitungannya akan menjadi seperti berikut:

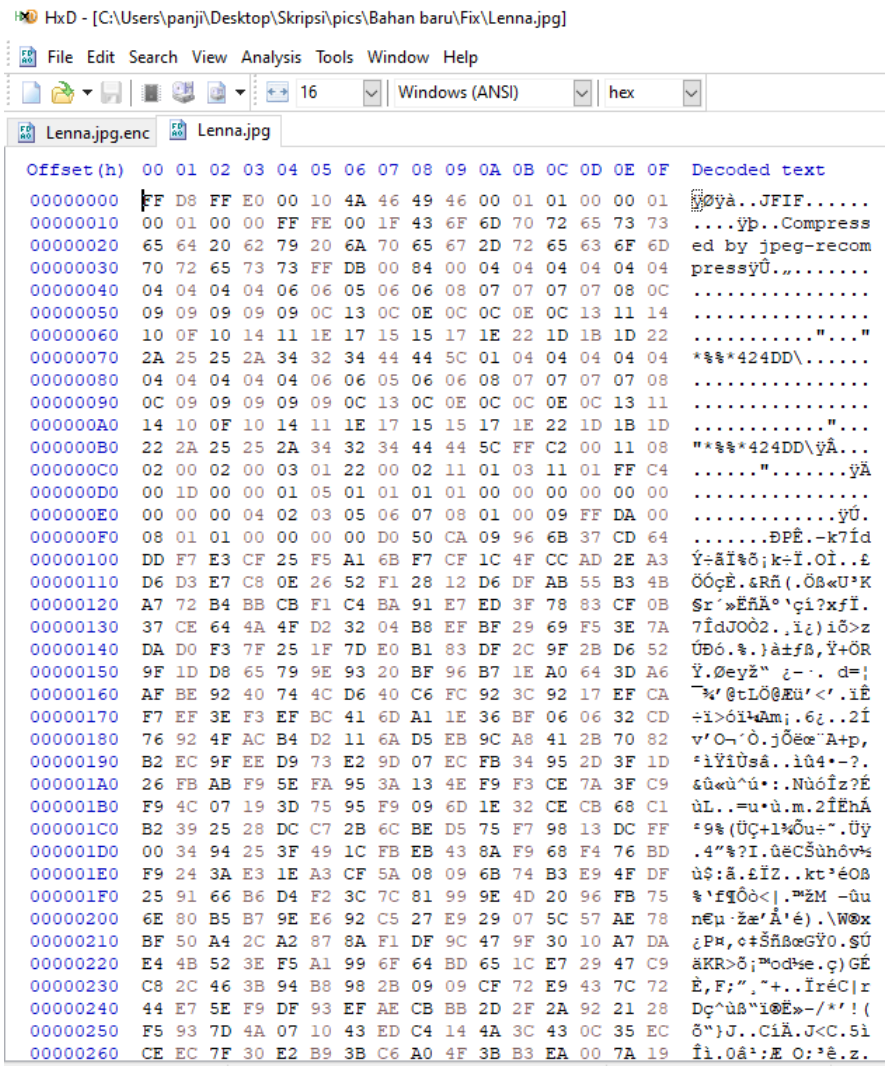
Tabel 4.*6* Hasil Perhitungan Dekompresi AES

Round	InvShiftRows	InvSubBytes	InvMixColumns	InvAddRoundKey
0				FF 00 49 01 D8 10 46 00 FF 4A 00 00 E0 46 01 01
1	96 3C 20 AF	35 6D 54 1B	EF 65 77 A2	35 6D 54 1B

	0A	D9	69	76	A3	E5	E4	0F	78	22	47	81	A3	E5	E4	0F
	FF	60	4F	45	7D	90	92	68	62	8F	37	34	7D	90	92	68
	F2	0B	EF	EC	04	9E	61	83	1A	4E	44	E8	04	9E	61	83
2	07	8C	7C	CA	38	F0	01	10	96	3C	20	AF	E4	84	2E	D4
	F4	0D	7E	95	BA	F3	8A	AD	D9	69	76	0A	02	D3	DD	F4
	D5	F3	62	D3	B5	7E	AB	A9	4F	45	FF	60	FE	D2	AE	4F
	A4	AB	AA	C5	1D	0E	62	07	EC	F2	0B	EF	F4	97	FF	45
3	3A	87	B2	BD	A2	EA	3E	CD	07	8C	7C	CA	BE	F6	22	D1
	D5	A3	3B	B1	B5	71	49	56	0D	7E	95	F4	7E	BA	82	9D
	FA	05	04	C2	14	36	30	A8	62	D3	D5	F3	9A	B8	BE	26
	B9	4C	06	FD	DB	5D	A5	21	C5	A4	AB	AA	F7	71	89	0D
4	37	33	7F	C2	B2	66	6B	A8	3A	87	B2	BD	73	23	01	06
	9A	22	1B	7E	37	94	44	8A	A3	3B	B1	D5	96	15	92	05
	A9	4D	62	A4	B7	65	AB	1D	04	C2	FA	05	8D	F3	38	68
	FF	28	A8	C3	7D	EE	6F	33	FD	B9	4C	06	08	02	1E	00
5	D1	BF	6B	F1	51	F4	05	2B	37	33	7F	C2	A9	10	FD	CF
	E4	F3	0D	F8	AE	7E	F3	E1	22	1B	7E	9A	16	0D	4B	92
	DE	B0	26	65	9C	FC	23	BC	62	A4	A9	4D	8F	61	30	21
	7F	4B	1E	77	6B	CC	E9	02	C3	FF	28	A8	84	0F	06	C1
6	91	85	96	62	AC	67	35	AB	D1	BF	6B	F1	E6	68	50	60
	8B	2B	A2	70	CE	0B	1A	D0	F3	0D	F8	E4	31	75	B2	F7
	11	21	41	34	E3	7B	F8	28	26	65	DE	B0	F7	F9	E9	4C
	84	65	64	B5	4F	BC	8C	D2	77	7F	4B	1E	53	4C	0D	60
7	5B	CF	34	AD	57	5F	28	18	91	85	96	62	B0	5C	D3	1F
	A6	6B	DB	49	C5	05	9F	A4	2B	A2	70	8B	B1	02	20	CC
	91	59	D5	1B	AC	15	B5	44	41	34	11	21	DFC	D8	6B	43
	7F	67	BB	0D	6B	0A	FE	F3	B5	84	65	64	B3	11	0A	37
8	57	81	F7	2D	DA	91	26	FA	5B	CF	34	AD	D3	97	45	52
	7C	62	BE	AE	01	AB	5A	BE	6B	DB	49	A6	E4	30	69	AA
	AD	79	8C	47	18	AF	F0	16	D5	1B	91	59	96	A3	ED	6F
	2A	6A	94	EF	95	58	E7	61	0D	7F	67	BB	49	74	4A	7E
9	2F	3D	6F	A1	4E	8B	06	F1	57	81	F7	2D	6B	AD	DB	33
	FF	64	63	04	7D	8C	00	30	62	BE	AE	7C	F3	05	36	CA
	2D	69	ED	37	FA	E4	53	B2	8C	47	AD	79	1C	CF	A6	04
	74	05	93	0C	CA	36	22	81	EF	2A	6A	94	D2	35	D5	41
10	CC	E4	62	09	27	AE	AB	40	2F	3D	6F	A1	13	9C	FA	B9
	50	8E	47	21	6C	E6	16	7B	64	63	04	FF	C7	D6	15	6C
	AC	22	AF	F3	AA	94	1B	7E	ED	37	2D	69	9E	AC	3E	22
	D4	31	87	18	19	2E	EA	34	0C	74	05	93	E0	FB	92	53
11	7C	5C	FF	25	01	A7	7D	C2	CC	E3	62	09	BD	3D	3A	47
	A0	A0	75	8F	47	47	3F	73	8E	37	21	50	39	B0	FE	48

	EC	AE	FD	B3	83	BE	21	4B	AF	F3	AC	22	2F	39	53	8F
	2E	E4	B7	03	C3	AE	20	D5	18	D4	31	87	5E	30	49	7C
12	2B	F3	89	1C	0B	7E	F2	C4	7C	5C	FF	25	FD	BA	67	A8
	73	3E	D5	6D	8F	D1	B5	B3	A0	75	8F	A0	38	56	31	20
	9E	99	F3	24	DF	F9	7E	A6	FD	B3	EC	AE	38	26	84	00
	C8	A6	F9	E7	B1	C5	69	B0	03	2E	E4	B7	DFC	7E	AA	14
13	CE	7B	A9	B6	EC	03	B7	79	2B	F3	89	1C	00	75	86	CD
	9C	6D	61	9C	1C	B3	D8	1C	3E	D5	6D	73	BE	E6	4C	B3
	00	93	84	DF	52	22	4F	EF	F3	24	9E	99	DA	2D	32	56
	C8	B2	C5	95	B1	3E	07	AD	E7	C8	A6	F9	65	74	24	27
14	EF	65	77	A2	61	BC	02	1A					61	BC	02	1A
	81	78	22	47	91	C1	94	16					91	C1	94	16
	37	34	62	8F	B2	28	AB	73					B2	28	AB	73
	4E	44	E8	1A	B6	86	C8	43					B6	86	C8	43

Sehingga hasil dari keseluruhan akan menjadi ke gambar aslinya seperti semula dan pada gambar di bawah ditampilkan bilangan hexadecimal dari gambar tersebut:



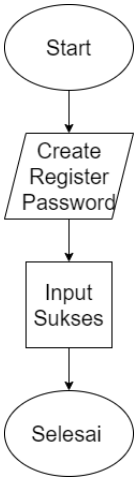
Gambar 12 Bilangan Hexadecimal setelah Di dekripsi

4.3. Flow Chart, Use Case, dan Class Diagram Aplikasi

Pada subbab ini akan dijelaskan alur keseluruhan program yang akan dijalankan Adapun didalamnya memuat *Flowchart*, *use case*, dan *class diagram*.

4.3.1. *Flowchart* Register

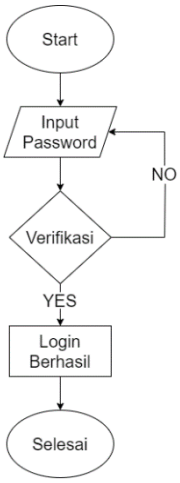
Berikut merupakan alur yang dibentuk dalam bentuk diagram yang menggambarkan proses algoritma dari register yang digambarkan dengan *Flowchart* sebagai berikut:



Gambar 4.13 Flowchart Register

4.3.2. *Flowchart* Login

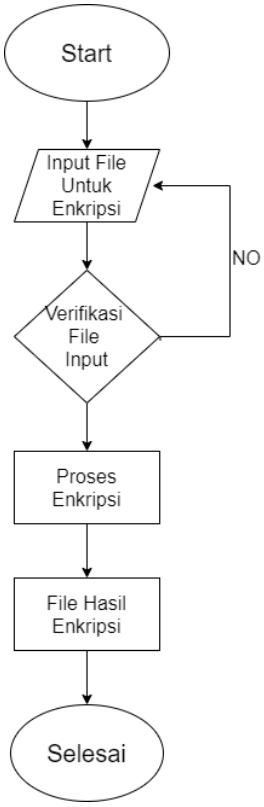
Berikut merupakan alur yang dibentuk dalam bentuk diagram yang menggambarkan proses algoritma dari login yang digambarkan dengan *Flowchart* sebagai berikut:



Gambar 4.14 Flowchart Login

4.3.3. *Flowchart* Enkripsi File

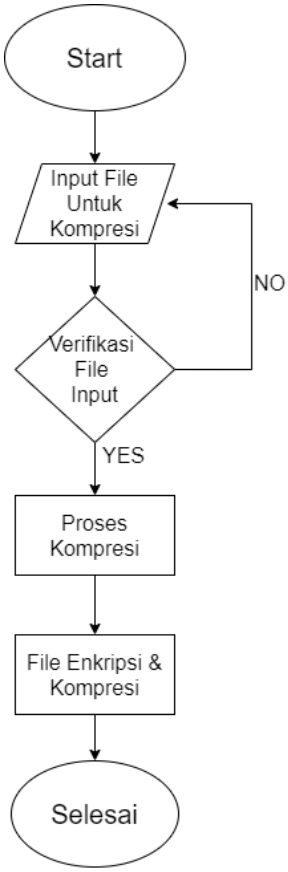
Berikut merupakan alur yang dibentuk dalam bentuk diagram yang menggambarkan proses algoritma dari enkripsi file dengan bertipe citra dengan menggunakan algoritma AES (*Advanced Encryption Standard*) yang digambarkan dengan *Flowchart* sebagai berikut:



Gambar 4.15 Flowchart Enkripsi

4.3.4. *Flowchart* Kompresi File

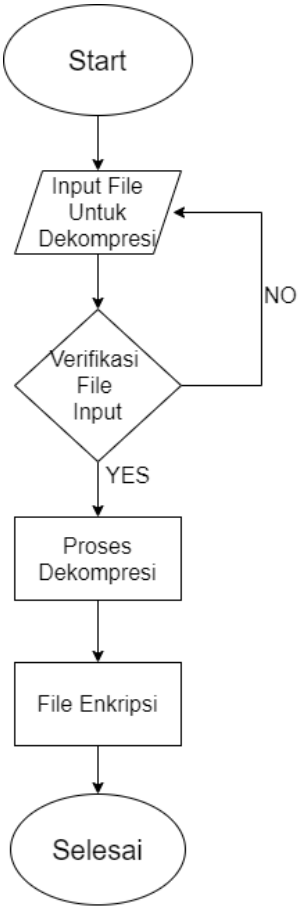
Berikut merupakan alur yang dibentuk diagram yang menggambarkan proses algoritma dari kompresi file dengan bertipe citra menggunakan algoritma LZW (*Lempel Ziv Welch*) yang digambarkan dengan *Flowchart* sebagai berikut:



Gambar 4.16 Flowchart Kompresi

4.3.5. *Flowchart* Dekompresi File

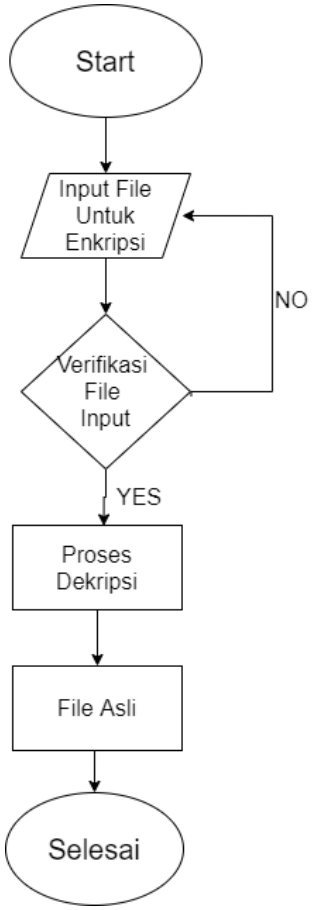
Berikut merupakan alur yang dibentuk diagram yang menggambarkan proses algoritma dari dekompresi file dengan bertipe citra menggunakan algoritma LZW (*Lempel Ziv Welch*) yang digambarkan dengan *Flowchart* sebagai berikut:



Gambar 4.17 Flowchart Dekompresi

4.3.6. *Flowchart* Dekripsi File

Berikut merupakan alur yang dibentuk diagram yang menggambarkan proses algoritma dari decompress file dengan bertipe citra menggunakan algoritma AES (Advacned Encryption Standard) yang digambarkan dengan *Flowchart* berikut:

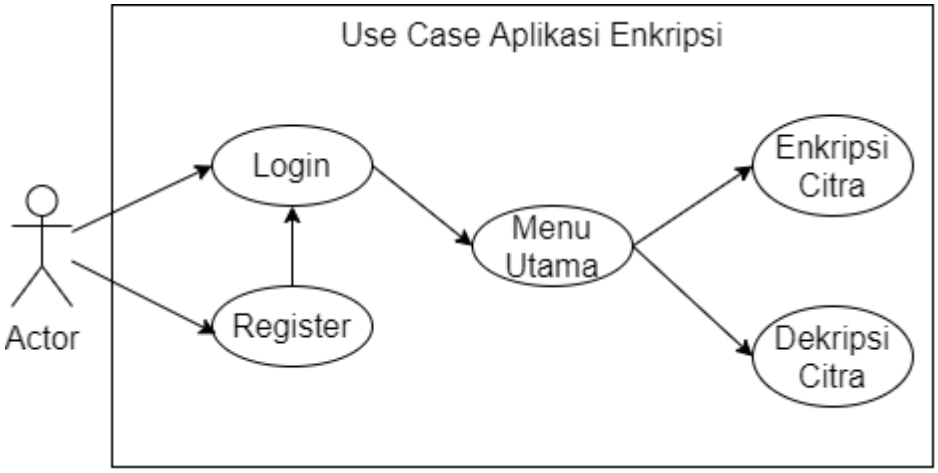


Gambar 4.18 Flowchart Dekripsi

4.3.7. Use Case Aplikasi

Berikut diagram use case untuk menjelaskan fungsi – fungsi yang berada di dalam sistem dan actor apa saja yang terlibat dalam fungsi tersebut. Dalam penelitian karena aplikasi untuk pengamanan data dan pemapatan data dilakukan dengan dua aplikasi yang berbeda, maka memiliki dua use case aplikasi yaitu sebagai berikut :

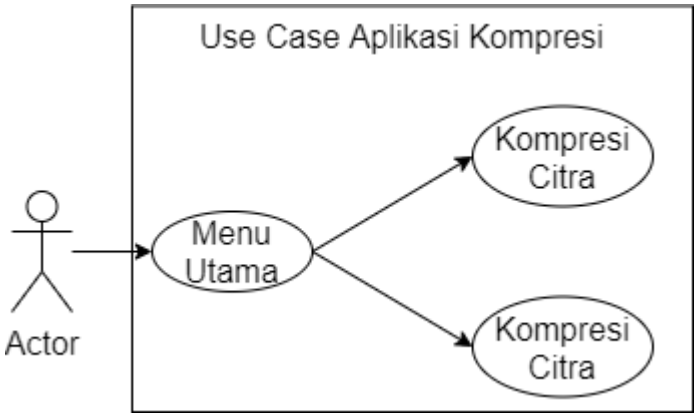
A. Use Case Aplikasi Enkripsi dan Dekripsi



Gambar 4.*19* Use Case Aplikasi Enkripsi dan Dekripsi

Pada tahap awal user akan masuk ke dalam sistem dan langsung ke halaman login apabila user sudah memiliki akun, namun apabila user tidak memiliki akun dan aplikasi membaca tidak ada akun yang terdaftar maka aplikasi akan langsung menyuruh user untuk membuat akun. Setelah proses login maka user akan langsung dibawa ke halaman utama. Dalam menu utama user dapat melakukan enkripsi dan dekripsi data. Dalam melakukan proses enkripsi dan dekripsi data diperlukan kunci yang juga merupakan *password* dari akun user tersebut. Dalam proses kunci terdapat dua operasi saja yaitu, enkripsi dan dekripsi.

B. Use Case Aplikasi Kompresi dan Dekompresi



Gambar 4.20 Use Case Aplikasi Kompresi dan Dekompresi

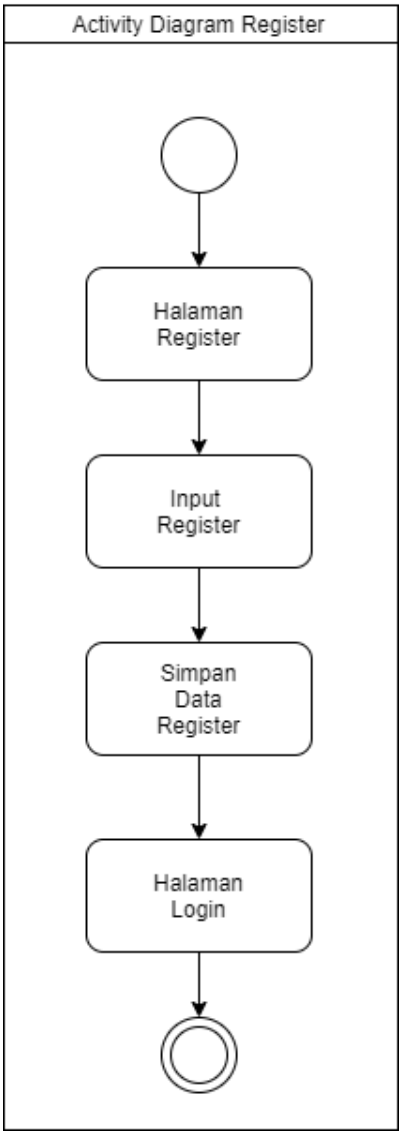
Pada tahap selanjutnya setelah user melakukan enkripsi dan dekripsi citra, user baru bisa melakukan kompresi dan dekompresi citra. User akan langsung dibawa ke menu utama aplikasi dan hanya memasukkan syntax ke dalam aplikasi untuk langsung melakukan kompresi dan dekompresi citra. Dalam proses hanya terdapat dua operasi yaitu kompresi dan dekompresi citra.

4.3.8. Activity Diagram

Activity Diagram adalah gambaran sebuah rancangan atau aktivitas pada sevuah sistem, dimana activity diagram dapat membantu memahami proses secara keseluruhan. Pada penelitian sistem, activity diagram dibagi menjadi enam bagian yaitu sebagai berikut :

A. *Activity Diagram Register*

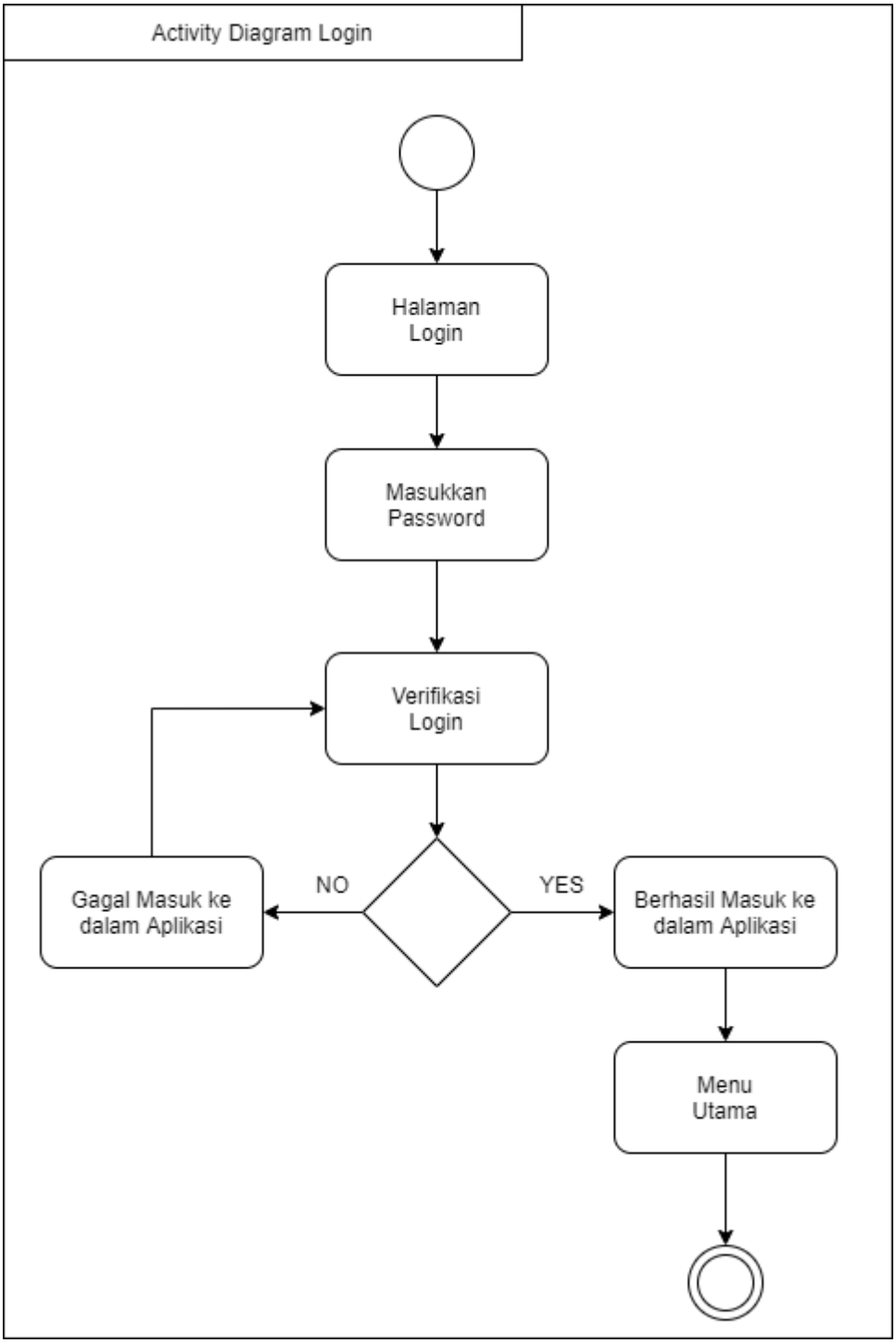
Dalam proses registrasi atau pendaftaran pengguna baru dapat dijelaskan melalui diagram di bawah. Sebelum user masuk ke aplikasi atau program, pertama kali user harus hak akses karena awal masuk ke aplikasi langsung masuk ke halaman register apabila belum ada yang terdaftar di aplikasi. Setelah berhasil daftar untuk mendapatkan hak akses maka user dapat melakukan login dan langsung ke menu utama.



Gambar 4.*21* Activity Diagram Register

B. Activity Diagram Login

Activity diagram login menjelaskan proses setelah melakukan register atau registrasi dan sudah memiliki hak akses. Pada proses login user yang sudah memiliki hak akses diminta untuk memasukkan password yang sekaligus merupakan kunci public untuk melakukan proses enkripsi dan dekripsi. Apabila berhasil di validasi maka program akan lanjut menuju ke halaman utama, namun apabila gagal di validasi maka program akan berhenti di halaman login saja seperti yang terdapat di diagram bawah.

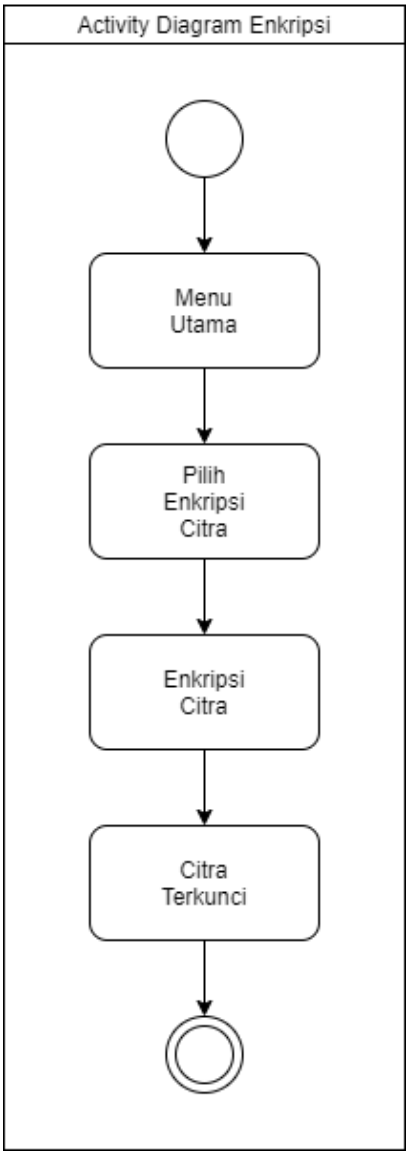


Gambar 4.22 Activity Diagram Login

C. *Activity Diagram* Enkripsi

Activity diagram enkripsi merupakan rangkaian proses enkripsi citra yaitu berupa data dengan berjenis file gambar dan

memiliki ekstensi .jpg dan .png. Pada menu utama user dapat melakukan npu citra yang akan di enkripsi Setelah selesai file tersebut akan menjadi file dengan berformat penguncian (.enc) dimana merupakan hasil dari proses enkripsi dengan menggunakan algoritma kriptografi AES (*Advanced Encryption Standard*) sebanyak 256 bit yang digunakan pada penelitian.

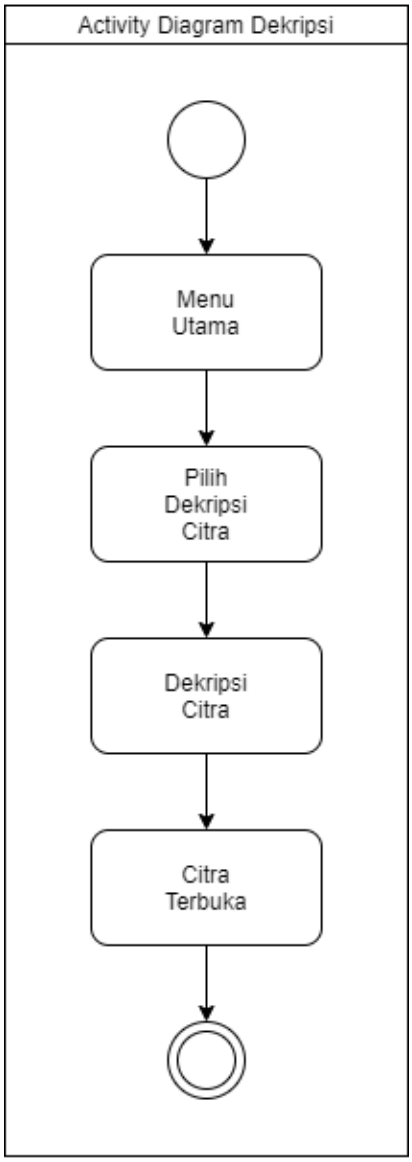


Gambar 4.*23* Activity Diagram Enkripsi

D. *Activity Diagram* Dekripsi

Pada proses dekripsi sama dengan proses enkripsi karena merupakan proses sebaliknya dari merubah file yang sudah

dienkripsi menjadi file awal. Setelah user memilih untuk proses dekripsi maka file yang sudah dienkripsi akan berubah menjadi file awal. Dengan menggunakan algoritma yang sama dengan enkripsi yaitu AES (Advacned Encryption Standard) sebanyak 256 bit yang digunakan pada proses.

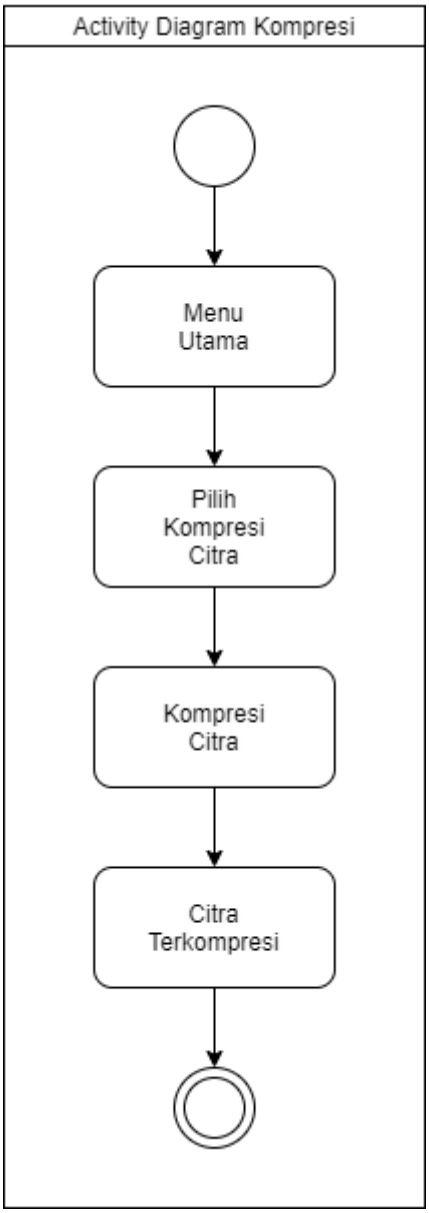


Gambar 4.24 Activity Diagram Dekripsi

E. *Activity Diagram* Kompresi

Activity diagram kompresi menjelaskan proses dimana kompresi akan dilakukan apabila proses enkripsi telah

dilaksanakan. Kompresi dilakukan untuk memperkecil atau mengurangi ukuran dari citra, pada proses kompresi user tidak diminta untuk memasukkan kunci apapun. Proses kompresi menggunakan algoritma LZW (Lempel-Ziv-Welch).

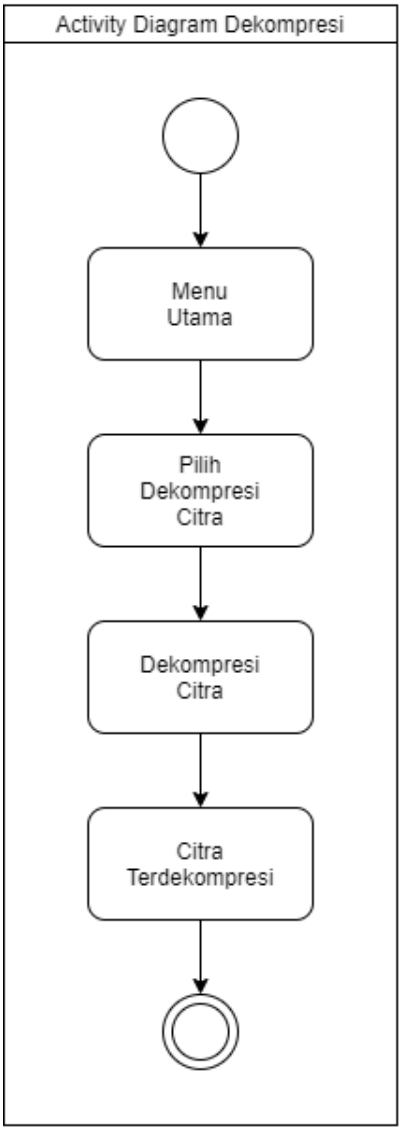


Gambar 4.*25* Activity Diagram Kompresi

F. *Activity Diagram* Dekompresi

Activity diagram dekompresi merupakan prises kebalikan dari proses kompresi, proses dekompresi memiliki tujuan untuk mengembalikkan file citra yang sudah dilakukan pengecilan atau

pengurangan ukuran file. Proses memasukkan file sebelumnya berformat kompresi menjadi berformat enkripsi. Proses dekompresi menggunakan algoritma LZW (Lempel-Ziv-Welch).



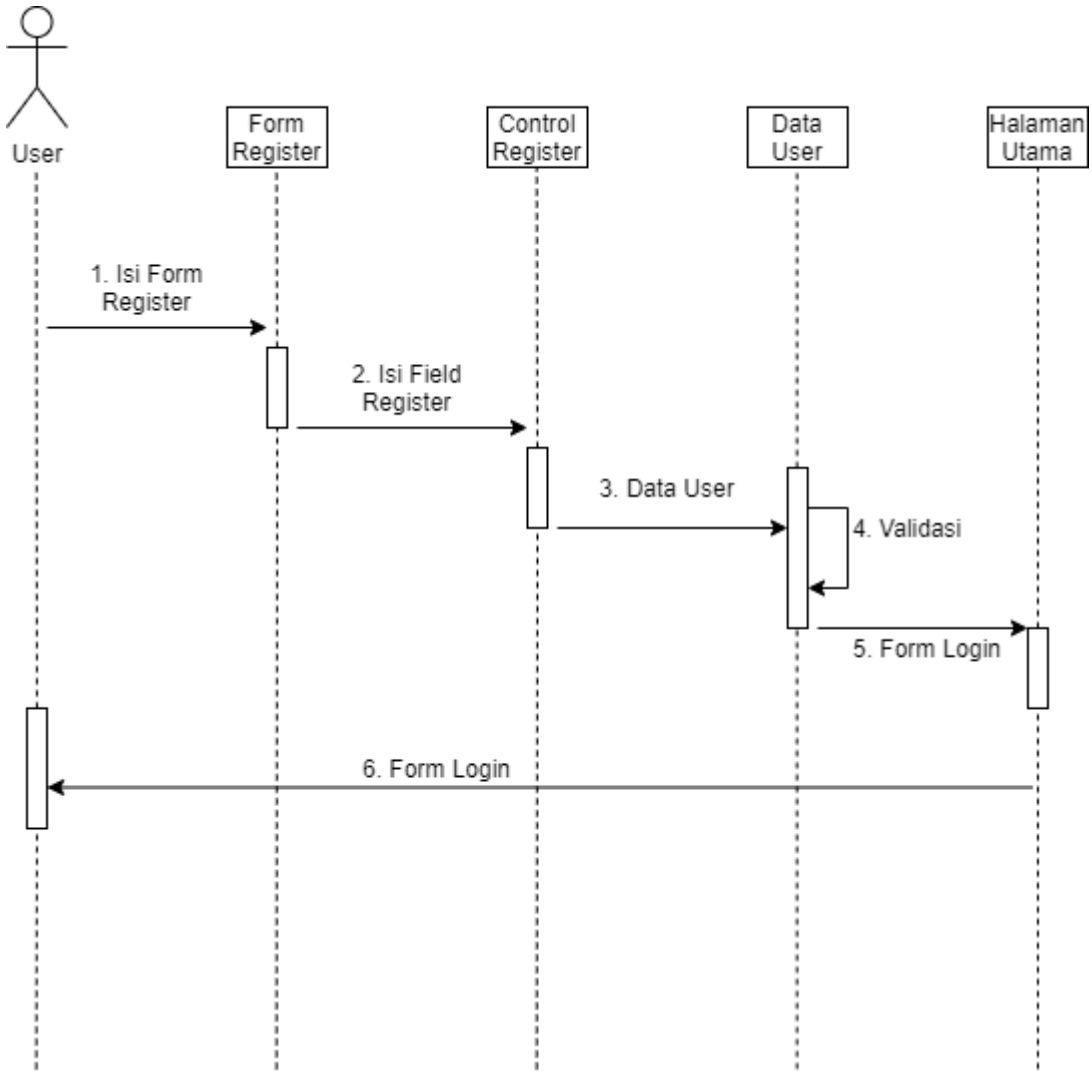
Gambar 4.26 Activity Diagram Dekompresi

4.3.9. Sequence Diagram

Sequence Diagram merupakan diagram yang menjelaskan urutan komunikasi dan nteraksi antar sesame objek lainnya dan diatur dalam suatu urutan waktu. Dalam mplementasi sistem yang di buat penelitian sequence diagram terbagi menjadi beberapa bagian yaitu sebagai berikut :

A. Sequence Diagram *Register*

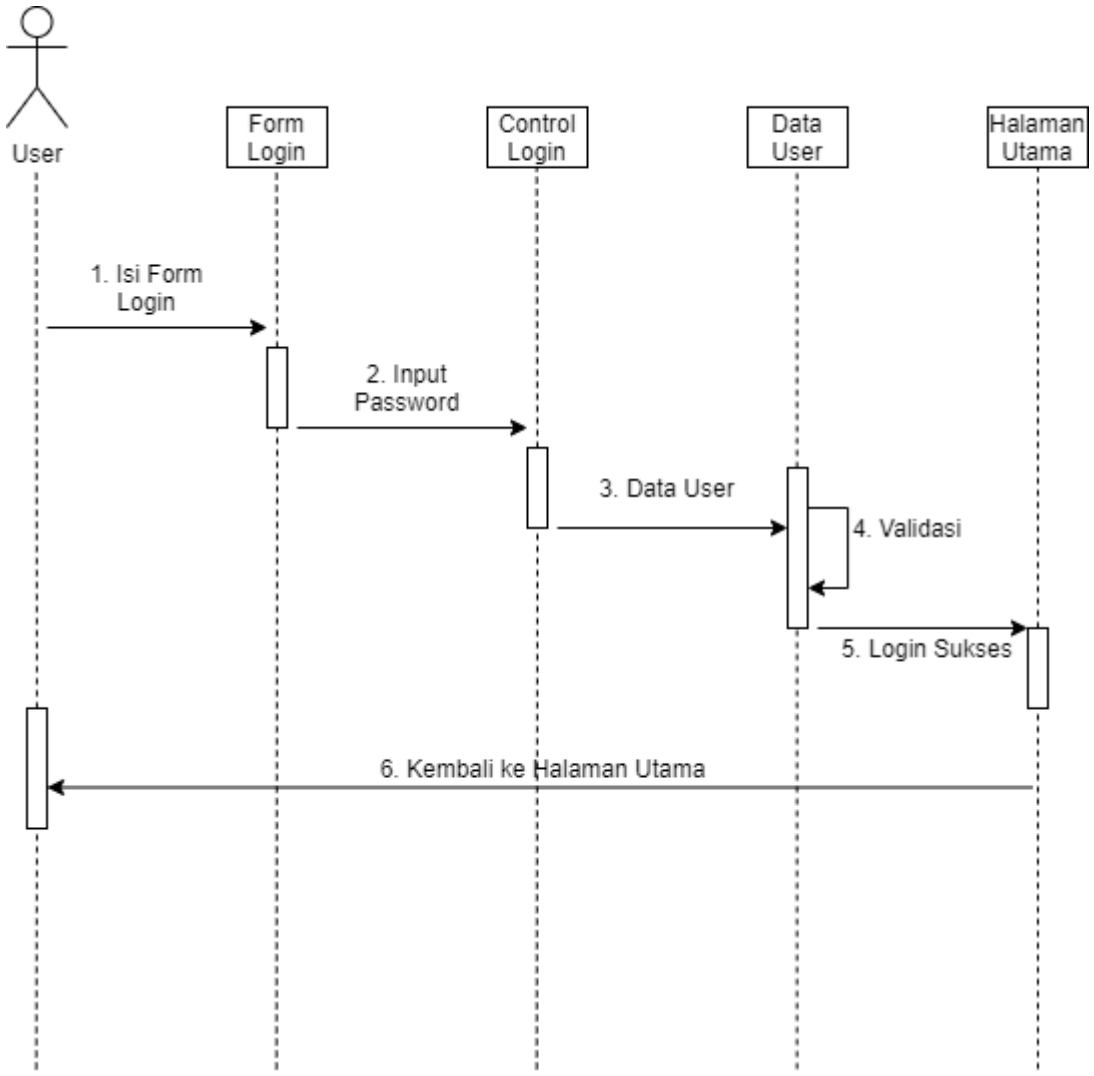
Sequence diagram register menejelaskan nteraksi dan komunikasi apa saja yang terjadi antara suatu objek dengan objek lainnya saat user pertama kali melakukan akses ke dalam aplikasi. Pada awal melakukkan akses user akan diarahkan ke halaman register apabila aplikasi tidak membaca ada user yang memiliki hak akses untuk menggunakan aplikasi tersebut. Jadi user harus melakukan registrasi terlebih dahulu untuk mendapatkan hak akses dengan mengisi password yang sekaligus nanti akan digunakan sebagai kunci public untuk proses enkripsi. Setelah berhasil melakukan proses registrasi data user akan tersimpan di dalam program. Setelah terseimpan maka user sudah bisa mendapatkan hak akses untuk menjalankan aplikasi dan masuk ke dalam aplikasi.



Gambar 4.27 Sequence Diagram Register

B. Sequence Diagram *Login*

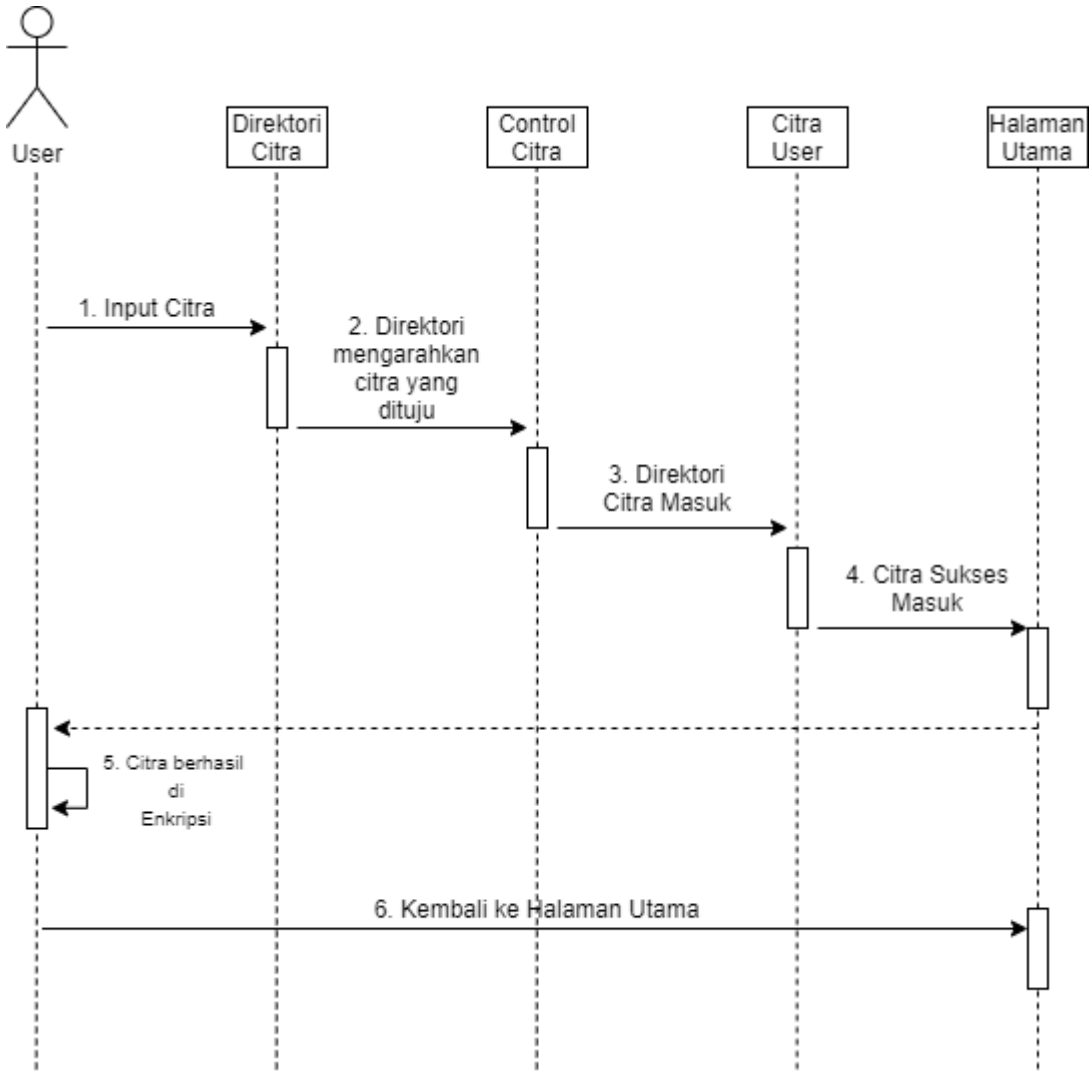
Sequence diagram login menjelaskan nteraksi dalam proses login, user yang melakukan akses halaman login untuk lanjut ke halaman utama. Proses login baru bisa dilakukan apabila user sudah memiliki password yang sudah terdaftar dalam aplikasi, jika belum maka harus melakukan registrasi. Pada proses login akan divalidasi password yang diinput oleh user apakah cocok dengan yang ada di dalam aplikasi, dengan begitu aplikasi akan memberikan hak akses kepada user tersebut untuk menuju ke halaman utama.



Gambar 4.28 Sequence Diagram Login

C. *Sequence Diagram* Enkripsi

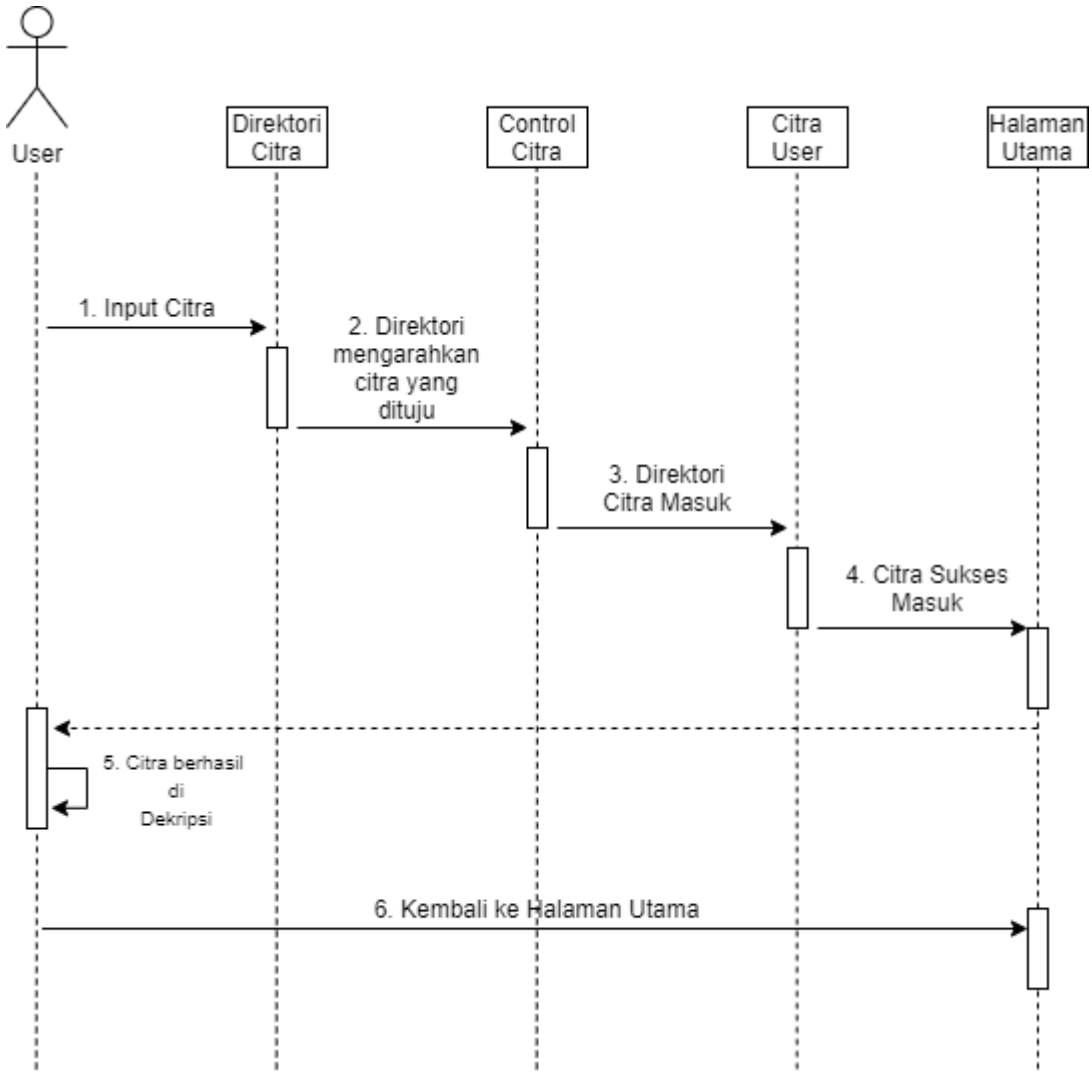
Sequence diagram enkripsi disini menjelaskan nteraksi dalam proses pengamana file citra. Pada proses user yang menjadi pihak berwenang dan memiliki akses untuk melakukan proses pengamanan dan pembukaan nanti. Hal tersebut terjadi karena user yang sudah masuk memiliki hak akses untuk melakukan proses tersebut. Pada proses ini user juga dapat memilih file yang akan dituju dan kemudian dapat dilakukan pengaman terhadap file yang dituju.



Gambar 4.29 Sequence Diagram Enkripsi

D. *Sequence Diagram* Dekripsi

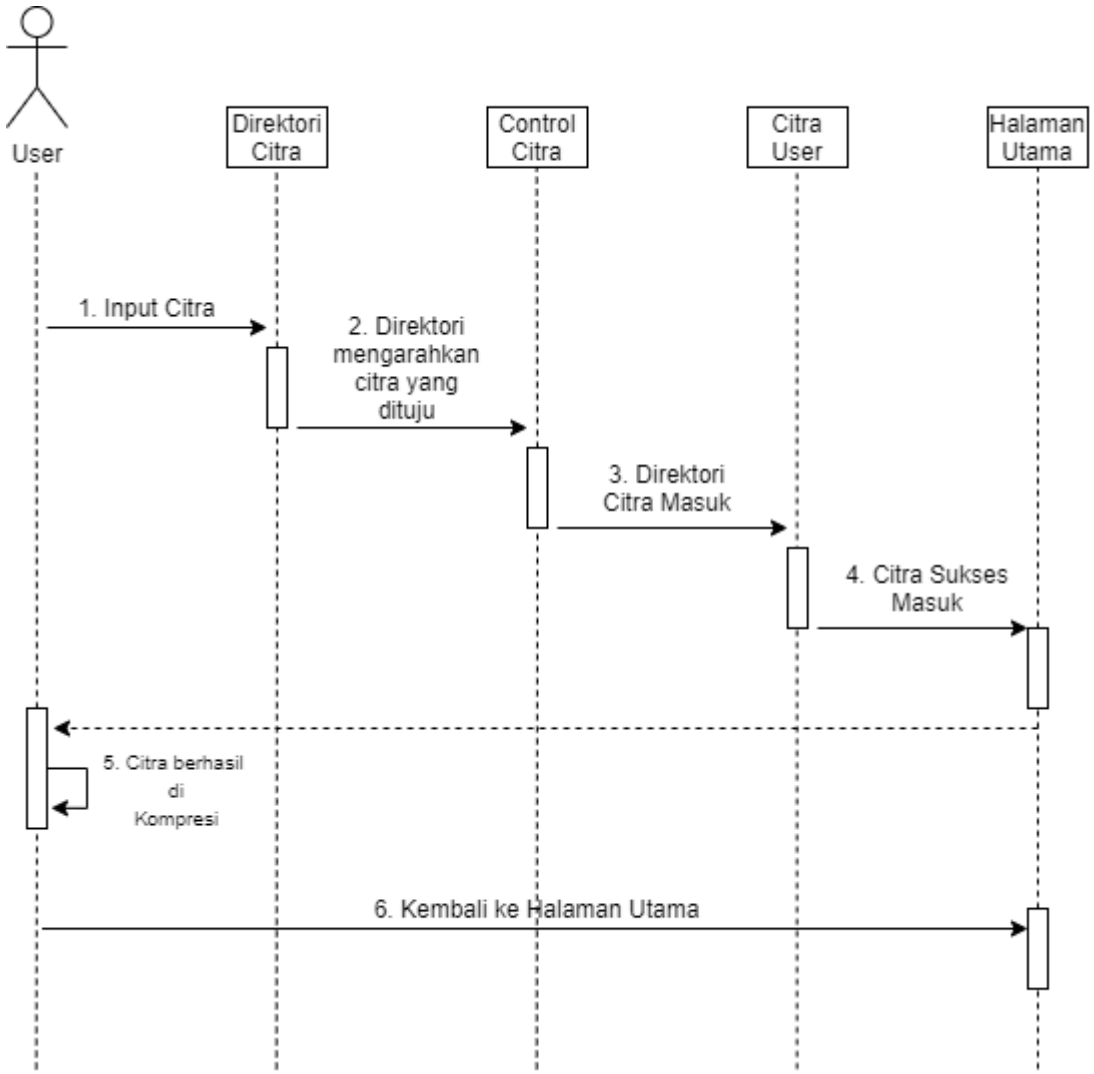
Sequence diagram dekripsi merupakan kebalikan dari sequence diagram enkripsi. Pada proses ini user yang memiliki hak akses dapat membuka file citra yang terkunci. Kemudian apabila sudah memilih file yang ngin dibuka maka akan Kembali ke format awal dan tidak mengalami perubahan apapun untuk menjaga keaslian dari file citra tersebut.



Gambar 4.30 Sequence Diagram Dekripsi

E. *Sequence Diagram* Kompresi

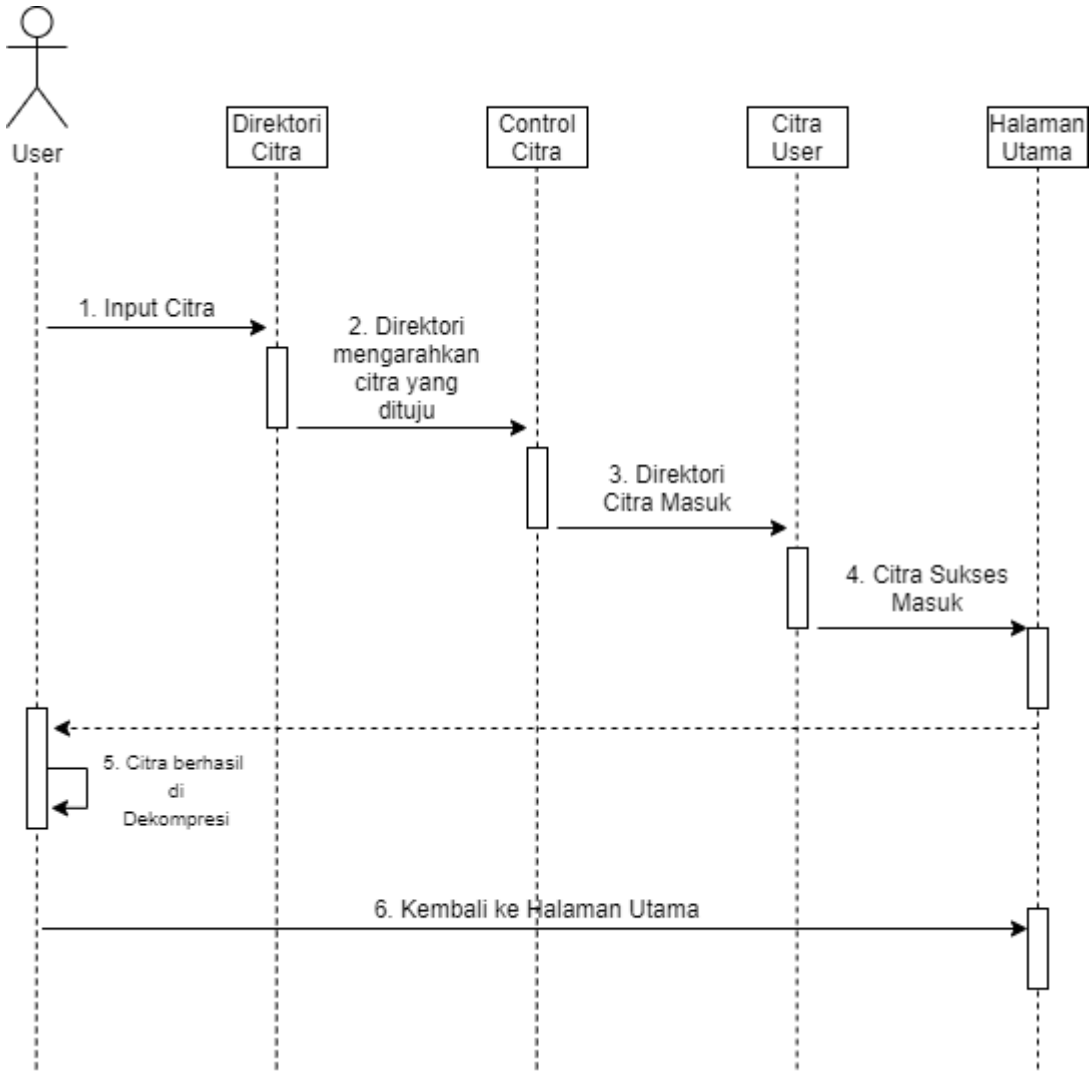
Sequence diagram kompresi menjelaskan tentang proses nteraksi bagaiman proses dari kompresi tu berjalan. Pada proses kompresi ini tidak memerlukan kunci untuk melaksanakan prosesnya hanya memerlukan file citra yang ngin dilakukan kompresi. Kompresi dilakukan setelah proses enkripsi dilakukan yang juga digunakan untuk mengurangi ukuran file citra setelah dilakukan proses enkripsi.



Gambar 4.31 Sequence Diagram Kompresi

F. *Sequence Diagram* Dekompresi

Sequence diagram dekompresi memiliki kemiripan dengan proses kompresi namun proses sebaliknya dari kompresi dimana pada proses interaksi ini akan dilakukan apabila file citra yang telah dikompresi ngin dikembalikkan ke file awal. Sama halnya dengan kompresi, pada proses ini tidak memerlukan kunci, proses ini juga dilakukkan sebelum dilakukannya proses dekripsi file citra tersebut. Proses ini juga mengembalikan ukuran file yang sudah diperkecil menjadi ukuran file semula.

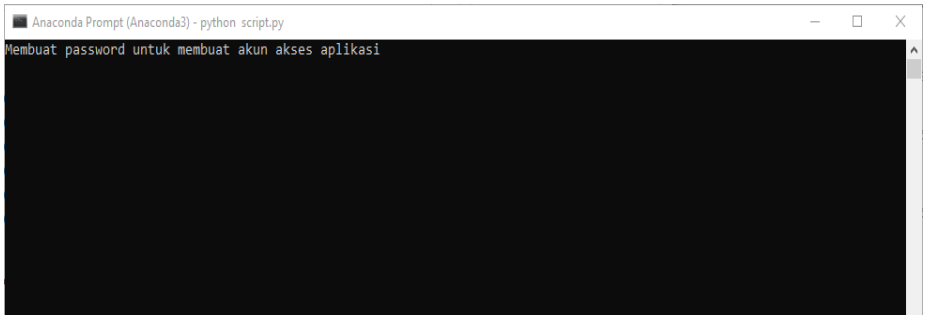


Gambar 4.32 Sequence Diagram Dekompresi

4.4. Tampilan Aplikasi

Pada subbab ini akan menampilkan keseluruhan dari tampilan aplikasi atau program yang telah dibuat oleh peneliti yang yang ditampilkan masih dalam berbentuk command prompt. Terbagi dalam beberapa kategori sebagai berikut.

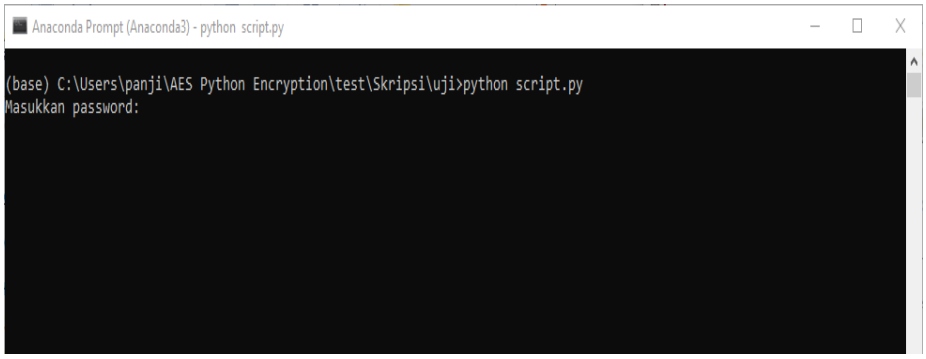
4.4.1. Tampilan Halaman *Register*



Gambar 4.33 Halaman Register

Pada halaman register merupakan halaman yang akan ditampilkan di awal kali apabila program belum memiliki akun yang terdaftar di programnya. Untuk mendapatkan akses ke dalam aplikasi utamanya maka user harus menginput password yang digunakan untuk sebagai hak akses menggunakan aplikasi enkripsi. Apabila user telah berhasil membuat akun yang hanya berupa password maka akun yang terdaftar akan di enkrip dalam satu folder dengan programnya tersebut dan user dapat langsung menuju ke halaman menu utama.

4.4.2. Tampilan Halaman *Login*

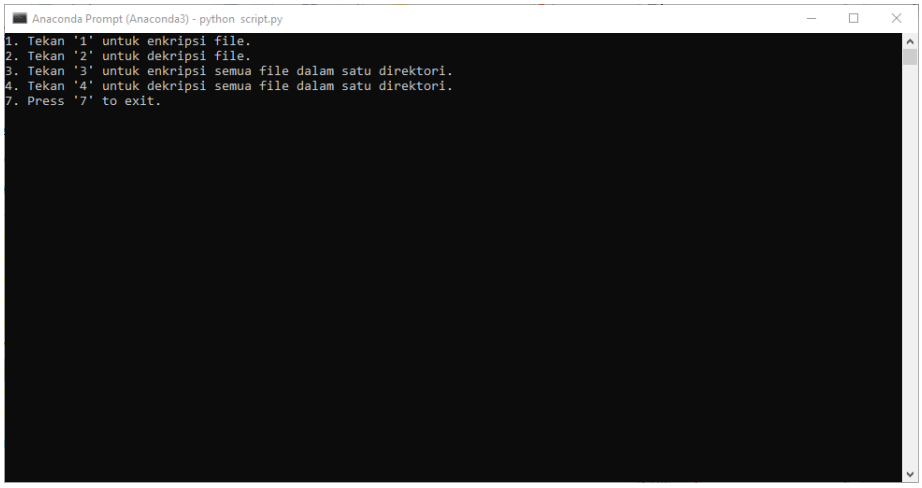


Gambar 4.34 Halaman Login

Pada halaman login merupakan gerbang utama untuk menggunakan aplikasi. Sebelum menggunakan aplikasi program akan menampilkan field password dan user diminta untuk memasukkan password yang sudah terdaftar. Jika user salah memasukkan password maka program akan terhenti di halaman

utama. Apabila user benar memasukkan password maka aplikasi akan langsung menuju ke halaman utama.

4.4.3. Tampilan Menu Utama Untuk Enkripsi dan Dekripsi



Gambar 4.35 Halaman Menu Utama

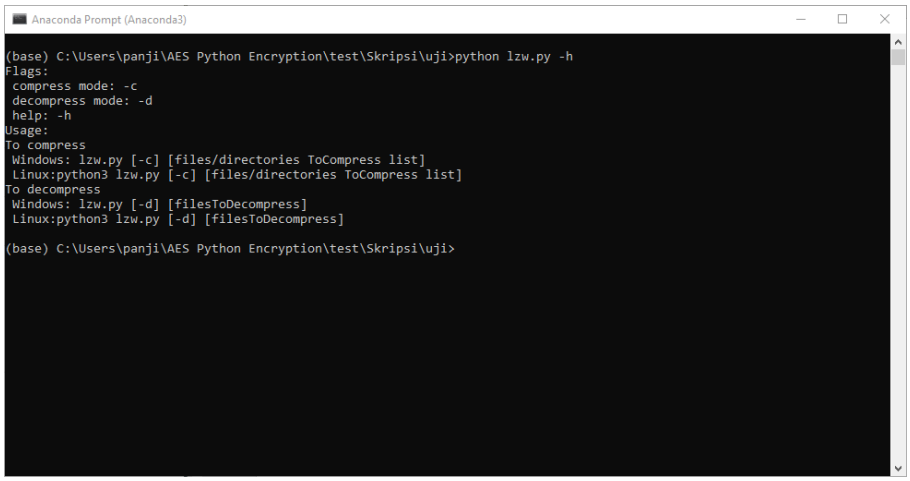
Pada halaman ini merupakan menu utama dari aplikasi untuk melakukkan proses enkripsi dan dekripsi citra. Jadi dalam menu utama proses melakukan kompresi dan dekompresi tidak dalam satu aplikasi utama.

Pada menu utama ada terdapat 5 pilihan yang akan ditampilkan dalam aplikasi yang terdiri dari Encrypt File, Decrypt File, Encrypt All Files, Decrypt All Files, dan Exit. Apabila user memilih Encrypt File maka user hanya bisa mengenkripsi satu citra dengan cara menginputkan nama citra tersebut dan dalam satu direktori dengan aplikasi. Apabila user memilih Decrypt File maka user hanya bisa mendekripsi satu citra yang telah dienkripsi dan berformat (.enc) menjadi ke file awal, lokasi file yang telah dienkrip harus satu direktori dengan aplikasi. Apabila user memilih Encrypt All Files maka user akan mengenkripsi semua citra yang terdapat dalam satu direktori tersebut ke dalam file enkripsi bertipe (.enc). Apabila user memilih Decrypt All Files maka user akan mendekripsi semua citra yang terdapat di dalam satu direktori dan yang telah terkunci kembali

menjadi file citra yang semula. Apabila user memilih Exit maka user akan keluar dari program tersebut.

4.4.4. Tampilan Halaman Untuk Melakukan Kompresi dan Dekompresi

Pada halaman untuk melakukan kompresi dan dekompresi, aplikasi hanya berbebtuk command prompt dan hanya menjalankannya dengan syntax. Terdapat 3 syntax utama di dalam program untuk kompresi dan dekompresi.



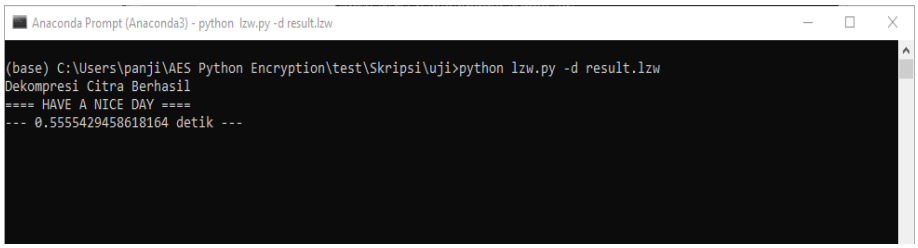
Gambar 4.*36* Halaman Untuk Melakukan Kompresi dan Dekompresi

Pada program di atas terdapat 3 pilihan syntax dengan cara yaitu, -c untuk melakukan kompresi data, -d untuk melakukan dekompresi, dan -h untuk menampilkan program seperti pada gambar 4.36 di atas.

Gambar 4.37 Contoh Syntax Untuk Melakukan Kompresi

Pada gambar di atas merupakan contoh apabila user melakukan kompresi, setelah user berhasil melakukan kompresi maka aka nada

notifikasi di program dan juga menampilkan waktu proses dari kompresi.



Gambar 4.*38* Contoh Syntax Untuk Melakukan Dekompresi

Pada gambar di atas merupakan contoh apabila user melakukan dekompresi, setelah user berhasil melakukan dekompresi sama seperti halnya kompresi, program akan menampilkan notifikasi dan menampilkan waktu proses dari dekompresi.

4.5. Analisis Data Hasil

Analisi data hasil pada proses bertujuan untuk memeriksa dan membuat pemodelan data dengan tujuan untuk mendapatkan hasil nformasi yang bermanfaat yang akhirnya dapat memberi petunjuk bagi peneliti untuk dapat mengambil keputusan akhir.

4.5.1. Analisis Ukuran Data

Pada analisis ukuran data dilakukan proses Analisa antara hubungan proses enkripsi dengan proses kompresi. Nilai yang didapat dari hasil penelitian mengalami perubahan dimana pada proses ini dapat dijelaskan bahwa file citra asli dengan file citra enkripsi dengan algoritma AES (*Advanced Encryption Standard*)dan file citra kompresi dengan menggunakan algoritma LZW (Lempel-Ziv-Welch) tidak memiliki ukuran yang sama.

Tabel 4.7 Pengujian Gambar Format .jpg

Pengujian Gambar Format (.jpg)					
No	Nama Citra	Ukuran File Awal	Ukuran File AES	Ukuran File LZW	Presentase
1	Akta.jpg	6796 kb	6976 kb	13864 kb	198 %
2	Lenna.jpg	50 kb	50 kb	99 kb	198 %
3	Sertif.jpg	1891 kb	1891 kb	3736 kb	197 %
4	Tiger.jpg	6439 kb	6493 kb	12911 kb	198 %

Tabel 4.8 Pengujian Gambar Format .png

Pengujian Gambar Format (.png)					
No	Nama Citra	Ukuran File Awal	Ukuran File AES	Ukuran File LZW	Presentase
1	Akta.png	16426 kb	16426 kb	32045 kb	197 %
2	Lenna.png	463 kb	463 kb	881 kb	190 %
3	Sertif.png	1167 kb	1167 kb	2279 kb	195 %
4	Tiger.png	6117 kb	6117 kb	12168 kb	198 %

Pada tabel setelah dilakukan proses enkripsi dengan AES disini menunjukkan bahwa ukuran citra asli dengan citra setelah di enkripsi memiliki ukuran yang sama dan tidak terjadi perubahan yang signifikkan. Namun setelah dilakukan proses kompresi dengan LZW maka terjadi penambahan ukuran file citra gambar yang sangat besar, sesuai dengan tabel 4.7 dan 4.8 dapat dilihat memiliki kenaikan ukuran antara 190 % sampai dengan 198 % atau 90 % sampai 98 % dari ukuran awal.

4.5.2. Analisis Waktu Eksekusi

Pada pengujian waktu eksekusi digunakan sebagai percobaan apakah ada pengaruh antara ukuran dengan waktu yang diperlukan untuk melakukan proses enkripsi, dekripsi, kompresi, dan dekompresi. Dalam hal ini percobaan waktu mengalami pengaruh dari komputer yang digunakan untuk melakukan eksekusi terlpas dari ukuran gambar tersebut. Dapat dilihat tabel di bawah adalah hasil pengujian waktu.

Tabel 4.9 Pengujian Waktu Gambar jpg

Pengujian Citra Format (.jpg)

No	Nama Gambar	Ukuran Gambar	Waktu Enkrip	Waktu Dekripsi	Waktu Kompresi	Waktu Dekompresi
1	Akta	16426 kb	142 ms	132 ms	11215 ms	6719 ms
2	Lenna	463 kb	7 ms	7 ms	22 ms	166 ms
3	sertif	1167 kb	14 ms	1 ms	627 ms	453 ms
4	tiger	6117 kb	101 ms	48 ms	3940 ms	2529 ms

Tabel 4.10 Pengujian Waktu Gambar png

Pengujian Citra Format (.png)						
No	Nama Gambar	Ukuran Gambar	Waktu Enkrip	Waktu Dekripsi	Waktu Kompresi	Waktu Dekompresi
1	Akta	16426 kb	142 ms	132 ms	11215 ms	6719 ms
2	Lenna	463 kb	7 ms	7 ms	22 ms	166 ms
3	sertif	1167 kb	14 ms	1 ms	627 ms	453 ms
4	tiger	6117 kb	101 ms	48 ms	3940 ms	2529 ms

Berdasrkan hasil dari pengujian di atas dapat disimpulkan bahwa ukuran gambar sangat berpengaruh untuk melakukan eksekusi tersebut. Kemudian ukuran gambar dan waktu eksekusi berbanding lurus yang berarti makin besar ukuran gambar, maka makin lama juga untuk melaksanakan prosesnya juga. Terlepas dari hal tersebut, pernagkat yang digunakan untuk melakukan eksekusi juga sangat berpengaruh, makin tinggi spesifikasinya maka ada kemungkinan makin cepet juga untuk waktu eksekusinya.

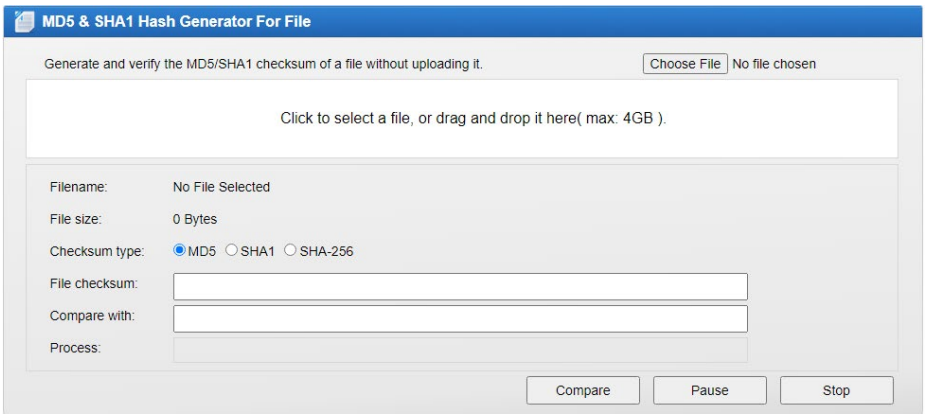
4.5.3. Analisis Hasil Menggunakan Checksum

Pada bagian ini akan dilakukan pengujian menggunakan checksum, pengujian bertujuan ntegritas dari dara yang sudah diproses enkripsi dan kompresi melalui aplikasi. Pada pengujian dengan checksum file akan diperiksa apakah telah terjadi perubahan

antara proses penguncian citra dan proses pembukaan citra yang dilakukan aplikasi. Proses pengujian dengan checksum menggunakan website yaitu dengan cara mengunggah ke website tersebut. Jika terjaid perubahan dalam data citra maka nilai yang akan ditampilkan dari checksum tentu akan berbeda.

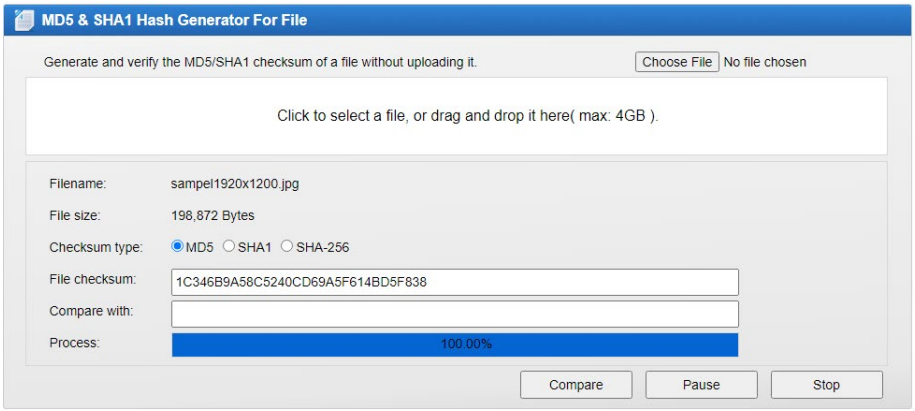
Berikut adalah langkah – langkah yang dilakukan untuk proses checksum adalah sebagai berikut.

A. Pertama buka browser dan kemudian menuju ke web http://onlinemd5.com/ dengan tampilan di bawah dimana terdiri dari form untuk proses pengecekan.



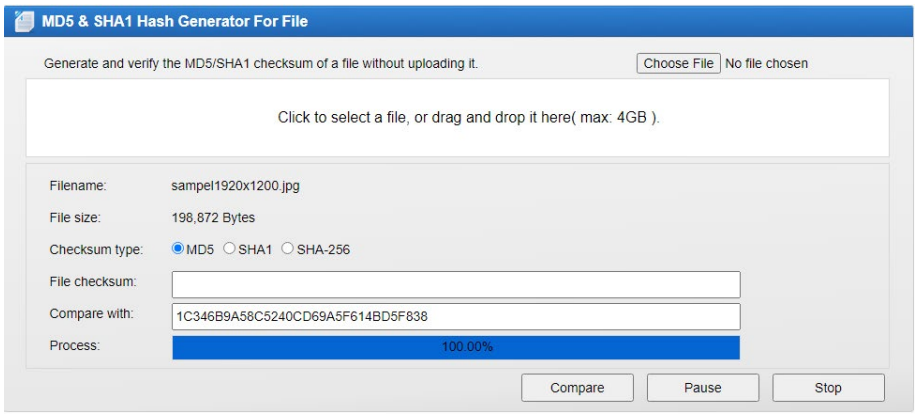
Gambar 4.39 Checksum 1

B. Untuk proses selanjutnya kita dapat melakukan proses pengunggahan berkas dengan cara pilih file atau bisa juga dengan cara drag and drop kemudian akan muncul nilai atau value dari file yang diunggah.



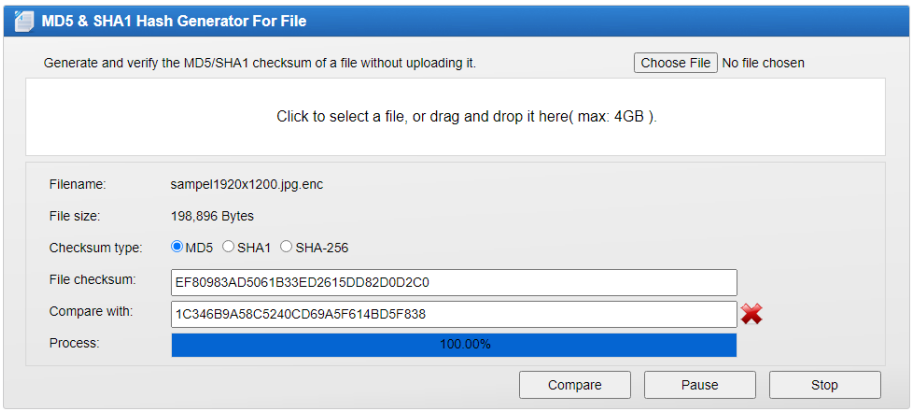
Gambar 4.40 Checksum 2

C. Selanjutnya lakukan cut pada hasil file checksum yang terdapat di kolom File checksum dan lakukan paste di dalam field compare with. Proses dilakukan untuk melakukan perbandingan antara file asli dengan file yang sudah melalui proses buka dan kunci adanya perbedaan atau tidak.



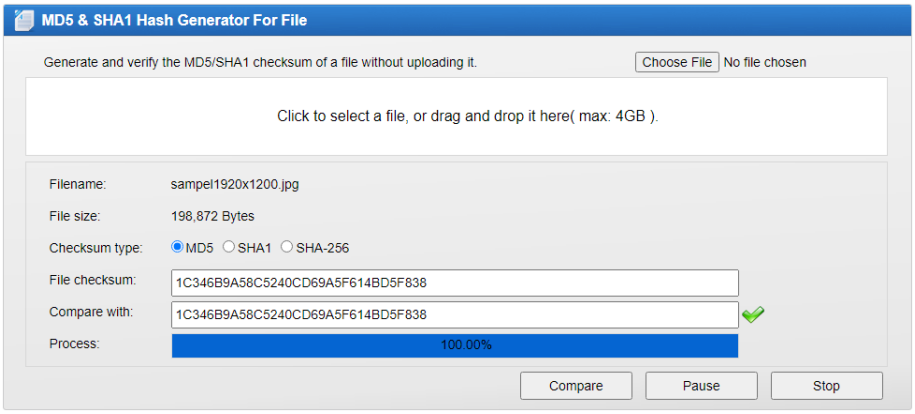
Gambar 4.41 Checksum 3

D. Selanjutnya lakukan pengunggahan file citra yang telah memiliki ekstensi (.enc), kemudian file tersebut akan melakukan proses perbandingan secara otomatis dan hasilnya akan keluar antara sama atau tidak.



Gambar 4.42 Checksum 4

E. Selanjutnya lakukan proses pengulangan dengan membandingkan antara file yang telah dilakukan proses penguncian dan pembukaan dengan file aslinya.



Gambar 4.43 Checksum 5

Pada hasil pengujian dengan menggunakan checksum file awal dengan file proses kunci, kemudian antara hasil pengujian file asli dengan file hasil dari proses penguncian dan pembukaan dapat dilihat pada tabel di bawah.

Tabel 4.11 Hasil Checksum Gambar jpg

Pengujian Checksum (.jpg)				
No	Nama Citra	Keterangan	Nilai Checksum	Keterangan
1	Akta	Berkas Awal	B0D7FE8337C14957A055B72B2C850EA1	-
		Penguncian	332E9640D2033FF9F8D746F187626239	Beda
		Pembukaan	B0D7FE8337C14957A055B72B2C850EA1	Sama
2	Lenna	Berkas Awal	85E0E104F57AD6B2FEE5276E64FE11BA	-
		Penguncian	9FC96EAC985B113DAFA5612C4EBBF187	Beda
		Pembukaan	85E0E104F57AD6B2FEE5276E64FE11BA	Sama
3	sertif	Berkas Awal	89D11546BD11E642A5234D6D7BDF8DB4	-
		Penguncian	C09BD5FDE9D26AB7668585DE83B942C5	Beda
		Pembukaan	89D11546BD11E642A5234D6D7BDF8DB4	Sama
4	tiger	Berkas Awal	AC7044A5026A42B22B9CB4C3E8BC12E2	-
		Penguncian	022A6C15DC6432E86C7C83AE4FA89FBC	Beda
		Pembukaan	AC7044A5026A42B22B9CB4C3E8BC12E2	Sama

Tabel 4.12 Tabel Hasil Checksum Gambar png

Pengujian Checksum (.png)				
No	Nama Citra	Keterangan	Nilai Checksum	Keterangan
1	Akta	Berkas Awal	24B197D7EEE78B4D21239BD311179E68	-
		Penguncian	483270F6EB7893C3D7868DA2E6892A3E	Beda
		Pembukaan	24B197D7EEE78B4D21239BD311179E68	Sama
2	Lenna	Berkas Awal	814A0034F5549E957EE61360D87457E5	-
		Penguncian	C554EC6B5EDD8FF2DC6605221DE5ADDB	Beda
		Pembukaan	814A0034F5549E957EE61360D87457E5	Sama
3	sertif	Berkas Awal	92DBFAADB717D73BA1B8BC0098C0A32D	-
		Penguncian	124025B2207C3FEB278591F9A2A48976	Beda
		Pembukaan	92DBFAADB717D73BA1B8BC0098C0A32D	Sama
4	tiger	Berkas Awal	7B5CCFFEA7735DE9E23ABC020B771B9C	-
		Penguncian	FA63862499553EF0AF047DCF3E6F6836	Beda
		Pembukaan	7B5CCFFEA7735DE9E23ABC020B771B9C	Sama

Berdasarkan hasil pengujian checksum di atas dapat disimpulkan bahwa adanya perubahan antara citra asli dibandingkan dengan citra hasil proses kunci. Dalam proses penguncian terdapat dua proses dengan algoritma enkripsi dan kompresi, nilai checksum mengalami perubahan pada format dan juga ntegritas dari citra tersebut. Kemudian pada hasil perbandingan antara citra asli dengan citra hasil proses pembukaan mendapatkan hasil yang sama dimana tidak ada perubahan dari segi nformasi dan juga ntegritas setelah melalui proses aplikasi tersebut kemudian format citra hasil buka pun kembali menjadi format asli dari citra tersebut.