



**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
AES(*ADVANCED ENCRYPTION STANDARD*) DAN
ALGORITMA KOMPRESI LZW(*LEMPER ZIV WELCH*) PADA
CITRA DIGITAL**

SKRIPSI

Panjianom Bayuaji Herlambang

1710511012

**PROGRAM STUDI INFORMATIKA
FAKULTAS LMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA
2022**



**IMPLEMENTASI ALGORITMA KRIPTOGRAFI
AES(*ADVANCED ENCRYPTION STANDARD*) DAN
ALGORITMA KOMPRESI LZW(*LEMPER ZIV WELCH*) PADA
CITRA DIGITAL**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer**

Panjianom Bayuaji Herlambang

1710511012

**PROGRAM STUDI INFORMATIKA
FAKULTAS LMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN
JAKARTA**

2022

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Panjianom Bayuaji Herlambang

NIM : 1710511012

Tanggal : 06 Desember 2021

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 06 Desember 2021
Yang Menyatakan,



(Panjianom Bayuaji Herlambang)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut :

Nama : Panjianom Bayuaji Herlambang
 NIM : 1710511012
 Program Studi : Informatika
 Judul Skripsi : Implementasi Algoritma Kriptografi AES (*Advanced Encryption Standard*) dan Algoritma Kompresi LZW (*Lempel Ziv Welch*) Pada Citra Digital

Telah berhasil dipatenkan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Henki Bavu Seta, S.Kom., MTI.

Penguji 1



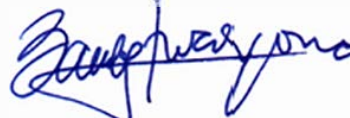
I Wayan Widi P. S.Kom., MT.

Penguji 2



Jayanta, S.Kom., M.Si.

Pembimbing 1



Bambang Tri Wahvono, S.Kom., M.Si

Pembimbing 2



Dr. Ernawati, M.Kom.

Dekan



Yuni Widiastiwi, S.Kom., M.Si.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Pengesahan : 13 Januari 2022



**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI
UNTUK KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Panjianom Bayuaji Herlambang

NIM : 1710511012

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan Ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non Ekklusif (*Non-exclusive Royalty Free Right*) atas karya Ilmiah saya yang berjudul :

Implementasi Algoritma Kriptografi Aes (*Advanced Encryption Standard*)

Dan Algoritma Kompresi Lzw (*Lempel Ziv Welch*) Pada Citra Digital

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 06 Desember 2021

Yang menyatakan,



Panjianom Bayuaji Herlambang

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES
(ADVANCED ENCRYPTION STANDARD) DAN
ALGORITMA KOMPRESI LZW (*LEMPER ZIV WELCH*)
PADA CITRA DIGITAL**

Panjianom Bayuaji Herlambang

ABSTRAK

Citra digital merupakan sebuah data yang dapat memuat banyak hal, baik tentang informasi yang penting atau tidak. Bahkan ada beberapa citra digital yang bisa digunakan untuk menyimpan hal yang bersifat rahasia. Informasi yang disimpan dalam citra digital yang bersifat rahasia ini juga bisa disalahgunakan apabila terdapat di pihak yang tidak bertanggung jawab. Banyaknya penyalahgunaan informasi yang dipakai dalam citra bisa dapat menyebabkan kerugian terhadap pihak yang menerima informasi tersebut. Penelitian ini bertujuan untuk mengembangkan atau melakukan pengamanan citra digital yang berupa gambar dengan menggunakan kombinasi antara algoritma kriptografi dan algoritma kompresi. Algoritma kriptografi yang digunakan merupakan AES dan algoritma kompresi yang digunakan merupakan LZW. Algoritma AES digunakan sebagai untuk proses enkripsi dan dekripsi, sedangkan algoritma LZW digunakan sebagai untuk proses kompresi dan dekompresi. Dari hasil penelitian ini kombinasi dari algoritma AES dan algoritma LZW berhasil mengamankan citra digital. Dimana pada proses awal adalah citra digital dilakukan proses enkripsi dan kemudian proses kompresi. Apabila ingin membuka kembali citra digital yang sudah dilakukan pengamanan maka hanya melakukan proses sebaliknya dan citra digital akan kembali seperti aslinya sebelum dilakukan proses pengamanan tersebut atau seperti file aslinya.

Kata Kunci : Citra Digital, Enkripsi, Kompresi, Dekompresi, Algoritma AES (*Advanced Encryption Standard*), Algoritma LZW (*Lempel Ziv Welch*).

**IMPLEMENTATION OF THE AES CRYPTOGRAPHIC
ALGORITHM (*ADVANCED ENCRYPTION STANDARD*) AND
LZW COMPRESSION ALGORITHM (*LEMPERL ZIV WELCH*)
ON DIGITAL IMAGERY**

Panjianom Bayuaji Herlambang

ABSTRACT

Digital images are data that can contain many things, whether important or not. There are even some digital images that can be used to keep things secret. The information stored in this confidential digital imagery can also be misused found by an irresponsible party. The amount of misuse of the information used in the image can cause harm to the party receiving the information. This study aims to develop or secure digital images in the form of images using a combination of cryptographic algorithms and compression algorithms. The cryptographic algorithm used is AES and the compression algorithm used is LZW. The AES algorithm is used for encryption and decryption process, while the LZW algorithm is used for the compression and decompression processes. From the result of this study, the combination of the AES algorithm and the LZW algorithm succeeded in securing digital images. Where in the initial process is the digital image encryption process and then the compression process. If we want to re-open a digital image that has been secured, then only do the reverse process and the digital image will return to its original state before the security process was carried out or like original file.

Keywords : Digital imagery, Encryption, Compression, Decryption, Decompression, AES Algorithms (*Advanced Encryption Standard*), LZW Algorithms (*Lempel Ziv Welch*).

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT atas segala hikmah dan rezekiNya, serta shalawat dan salam kita panjatkan kepada Nabi Muhammad SAW sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) dan Algoritma Kompresi LZW (Lempel-Ziv-Welch) Pada Citra Digital” yang mana ditunjukkan untuk sebagai salah satu syarat untuk menyelesaikan studi agar memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Dalam penyusunan dan penulisan tugas akhir ini tak lepas dari bantuan orang – orang disekitar penulis. Maka dari itu, dalam kesempatan kali ini penulis ingin mengucapkan rasa terima kasih yang sebesar – besarnya kepada pihak yang sudah membantu dalam penyusunan skripsi ini terutama kepada :

1. Ibu, bapak, dan kakak penulis yang selalu memberikan doa dan dukungan kepada setiap hari dari awal penulis Menyusun skripsi hingga sampai selesai.
2. Bapak Jayanta, S.Kom., M.Si. sebagai dosen pembimbing pertama dan Bapak Bambang Tri Wahyono, S.Kom., M.Si. sebagai dosen pembimbing kedua yang telah bersedia untuk meluangkan waktunya memberikan penulis bimbingan, masukan, kritik, saran, dan serta dukungan selama penulis melakukan penelitian tugas akhir penulis.
3. Ibu Yuni Widiastiwi, S.Kom., M.Si selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta dan Bapak Bayu Hananto, S.Kom., M.Kom. selaku dosen Pembimbing Akademik penulis dari semester satu sampai selesai.
4. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah mendidik dan memberikan ilmu yang bermanfaat kepada penulis.
5. Sahabat – sahabat saya baik yang berada di lingkungan rumah atau lingkungan SMA penulis yang selalu memberikan dukungan kepada penulis hingga penulis bisa menyelesaikan tugas akhirnya.
6. Rekan – rekan saya yang berada di seperjuangan Informatika yang tidak bisa disebutkan satu persatu, yang telah memberikan dukungan kepada penulis.

7. Semua pihak yang penulis tidak bisa sebutkan satu persatu, yang telah memberikan dukungan kepada penulis.

Semoga Allah SWT memberikan balasan yang berlipat ganda kepada kita semua. Penulis menyadari bahwa tugas akhir ini belum sempurna, baik dari segi materi maupun penyajiannya. Oleh karena itu, saran dan kritik yang membangun sangat diharapkan dalam penyempurnaan tugas akhir ini. Akhir kata, semoga skripsi ini dapat bermanfaat dan menambah wawasan bagi para pembacanya.

Jakarta, 06 Desember 2021

Penulis,

Panjianom Bayuaji Herlambang

DAFTAR ISI

HALAMAN JUDUL.....	ii
PERNYATAAN ORISINALITAS	iii
LEMBAR PENGESAHAN	iv
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL.....	xvi
DAFTAR LAMPIRAN.....	xvii
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian.....	2
1.5. Manfaat Penelitian.....	3
1.6. Ruang Lingkup	3
1.7. Luaran yang Diharapkan	3
1.8. Sistematika Penulisan.....	3
BAB 2 TINJAUAN PUSTAKA	5
2.1. Kriptografi	5
2.2. Enkripsi	5
2.3. Algoritma AES (<i>Advanced Encryption Standard</i>)	6

2.4.	Kompresi	12
2.5.	Algoritma LZW (<i>Lempel-Ziv-Welch</i>).....	13
2.6.	Citra Digital	13
2.7.	Python.....	16
BAB 3 METODE PENELITIAN.....		17
3.1.	Kerangka Pikir.....	17
3.2.	Alur Enkripsi dan Dekripsi.....	19
3.3.	Alur Kompresi dan Dekompresi.....	21
3.4.	Alat Bantu Penelitian.....	23
3.5.	Jadwal Kegiatan	25
BAB 4 PEMBAHASAN		26
4.1.	Sumber Data	26
4.1.1.	Sumber Data.....	26
4.2.	Perhitungan AES dan LZW	28
4.3.	Flow Chart, Use Case, dan Class Diagram Aplikasi	47
4.3.1.	<i>Flowchart</i> Register.....	47
4.3.2.	<i>Flowchart</i> Login	48
4.3.3.	<i>Flowchart</i> Enkripsi File	48
4.3.4.	<i>Flowchart</i> Kompresi File	49
4.3.5.	<i>Flowchart</i> Dekompresi File	50
4.3.6.	<i>Flowchart</i> Dekripsi File	51
4.3.7.	Use Case Aplikasi	52
4.3.8.	Activity Diagram.....	54
4.3.9.	Sequence Diagram	60
4.4.	Tampilan Aplikasi	67
4.4.1.	Tampilan Halaman <i>Register</i>	68

4.4.2.	Tampilan Halaman <i>Login</i>	68
4.4.3.	Tampilan Menu Utama Untuk Enkripsi dan Dekripsi	69
4.4.4.	Tampilan Halaman Untuk Melakukan Kompresi dan Dekompresi	70
4.5.	Analisis Data Hasil	71
4.5.1.	Analisis Ukuran Data	71
4.5.2.	Analisis Waktu Eksekusi.....	72
4.5.3.	Analisis Hasil Menggunakan Checksum	73
BAB 5 PENUTUP		78
5.1.	Kesimpulan.....	78
5.2.	Saran	79
DAFTAR PUSTAKA		80
RIWAYAT HIDUP.....		81

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi AES	7
Gambar 2.2 Tabel S-Box.....	7
Gambar 2.3 Hasil Transformasi Shiftrows.....	8
Gambar 2.4 Transformasi AddRoundKey	9
Gambar 2.5 Proses Dekripsi AES	10
Gambar 2.6 Transformasi Shiftrows	10
Gambar 2.7 Tabel nverse S-Box	11
Gambar 2.8 Matriks nvMixColumns	11
Gambar 2.9 Hasil Perkalian Matriks.....	12
Gambar 2.10 Sistem Koordinat Citra.....	13
Gambar 2.11 Matriks Citra Digital	14
Gambar 2.12 Citra Biner	14
Gambar 2.13 Citra Grayscale.....	15
Gambar 2.14 Citra RGB.....	15
Gambar 3.1 Kerangka Pikir.....	17
Gambar 3.2 Alur Enkripsi dan Dekripsi	19
Gambar 3.2 Alur Enkripsi.....	20
Gambar 3.3 Proses Dekripsi.....	21
Gambar 3.4 Alur Kompresi dan Dekompresi	22
Gambar 3.5 Proses Kompresi.....	23
Gambar 3.6 Proses Dekompresi.....	23
Gambar 4.1 Sampel Gambar Lenna	27
Gambar 4.2 Sampel Sertifikat Seminar Gambar.....	27
Gambar 4.3 Sampel Surat Dokumen Gambar.....	27
Gambar 4.4 Sampel Gambar Tiger	28
Gambar 4.5 Barisan Hexadecimal.....	29
Gambar 4.6 Gambar Barisan Hexadecimal Key	30
Gambar 4.7 Tabel S-Box.....	34

Gambar 4.8 Barisan Hexadecimal Hasil Enkripsi.....	38
Gambar 4.9 Tabel ASCII 1	39
Gambar 4.10 Tabel ASCII 2	40
Gambar 4.11 Bilangan Hexadecimal yang akan DiDekripsi	44
Gambar 4.12 Bilangan Hexadecimal setelah Di dekripsi	47
Gambar 4.13 Flowchart Register	48
Gambar 4.14 Flowchart Login	48
Gambar 4.15 Flowchart Enkripsi	49
Gambar 4.16 Flowchart Kompresi	50
Gambar 4.17 Flowchart Dekompresi	51
Gambar 4.18 Flowchart Dekripsi	52
Gambar 4.19 Use Case Aplikasi Enkripsi dan Dekripsi	53
Gambar 4.20 Use Case Aplikasi Kompresi dan Dekompresi	53
Gambar 4.21 Activity Diagram Register	55
Gambar 4.22 Activity Diagram Login	56
Gambar 4.23 Activity Diagram Enkripsi	57
Gambar 4.24 Activity Diagram Dekripsi	58
Gambar 4.25 Activity Diagram Kompresi	59
Gambar 4.26 Activity Diagram Dekompresi	60
Gambar 4.27 Sequence Diagram Register	62
Gambar 4.28 Sequence Diagram Login	63
Gambar 4.29 Sequence Diagram Enkripsi	64
Gambar 4.30 Sequence Diagram Dekripsi.....	65
Gambar 4.31 Sequence Diagram Kompresi.....	66
Gambar 4.32 Sequence Diagram Dekompresi	67
Gambar 4.33 Halaman Register	68
Gambar 4.34 Halaman Login	68
Gambar 4.35 Halaman Menu Utama	69
Gambar 4.36 Halaman Untuk Melakukan Kompresi dan Dekompresi	70
Gambar 4.37 Contoh Syntax Untuk Melakukan Kompresi	70
Gambar 4.38 Contoh Syntax Untuk Melakukan Dekompresi	71
Gambar 4.39 Checksum 1	74

Gambar 4.40 Checksum 2	74
Gambar 4.41 Checksum 3	75
Gambar 4.42 Checksum 4	75
Gambar 4.43 Checksum 5	76

DAFTAR TABEL

Tabel 3.1 Jadwal Kegiatan	25
Tabel 4.1 Sumber Data.....	26
Tabel 4.2 RCon (Round Constant).....	32
Tabel 4.3 Tabel Hasil Perhitungan Enkripsi AES.....	36
Tabel 4.4 Hasil Perhitungan Kompresi LZW	41
Tabel 4.5 Hasil Perhitungan Dekompresi LZW.....	42
Tabel 4.6 Hasil Perhitungan Dekompresi AES.....	44
Tabel 4.7 Pengujian Gambar Format .jpg	71
Tabel 4.8 Pengujian Gambar Format .png	72
Tabel 4.9 Pengujian Waktu Gambar jpg	72
Tabel 4.10 Pengujian Waktu Gambar png	73
Tabel 4.11 Hasil Checksum Gambar jpg	76
Tabel 4.12 Tabel Hasil Checksum Gambar png	77

DAFTAR LAMPIRAN

Lampiran 1 Source Code Aplikasi AES	82
Lampiran 2 Source Code Aplikasi LZW	87