



THESIS

**ENKRIPSI DATASET DENGAN MENGGUNAKAN ALGORITMA
HOMOMORFIK PAILLIER dan RIVEST SHAMIR ADLEMAN (RSA)
PADA SISTEM PENDETEKSI OBJEK dengan ALGORITMA YOLOv8**

HASIL TESIS



**Nama : Ahmad Faizin
NIM : 55423110011**

**UNIVERSITAS
MERCU BUANA**

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK**

UNIVERSITAS MERCU BUANA

JAKARTA

2025



THESIS

ENKRIPSI DATASET DENGAN MENGGUNAKAN ALGORITMA HOMOMORFIK PAILLIER dan RIVEST SHAMIR ADLEMAN (RSA) PADA SISTEM PENDETEKSI OBJEK dengan ALGORITMA YOLOv8

Diajukan sebagai salah satu syarat untuk menyelesaikan
Program Studi Magister Teknik Elektro (S2)

Nama : Ahmad Faizin
NIM : 55423110011
Pembimbing : Dr. Regina Lionnie, ST., MT

UNIVERSITAS
MERCU BUANA

**PROGRAM STUDI MAGISTER TEKNIK ELEKTRO
FAKULTAS TEKNIK**

UNIVERSITAS MERCU BUANA

JAKARTA

2025

SURAT KETERANGAN HASIL *SIMILARITY*

Menerangkan bahwa Karya Ilmiah/Laporan Tugas Akhir/Skripsi pada BAB I, BAB II, BAB III, BAB IV dan BAB V atas nama:

Nama : **Ahmad Faizin**
NIM : **55423110011**
Program Studi : **Magister Teknik Elektro**
Judul Tugas Akhir / Tesis
/ Praktek Keinsinyuran : **ENKRIPSI DATASET dengan MENGGUNAKAN**
ALGORITMA
HOMOMORFIK PAILLIER dan RIVEST SHAMIR
ADLEMAN (RSA)
PADA SISTEM PENDETEKSI OBJEK dengan
ALGORITMA YOLOv8

Telah dilakukan pengecekan *Similarity* menggunakan aplikasi/sistem *Turnitin* pada **Jumat, 15 Agustus 2025** dengan hasil presentase sebesar **9 %** dan dinyatakan memenuhi standar sesuai dengan ketentuan yang berlaku di Fakultas Teknik Universitas Mercu Buana.
Demikian surat keterangan ini dibuat dan digunakan sebagaimana mestinya.

Jakarta, 15 Agustus 2025

Administrator Turnitin,



Itmam Haidi Syarif

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Ahmad Faizin

NIM : 55423110011

Program Studi : Magister Teknik Elektro

Judul Laporan Tesis : Enkripsi Dataset dengan Menggunakan Algoritma

Homomorfik Paillier dan Rivest Shamir Adleman
(RSA) pada Sistem Pendeteksi Objek dengan
Algoritma YOLOv8.

Dengan ini menyatakan bahwa hasil penulisan Tesis yang telah saya buat ini merupakan hasil karya saya sendiri dan benar keasliannya. Apabila ternyata dikemudian hari penulisan Tesis ini merupakan hasil plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggung jawabkan sekaligus bersedia menerima sanksi berdasarkan aturan di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan

Penulis,



Ahmad Faizin

HALAMAN PENGESAHAN

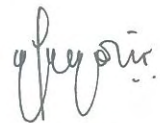
Laporan Skripsi / Tesis ini diajukan oleh :

Nama : Ahmad Faizin
NIM : 55423110011
Program Studi : Magister Teknik Elektro
Judul Tesis : Enkripsi Dataset dengan Menggunakan Algoritma
Homomorfik Paillier dan Rivest Shamir Adleman (RSA)
pada Sistem Pendeteksi Objek dengan Algoritma YOLOv8

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata S2 pada Program Studi Magister Teknik Elektro, Fakultas Teknik Universitas Mercu Buana.

Disahkan Oleh :

Pembimbing : Dr. Regina Lionnie, ST., MT
NIDN : 0301028903
Ketua Penguji : Yudhi Gunardi, S.T., M.T., Ph.D
NIDN : 0330086902
Anggota Penguji : Prof. Dr. Ir. Setiyo Budiyo, ST., MT., IPU.,
Asean-Eng., APEC-Eng
NIDN : 0312118206

()

()

()

Jakarta, 30 Juli 2025

Mengetahui,

Dekan
Fakultas Teknik

Ketua Program Studi
Magister Teknik Elektro


Dr. Zulfa Fitri Ikatinasari, M.T


Prof. Dr. Ir. Setiyo Budiyo,
ST., MT., IPU., Asean-Eng., APEC-Eng

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Laporan Tesis ini. Penulisan Laporan Tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Teknik Elektro pada Fakultas Teknik Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Prof. Dr. Andi Adriansyah, M. Eng., selaku Rektor Universitas Mercu Buana
2. Bapak Prof. Dr. Setiyo Budiyanto, ST.,MT.,IPU., Ascan-Eng.,APEC-Eng. Selaku Kaprodi Magister Teknik Elektro
3. Dr. Regina Lionnie, ST., MT selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
4. Yudhi Gunardi dan Prof. Dr. Ir. Setiyo Budiyanto, ST.,MT.,IPU., Ascan-Eng.,APEC-Eng selaku Dosen Penguji Tugas Akhir atas koreksi dan arahan serta masukannya.
5. Bapak, Ibu, Mertua, dan Istri, yang selalu mendoakan dan memberikan semangat serta dukungannya.
6. Teman – teman penulis, baik yang berada dikampus dan diluar kampus yang telah mau berbagi pikiran serta memberikan dukungan secara moral.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Laporan Magang/Skripsi/Tesis/Disertasi ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 30 JULI 2025



Ahmad Faizin

Enkripsi Dataset dengan Menggunakan Algoritma Homomorfik Paillier dan Rivest Shamir Adleman (RSA) pada Sistem Pendeteksi Objek dengan Algoritma YOLOv8

Ahmad Faizin

Program Magister Teknik Elektro, Fakultas Teknik, Universitas Mercu Buana
Jakarta

email : faizin657@gmail.com

ABSTRAK

Saat ini, telah banyak penelitian yang berkaitan dengan pendeteksian objek, akan tetapi masih sedikit yang memperhatikan aspek keamanan data, khususnya enkripsi terhadap dataset yang digunakan, hal ini sangatlah penting karena dataset pada sistem pendeteksian objek merupakan dataset pribadi dari setiap objek yang direkam, sehingga sangat penting untuk dijaga kerahasiaannya dari pihak yang tidak berwenang.

Pada penelitian ini dilakukan proses enkripsi dataset pada sistem pendeteksian objek dengan menggunakan algoritma Homomorfik Paillier dan melakukan enkripsi kunci pribadi dengan menggunakan algoritma RSA untuk meningkatkan keamanan dari dataset yang dienkripsi. Proses enkripsi dilakukan pada *channels* R dan G dari gambar RGB, kemudian melakukan pelatihan model deteksi objek manusia dengan menggunakan dataset yang terenkripsi.

Keberhasilan enkripsi dianalisa berdasarkan parameter MSE, PSNR, dan SSIM, yang menunjukkan bahwa dataset telah berhasil dienkripsi dan sangat sulit untuk diidentifikasi sebagai sebuah objek. Enkripsi yang dilakukan pada kunci pribadi meningkatkan keamanan dari dataset sehingga diperlukan estimasi waktu untuk melakukan pemecahan kunci selama $1 * 10^{17}$ tahun. Proses enkripsi 2 *channels* pada algoritma Homomorfik Paillier membutuhkan waktu 8-9 menit pada setiap gambar dengan penggunaan RAM mencapai 79%. Walaupun hasil deteksi pada dataset yang terenkripsi memiliki penurunan kualitas jika dibandingkan dengan dataset yang tidak dienkripsi, dengan hasil deteksi yang tidak sesuai pada beberapa kondisi, akan tetapi secara umum penelitian ini menunjukkan bahwa sistem enkripsi pada dataset pendeteksian objek mendapatkan hasil persentase keberhasilan yang signifikan diantara 80-97% pada saat pengujian.

Kata Kunci : Enkripsi Homomorfik Paillier, RSA, Deteksi Objek, YOLOv8, Dataset Gambar, Keamanan Data.

ABSTRACT

Currently, numerous studies have focused on object detection; however, little attention has been given to data security, particularly the encryption of the datasets used. This is a crucial concern, as datasets in object detection systems often contain private information related to the recorded objects, making it essential to ensure their confidentiality and protect them from unauthorized access.

This study describes the use of image-based datasets encrypted using the Homomorphic Paillier algorithm, with the private key further secured using the RSA algorithm to enhance the overall security of the encrypted dataset. The encryption process is applied to the R and G *channels* of RGB images, followed by training a human-object detection model using encrypted dataset.

The success of the encryption is evaluated using MSE, PSNR, and SSIM metrics, these results indicate that the dataset has been successfully encrypted and is difficult to visually recognize as an object. The dual encryption scheme provides strong cryptographic security, with brute-force the key estimated to require $1 * 10^{117}$ years. Encrypting two *channels* using the Homomorphic Paillier algorithm takes approximately 8–9 minutes per image, with RAM usage reaching up to 79%. Training the model with the encrypted dataset produces good results, achieving near-perfect precision, low train loss, and high mAP50 scores. Although detection results using the encrypted dataset show reduced quality compared to those using unencrypted data, particularly under certain conditions where incorrect detections may occur, overall the study demonstrates that encrypting the dataset of object detection does not hinder the system's ability to detect objects effectively with a presented between 80-97%.

Keywords: *Homomorphic Paillier Encryption, RSA, Object Detection, YOLOv8, Image Dataset, Data Security.*

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN SIMILARITY CHECK	ii
LEMBAR PERNYATAAN	iii
KATA PENGANTAR.....	v
ABSTRAK	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI	viii
DAFTAR GAMBAR.....	iv
DAFTAR TABEL	v
DAFTAR SINGKATAN.....	vi
DAFTAR SIMBOL	vii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan	4
1.4 Batasan Masalah	4
1.5 Metodologi Penelitian.....	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	7
2.1 Tinjauan Pustaka.....	7
2.2 Enkripsi dan Deskripsi	16
2.3 Algoritma Homomorfik.....	17
2.4 Algoritma Homomorfik Paillier	18
2.5 Algoritma RSA.....	19
2.6 Kriptografi	21
2.7 Pengolahan Citra Digital	22
2.8 Yolo V8.....	23
2.9 <i>Visual Studio Code</i>	24
2.10 Metrik Kualitas Gambar (MSE, PSNR, dan SSIM)	25
2.11 <i>General Number Field Sieve</i> (GNFS)	28
BAB III METODOLOGI PENELITIAN	30
3.1 Diagram Blok.....	30

3.2	Perancangan Program Perangkat Lunak	31
3.2.1	Enkripsi Dataset Menggunakan Algoritma Homomorfik Paillier	31
3.2.2	Melakukan Enkripsi Kunci HE Paillier dengan Algoritma RSA	32
3.2.3	Pelatihan Dataset	33
3.2.4	Perancangan Perangkat Lunak Pendeteksi Objek	33
3.3	Diagram Alir Penelitian	35
3.4	Skema Penelitian.....	39
BAB IV HASIL DAN PEMBAHASAN.....		41
4.1	Enkripsi Dataset dengan Algoritma Perancangan.....	41
4.1.1	Tujuan Enkripsi Dataset	42
4.1.2	Prosedur Enkripsi Data.....	42
4.1.3	Proses Enkripsi	44
4.1.4	Menghitung nilai MSE, PSNR, dan SSIM	45
4.1.5	Waktu Enkripsi	55
4.1.6	Ukuran Gambar Sebelum dan Sesudah Enkripsi.....	56
4.2	Enkripsi Kunci Homomorfik Paillier dengan Algoritma RSA	58
4.2.1	Tujuan Enkripsi Kunci Homomorfik Paillier	59
4.2.2	Prosedur Enkripsi	59
4.2.3	Menguji Keamanan dari Kunci RSA dan Homomorfik Paillier.....	60
4.3	Performa CPU dan RAM.....	61
4.3.1	Performa CPU	61
4.3.2	Performa RAM (<i>Random Access Memory</i>).....	62
4.4	Melatih Dataset dengan Algoritma Pendeteksian Objek	64
4.4.1	Pelatihan Dataset	64
4.5	Uji <i>Confidence</i> Pendeteksian Objek.....	66
4.5.1	Tujuan Pengujian Tingkat <i>Confidence</i>	66
4.5.2	Prosedur Pengujian Tingkat <i>Confidence</i>	66
4.5.3	Hasil Pengujian Deteksi Objek.....	66
4.5.4	Hasil Pengujian Pendeteksian Objek dengan Halangan	69
BAB V KESIMPULAN DAN SARAN		72
5.1	Kesimpulan	72
5.2	Saran	73
DAFTAR PUSTAKA.....		vi
LAMPIRAN.....		xi

DAFTAR GAMBAR

Gambar 2. 1 Kriptografi.....	22
Gambar 2. 2 Arsitektur YOLOv8 [1]	24
Gambar 2. 3 Visual Studio Code.....	25
Gambar 3. 1 Blok Diagram	30
Gambar 3. 2 <i>Flowchart</i> Enkripsi Homomorfik.....	31
Gambar 3. 3 <i>Flowchart</i> Enkripsi Kunci HE Paillier dengan Algoritma RSA	32
Gambar 3. 4 Preprosesing Dataset	33
Gambar 3. 5 <i>Flowchart</i> Pendeteksi Objek	34
Gambar 3. 6 Diagram Alir Penelitian.....	37
Gambar 3. 7 Skema Penelitian.....	39
Gambar 4. 1 Dataset Wajah [38]	42
Gambar 4. 2 Perbandingan gambar asli dengan enkripsi 1 <i>channel</i> dan 2 <i>channels</i>	45
Gambar 4. 3 Waktu Enkripsi pada masing-masing gambar	56
Gambar 4. 4 Performa CPU sebelum proses enkripsi.....	61
Gambar 4. 5 Performa CPU pada saat proses enkripsi	62
Gambar 4. 6 Performa RAM sebelum proses enkripsi berjalan	63
Gambar 4. 7 Performa RAM pada saat proses enkripsi.....	63
Gambar 4. 8 Hasil dari data training pada 25 epoch.....	65
Gambar 4. 9 <i>Confusion Matrix</i>	65
Gambar 4. 10 Hasil Deteksi pada Dataset Enkripsi 2 <i>Channels</i>	67
Gambar 4. 11 Hasil Deteksi pada Dataset Sebelum di Enkripsi	67
Gambar 4. 12 Grafik Akurasi pada Dataset yang Sudah Enkripsi 2 <i>Channels</i>	68
Gambar 4. 13 Grafik <i>Confidence</i> pada Dataset Tanpa Enkripsi 2 <i>Channels</i>	68
Gambar 4. 14 Hasil Deteksi pada Dataset Setelah di Enkripsi 2 <i>channels</i> dengan Objek Penghalang	69
Gambar 4. 15 Hasil Deteksi pada Dataset Sebelum di Enkripsi 2 <i>Channels</i> dengan Objek Penghalang	70
Gambar 4. 16 Grafik hasil Dataset yang Sudah di Enkripsi 2 <i>Channels</i>	70
Gambar 4. 17 Grafik hasil pada Dataset Tanpa Enkripsi 2 <i>Channels</i>	71
Gambar Lampiran 1 Hasil Enkripsi Gambar Grayscale	xiii
Gambar Lampiran 2 Hasil Enkripsi Gambar RGB	xiv
Gambar Lampiran 3 Hasil Deteksi pada 5 FPS	xiv
Gambar Lampiran 4 Hasil Deteksi pada 10 FPS	xv
Gambar Lampiran 5 Hasil Deteksi pada 15 FPS	xv

DAFTAR TABEL

Tabel 2. 1 Literature Review	10
Tabel 4. 1 Kunci Publik.....	43
Tabel 4. 2 Kunci Pribadi.....	44
Tabel 4. 3 Nilai MSE untuk beberapa koresponden pada hasil enkripsi <i>channels</i> 2 (<i>Red</i> dan <i>Green</i>)	48
Tabel 4. 4 Nilai MSE untuk beberapa koresponden pada hasil enkripsi <i>channel</i> 1 (<i>Red</i>).....	49
Tabel 4. 5 Nilai PSNR untuk beberapa koresponden pada hasil enkripsi 2 <i>channels</i> (<i>Red</i> dan <i>Green</i>)	51
Tabel 4. 6 Nilai PSNR untuk beberapa koresponden pada hasil enkripsi 1 <i>channel</i> (<i>Red</i>).....	51
Tabel 4. 7 Nilai SSIM untuk beberapa koresponden pada hasil enkripsi 2 <i>channels</i> (<i>Red</i> dan <i>Green</i>)	54
Tabel 4. 8 Nilai SSIM untuk beberapa koresponden pada hasil enkripsi 1 <i>channel</i> (<i>Red</i>).....	55
Tabel 4. 9 Perbedaan ukuran gambar antara gambar asli dengan hasil enkripsi 2 <i>channels</i>	57
Tabel 4. 10 Perbedaan ukuran gambar antara gambar asli dengan hasil enkripsi 1 <i>channel</i>	58
Tabel 4. 14 Simulasi Waktu yang Dibutuhkan untuk Pemecahan Kunci RSA dan Homomorfik Paillier	60
Tabel 4. 11 Kunci Publik RSA	xi
Tabel 4. 12 Kunci Pribadi RSA.....	xii
Tabel 4. 13 Hasil Enkripsi Kunci Publik Homomorfik Paillier	xiii

UNIVERSITAS
MERCU BUANA

DAFTAR SINGKATAN

YOLOv8	:	<i>You Only Look Once versi 8</i>
RSA	:	<i>Rivest Shamir Adleman</i>
HE Paillier	:	<i>Homomorphic Encryption Paillier</i>
MSE	:	<i>Mean Square Error</i>
PSNR	:	<i>Peak Signal to Noise Ratio</i>
SSIM	:	<i>Structural Similarity Index Measure</i>
FHE	:	<i>Fully Homomorphic Encryption</i>
HE	:	<i>Homomorphic Encryption</i>
GNFS	:	<i>General Number Field Sieve</i>
dB	:	<i>Desible</i>
RGB	:	<i>Red, Green, Blue</i>



DAFTAR SIMBOL

E	: Algoritma homomorfik
$m_1, m_2 \in M$	: Dua buah pesan yang berada dalam himpunan pesan M
n	: Hasil perkalian dua buah bilangan prima besar (p dan q)
p	: Bilangan prima besar
q	: Bilangan prima besar
g	: Generator group
γ	: <i>least common multiple</i> (LCM) dari $p-1$ dan $q-1$
σ	: modular <i>multiplicative invers</i> dari γ dan n
x	: Nilai kongruen dengan 1 mod n
c	: <i>Chipertext</i>
r	: Nilai bilangan acak yang relative prima dengan bilangan n
m	: Modular
d	: Kunci pribadi untuk proses deskripsi
k	: Hasil percobaan nilai untuk mendapatkan nilai d yang merupakan bilangan bulat
e	: Kunci publik untuk proses enkripsi pesan
$I(i,j)$	: Piksel pada posisi i,j Digambar asli
$K(i,j)$	: Piksel pada posisi i,j Digambar terenkripsi
MAX	: Nilai maksimum dari intensitas piksel
μ_x, μ_y	: Rata-rata intensitas piksel pada gambar x dan y
σ_x^2, σ_y^2	: Variansi intensitas piksel pada gambar x dan y
σ_x, σ_y	: Kovarians antara x dan y
$C1, C2$	: Konstanta kecil untuk mencegah pembagian dengan nol

UNIVERSITAS
MERCU BUANA