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

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

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:

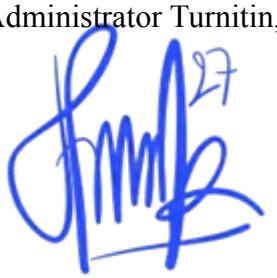
Nama	**:**	**Ahmad Faizin**
NIM	**:**	**55423110011**
Program Studi	**:**	**Magister Teknik Elektro**
Judul Tugas Akhir / Tesis / Praktek Keinsinyuran	**:**	**ENKRIPSI DATASET dengan MENGGUNAKAN ALGORITMA HOMOMORFIK PAILLIER dan RIVEST SHAMIR ADLEMAN (RSA) PADA SISTEM PENDETEKSI OBJEK dengan ALGORITMA 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 Budiyanto, ST.,MT.,IPU., Asean-Eng.,APEC-Eng	( )
NIDN	:	0312118206	

Jakarta, 30 Juli 2025

Mengetahui,

Dekan	Ketua Program Studi
Fakultas Teknik	Magister Teknik Elektro
Dr. Zulfa Fitri Ikatrinasari, M.T	Prof. Dr. Ir. Setiyo Budiyanto, 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., Asean-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., Asean-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 berdasarakn 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 $1 * 10^{117}$ 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, Yolo*v8,* 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 *channel*s 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 *channel*s 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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

YOLO*v8*	:	*You Only Look Once versi 8*
RSA	:	Rivest Shamir Adleman
HE Paillier	:	*Homomorphic Encryption Paillier*
MSE	:	*Mean Square Error*
PSNR	:	*Peak Signal to Noise Ratio*
SSIM	:	*Structural Similarity Index Measure*
FHE	:	*Fully Homomorphic Encryption*
HE	:	*Homomorphic Encryption*
GNFS	:	*General Number Field Sieve*
dB	:	*Desible*
RGB	:	*Red, Green, Blue*

DAFTAR SIMBOL

E	:	Algortima homomorfik
$m1,m2 \in M$	:	Dua buah pesan yang berada dalam himpunan pesan M
n	:	Haslil perkalian dua buah bilangan prima besar(p dan q)
p	:	Bilangan prima besar
q	:	Bilangan prima besar
g	:	Gerator group
γ	:	*least common multiple* (LCM) dari $p-1$ dan $q-1$
σ	:	modular *multiplicative invers* dari γ dan n
x	:	Nilai kongruen dengan 1 mod n
c	:	*Chipertext*
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
$\mu x, \mu y$	:	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