

**IMPLEMENTASI PESAN TERSEMBUNYI PADA CITRA  
DIGITAL DENGAN ALGORITMA LEAST SIGNIFICANT BIT  
(LSB) DAN ADVANCED ENCRYPTION STANDARD (AES)**

**SKRIPSI**



Franli Chandra Thian

1911500005

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG**

**2023**

**IMPLEMENTASI PESAN TERSEMBUNYI PADA CITRA  
DIGITAL DENGAN ALGORITMA LEAST SIGNIFICANT BIT  
(LSB) DAN ADVANCED ENCRYPTION STANDARD (AES)**

**SKRIPSI**

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



Oleh :

Franli Chandra Thian

1911500005

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG**

**2023**

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 1911500005

Nama : Franli Chandra Thian

Judul Skripsi : IMPLEMENTASI PESAN TERSEMBUNYI PADA CITRA  
DIGITAL DENGAN ALGORITMA LEAST SIGNIFICANT  
BIT (LSB) DAN ADVANCED ENCRYPTION STANDARD  
(AES)

Menyatakan bahwa skripsi saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan di dalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 20 Juli 2023



Franli Chandra Thian

**LEMBAR PENGESAHAN SKRIPSI**

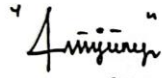
**IMPLEMENTASI PESAN TERSEMBUNYI PADA CITRA DIGITAL  
DENGAN ALGORITMA *LEAST SIGNIFICANT BIT* (LSB) DAN *ADVANCED  
ENCRYPTION STANDARD* (AES)**

Yang dipersiapkan dan disusun oleh

**FRANLI CHANDRA THIAN  
1911500005**

Telah dipertahankan di depan Dewan Penguji  
Pada tanggal 07 Agustus 2023

**Susunan Dewan Penguji  
Anggota**



**Dwi Yuny Sylfania, M.Kom  
NIDN. 0207069301**

**Kaprodi Teknik Informatika**

  
**Chandra Kirana, M.Kom  
NIDN. 0228108501**

**Dosen Pembimbing**



**Laurentinus, M.Kom  
NIDN. 0201079201**

**Ketua Penguji**



**Rahmat Sulaiman, M.Kom  
NIDN. 0208019401**

Skripsi ini telah diterima dan sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 15 Agustus 2023

**DEKAN FAKULTAS TEKNOLOGI INFORMASI  
SRIP ATMA LUHUR**

  
**Ellya Helmut, M.Kom  
NIDN. 0201027901**

## **KATA PENGANTAR**

Puji syukur kehadiran Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika Institut Sains dan Bisnis (ISB) Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Tuhan yang telah menciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, S.T., M.Sc., selaku Rektor ISB Atma Luhur.
5. Bapak Ellya Helmud, M.Kom, selaku Dekan Fakultas Teknologi Informasi.
6. Bapak Chandra Kirana, M. Kom Selaku Kaprodi Teknik Informatika.
7. Bapak Laurentinus, M.Kom. selaku dosen pembimbing.
8. Saudara dan sahabat-sahabatku terutama kawan-kawan angkatan 2019 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan karunia dan berkat-Nya, Amin.

Pangkalpinang, Juli 2023

Penulis

## **ABSTRACT**

*Currently, the development of information technology is rapid and has become one of the most important parts of human life. Therefore, data must be stored in a container that can strengthen data protection to ensure the confidentiality of data sent via media such as the Internet. Protecting data with cryptographic or steganographic methods alone is not enough, because there are weaknesses that third parties suspect in existing communication messages. Therefore, to cover the message, an application was developed for the media, namely an application with a combination of steganography and encryption, using the Least Significant Bit (LSB) method for steganography and Advanced Encryption Standard (AES) for encryption. The results of the developed application successfully convert text messages into digital images that are almost invisible from the original image, and can also be decoded without failure.*

**Keywords :** *Image Files, Steganography, LSB, Cryptography, AES*

## ABSTRAK

Saat ini perkembangan teknologi informasi sudah pesat dan telah menjadi salah satu bagian terpenting dalam kehidupan manusia. Oleh karena itu, data harus disimpan pada wadah yang dapat memperkuat perlindungan data untuk menjamin kerahasiaan data yang dikirimkan melalui media seperti Internet. Melindungi data dengan metode kriptografi atau steganografi saja tidak cukup, karena terdapat kelemahan yang dicurigai pihak ketiga dalam pesan komunikasi yang ada. Oleh karena itu, untuk menutupi pesan tersebut dikembangkan sebuah aplikasi untuk medianya yaitu aplikasi dengan kombinasi steganografi dan enkripsi, dengan memakai metode *Least Significant Bit* (LSB) untuk steganografi dan dilakukan *Advanced Encryption Standard* (AES) untuk enkripsi. Hasil dari aplikasi yang dikembangkan berhasil mengubah pesan teks menjadi gambar digital yang hampir tidak terlihat dari gambar aslinya, dan juga dapat didekodekan tanpa kegagalan.

Kata Kunci : *File Citra* , *Steganography*, *LSB*, *Cryptography*, *AES*

## DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN .....	ii
LEMBAR PENGESAHAN .....	iii
KATA PENGANTAR .....	ii
<i>ABSTRACT</i> .....	iv
ABSTRAK .....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR .....	viii
DAFTAR TABEL.....	x
DAFTAR SIMBOL.....	xi
BAB I PENDAHULUAN .....	1
1.1    Latar Belakang .....	1
1.2    Rumusan Masalah .....	2
1.3    Tujuan dan Manfaat Penelitian.....	3
1.3.1    Tujuan Penelitian .....	3
1.3.2    Manfaat Penelitian .....	3
1.4    Batasan Masalah.....	3
1.5    Sistematika Penulisan.....	4
BAB II LANDASAN TEORI .....	6
2.1    Model <i>Prototype</i> .....	6
2.2    Metode Pemrograman Berorientasi Obyek (OOP).....	7
2.3    UML (Unified Modelling Language).....	8
2.4    Implementasi .....	10
2.5    Steganografi.....	10
2.6    Kriptografi .....	13
2.6.1    Definisi .....	13
2.6.2    Metode.....	14
2.6.3    Algoritma AES ( <i>Advanced Encryption Standard</i> ).....	16
2.7    Citra Digital .....	23



2.8	Bahasa Pemrograman Java .....	24
2.9	Penelitian Terdahulu.....	25
BAB III METODOLOGI PENELITIAN .....		29
3.1	Model Pengembangan Perangkat Lunak .....	29
3.2	Metode Penelitian Pengembangan Perangkat Lunak .....	30
3.3	UML (Unified Modelling Language).....	30
3.4	Algoritma Pendukung.....	31
3.4.1	Algoritma LSB .....	31
3.4.2	Algoritma AES.....	32
BAB IV HASIL DAN PEMBAHASAN .....		47
4.1	Analisis Masalah .....	47
4.1.1	Analisis Kebutuhan .....	47
4.1.2	Analisis Sistem Berjalan .....	50
4.2	Perancangan Sistem.....	50
4.2.1	Analisis Sistem Usulan .....	50
4.2.2	Rancangan Sistem .....	51
4.2.3	Rancangan Layar.....	60
4.3	Implementasi .....	63
4.3.1	Tampilan Layar .....	63
4.3.2	Pengujian.....	67
BAB V PENUTUP.....		71
5.1	Kesimpulan.....	71
5.2	Saran.....	71
DAFTAR PUSTAKA .....		72
LAMPIRAN.....		74

## DAFTAR GAMBAR

	Halaman
Gambar 2.1 Contoh Use Case Diagram[8] .....	8
Gambar 2.2 Contoh Activity Diagram[8] .....	9
Gambar 2.3 Contoh Class Diagram[8].....	9
Gambar 2.4 Proses Embedding[2] .....	11
Gambar 2.5 Proses Ekstrasi[2].....	12
Gambar 2.6 Proses Enkripsi AES-256[5] .....	18
Gambar 2.7 Substitusi S-Box[5] .....	19
Gambar 2.8 Transformasi <i>ShiftRow</i> [5] .....	20
Gambar 2.9 Transformasi <i>mixcolumn</i> [5] .....	20
Gambar 2.10 Perkalian Matriks[5].....	20
Gambar 2.11 Proses Dekripsi AES-256[5] .....	21
Gambar 2.12 Transformasi <i>InvShiftRow</i> [5] .....	21
Gambar 2.13 Tabel Inverse S-Box[5] .....	22
Gambar 2.14 Matrik <i>InvMixColumns</i> [5].....	22
Gambar 2.15 Hasil Perkalian Matrik <i>InvMixColumns</i> [5] .....	23
Gambar 3.1 Rotasi Kolom Terakhir.....	34
Gambar 3.2 Hasil <i>SubBytes</i> .....	35
Gambar 3.3 Hasil dari XOR <i>Rcon</i> .....	36
Gambar 3.4 Penjelasan dari Hasil Round-2 .....	37
Gambar 3.5 Hasil Proses Ekspansi Key .....	38
Gambar 3.6 <i>Addroundkey</i> Round-1 .....	38
Gambar 3.7 Transformasi S-Box .....	39
Gambar 3.8 Proses <i>Shiftrows</i> .....	39
Gambar 3.9 Proses <i>MixColumns</i> Round-1 kolom 1 baris 1 .....	40
Gambar 3.10 Hasil Proses Enkripsi AES 256.....	41
Gambar 3.11 Bukti Kesesuaian Enkripsi AES 256 dengan tools AES converter..	42
Gambar 3.12 Bukti kesesuaian Hex dan Base64 .....	42
Gambar 3.13 Proses <i>InvAddroundkey</i> .....	43

Gambar 3.14 Proses InvShiftRows .....	43
Gambar 3.15 Proses InvSubBytes.....	43
Gambar 3.16 Tabel Inv S-Box .....	44
Gambar 3.17 Proses XOR dengan RoundKeys 14 .....	44
Gambar 3.18 Proses InvMixColumns .....	45
Gambar 3.19 Hasil Proses InvMixColumns round-13 .....	45
Gambar 3.20 Hasil Keseluruhan Proses Dekripsi AES 256 .....	46
Gambar 4.1 Activity Diagram Proses Sistem Berjalan .....	50
Gambar 4.2 Activity Diagram Analisis Sistem Usulan .....	51
Gambar 4.3 Use Case Diagram Aplikasi .....	52
Gambar 4.4 Activity Diagram Enkripsi Pesan.....	55
Gambar 4.5 Activity Diagram Dekripsi Penerima.....	56
Gambar 4.6 Sequence Diagram Form Login .....	57
Gambar 4.7 Sequence Diagram Form Utama .....	58
Gambar 4.8 Sequence Diagram Steganography Encode.....	59
Gambar 4.9 Sequence Diagram Steganography Decode .....	60
Gambar 4.10 Rancangan Layar Login .....	60
Gambar 4.11 Rancangan Layar Menu Utama.....	61
Gambar 4.12 Rancangan Layar Encode.....	61
Gambar 4.13 Rancangan Layar Decode.....	62
Gambar 4.14 Tampilan Layar Login.....	63
Gambar 4.15 Tampilan Layar Halaman Utama .....	64
Gambar 4.16 Tampilan Layar Encode Steganography .....	65
Gambar 4.17 Menu Open Image.....	65
Gambar 4.18 Tampilan Layar Menu Decode Steganography.....	66
Gambar 4.19 Output Hasil NetBeans 8.2 Encode.....	68

## DAFTAR TABEL

	Halaman
Tabel 2.1 Perbandingan AES[5] .....	16
Tabel 2.2 Tinjauan Penelitian Terdahulu .....	25
Tabel 3.1 Blok Kunci .....	33
Tabel 3.2 Konversi Nilai ASCII.....	33
Tabel 3.3 Konversi Blok Kunci .....	34
Tabel 3.4 Tabel S-Box .....	35
Tabel 3.5 Tabel Rcon .....	36
Tabel 4.1 Use Case Description Login .....	52
Tabel 4.2 Use Case Description Enkripsi .....	53
Tabel 4.3 Use Case Description Dekripsi .....	53
Tabel 4.4 Use Case Description Logout .....	54
Tabel 4.5 Identifikasi Kebutuhan Fungsional .....	67
Tabel 4.6 Identifikasi Kebutuhan Non-fungsional.....	68
Tabel 4.7 Pengujian Algoritma .....	69

## DAFTAR SIMBOL

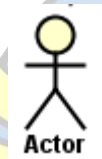
### 1. Simbol Use Case Diagram

Use case



Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau *actor*, biasanya dinyatakan dengan kata kerja di awal *frase* nama *use case*.

Actor



Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang dibuat itu sendiri, jadi walaupun simbol dalam *actor* adalah gambar, tetapi *actor* belum tentu merupakan orang. Biasanya dinyatakan menggunakan kata benda di awal *frase* nama aktor.

Asosiasi (*Association*)



Komunikasi antar aktor dan use case yang berpartisipasi pada use case atau use case memiliki interaksi dengan aktor.

Ekstensi (*Extend*)



Relasi use case tambahan ke sebuah use case di mana use case yang ditambahkan dapat berdiri sendiri walau tanpa use case tambahan itu, mirip dengan prinsip *inheritance* pada pemrograman berorientasi objek, biasanya use case tambahan memiliki nama depan yang sama dengan nama use case yang ditambahkan.

Generalisasi  
(*Generalization*)



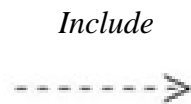
Hubungan generalisasi dan spesialisasi (umum-khusus) antara dua buah use case di mana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.

Relasi use case tambahan ke use case di mana use case yang ditambahkan memerlukan use case ini untuk menjalankan fungsinya atau sebagai syarat dijalankannya use case ini. Ada 2 sudut pandang yang cukup besar mengenai *include* di use case:

*Include* berarti use case yang ditambahkan akan selalu di panggil saat use case tambahan dijalankan.

*Include* berarti use case yang tambahan apakah use case yang ditambahkan telah dijalankan.

Kedua interpretasi di atas dapat di anut salah satu atau keduanya tergantung pada pertimbangan interpretasi yang dibutuhkan.



## 2. Simbol Activity Diagram

Status Awal (*Initial State*)



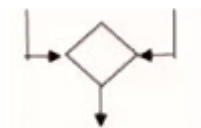
Status awal aktifitas sebuah sistem.

Aktifitas



Aktifitas yang dilakukan sistem, aktifitas biasanya diawali dengan kata kerja.

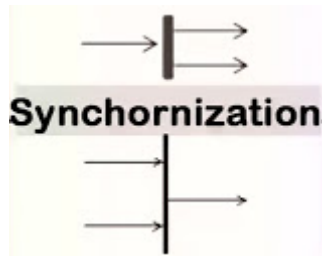
*Decision*



Asosiasi jika ada pilihan aktifitas lebih dari satu.

*Synchronization (Fork, Join)*

Asosiasi untuk menggambarkan gabungan (join) maupun percabangan (fork) aktifitas.



Status akhir (*Final state*)



Status akhir yang dilakukan sebuah sistem.

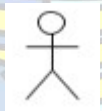
*Swimlane*



Memisahkan aktifitas yang satu dengan aktifitas yang lainnya.

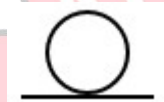
### 3. Simbol *Sequence Diagram*

*Actor*



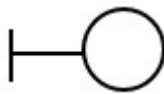
Menggambarkan orang yang berinteraksi dengan sistem.

*Entity Class*



Menggambarkan hubungan kegiatan yang akan dilakukan.

*Boundery Class*



Menggambarkan sebuah penggambaran dari sebuah *form*.

*Control Class*



Menggambarkan hubungan antar *boundry* dengan tabel.

*Lifeline*

Menggambarkan tempat mulai dan berakhirnya sebuah pesan.



*Line Message*



Menggambarkan pengiriman pesan.

