

**IMPLEMENTASI PENYISIPAN PESAN TEKS PADA CITRA
DIGITAL DENGAN LSB DAN AES 256**

SKRIPSI



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG
2020/2021**

**IMPLEMENTASI PENYISIPAN PESAN TEKS PADA
CITRA DIGITAL DENGAN LSB DAN AES 256**

SKRIPSI

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



Oleh :
Andre Chandra
171150007

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG
2020/2021**

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 1711500007

Nama : Andre Chandra

Judul Skripsi : IMPLEMENTASI PENYISIPAN PESAN TEKS PADA CITRA
DIGITAL DENGAN LSB DAN AES 256

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, 9 Agustus 2021



Andre Chandra

LEMBAR PENGESAHAN SKRIPSI

**IMPLEMENTASI PENYISIPAN PESAN TEKS PADA
CITRA DIGITAL DENGAN LSB DAN AES 256**

Yang dipersiapkan dan disusun oleh

**Andre Chandra
171150007**

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 9 Agustus 2021

**Susunan Dewan Penguji
Anggota**



**Devi Irawan, M.Kom
NIDN. 0231018201**

Dosen Pembimbing



**Yohanes Setiawan, M.Kom.
NIDN. 0219068501**

Kaprodi Teknik informatika


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

Ketua Penguji



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

Skripsi ini telah diterima dan sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 16 Agustus 2021

DEKAN FAKULTAS TEKNOLOGI INFORMASI

ISB ATMA LUHUR

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

KATA PENGANTAR

Puji syukur kehadirat 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 Chandra Kirana, M.Kom. Selaku Kaprodi Teknik Informatika.
6. Bapak Yohanes Setiawan, M.Kom. selaku dosen pembimbing.
7. Saudara dan sahabat-sahabatku terutama kawan-kawan angkatan 2017 yang telah memberikan dukungan moral untuk terus menyelesaikan skripsi ini.

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

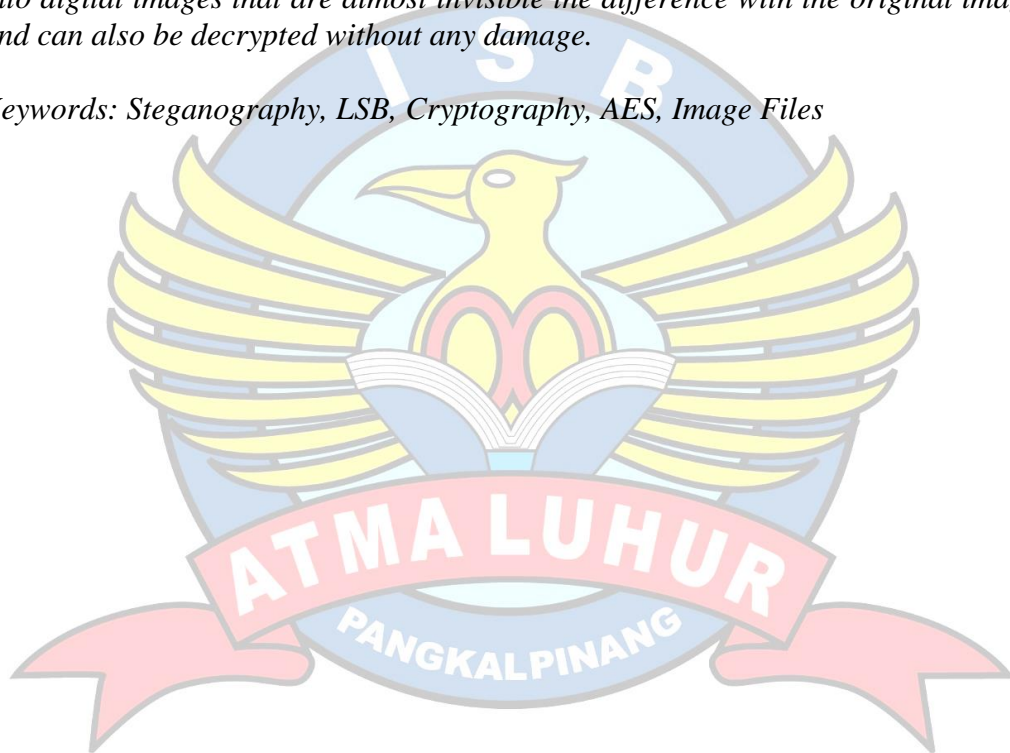
Pangkalpinang, Agustus 2021

Penulis

ABSTRACT

In this modern era, the use of global networks such as the internet has become public communication and can be accessed almost anywhere. Therefore, a high level of data security is needed so that communication is not accessed by just anyone. Data security with cryptographic or steganographic methods is not enough because it has loopholes that make third parties suspicious of existing communication messages, so an application was developed to disguise the message on a medium, namely an application with a combination of steganography and cryptography using the Least Significant Bit (LSB) method to steganography and Advanced Encryption Standard (AES) for cryptography. With the results of the developed application, it succeeded in disguising text messages into digital images that are almost invisible the difference with the original image and can also be decrypted without any damage.

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



ABSTRAK

Di zaman modern ini, penggunaan jaringan *global* seperti internet sudah menjadi komunikasi umum masyarakat dan dapat diakses hampir dimanapun. Oleh karena itu dibutuhkan suatu keamanan data dengan tingkat yang tinggi agar komunikasi tidak diakses oleh sembarang orang. Pengamanan data dengan metode kriptografi atau steganografi tidak cukup karena mempunyai celah yang membuat pihak ketiga curiga dengan pesan komunikasi yang ada, maka dikembangkanlah suatu aplikasi untuk menyamarkan pesan tersebut pada suatu media yaitu aplikasi dengan kombinasi steganografi dan kriptografi menggunakan metode *Least Significant Bit*(LSB) untuk steganografi dan *Advanced Encryption Standar*(AES) untuk kriptografi. Dengan hasil aplikasi yang dikembangkan berhasil menyamarkan pesan teks ke citra digital yang hampir tidak terlihat perbedaannya dengan gambar yang asli dan juga dapat didekripsi tanpa adanya kerusakan.

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



DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN SKRIPSI	ii
KATA PENGANTAR	iii
ABSTRACT	iv
ABSTRAK	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	xi
DAFTAR SIMBOL	xii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan dan Manfaat Penelitian	4
1.4. Batasan Masalah	4
1.5. Sistematika Penulisan	5
BAB II LANDASAN TEORI	7
2.1 Model Waterfall	7
2.2 Metode Pemrograman Berorientasi Obyek (OOP)	12
2.3 UML (Unified Modelling Language)	14
2.4 Implementasi	24
2.5 Steganografi	25
2.6 Kriptografi	30
2.6.1 Definisi	30
2.6.2 Metode	32
2.6.3 Terminologi	34
2.6.4 Algoritma AES (Advanced Encryption Standard)	35
2.7 Citra Digital	42
2.8 Bahasa Pemrograman Java	45
2.9 Penelitian Terdahulu	47

BAB III METODOLOGI PENELITIAN	51
3.1 Model Penelitian.....	51
3.1.1 Model SDLC	51
3.2 Object Oriented Programming (OOP).....	52
3.3 UML (Unified Modelling Language)	52
3.4 Algoritma Pendukung.....	53
3.4.1 Algoritma LSB	53
3.4.2 Algoritma AES	55
BAB IV HASIL DAN PEMBAHASAN	78
4.1 Perencanaan	78
4.2 Analisis Masalah	78
4.2.1 Analisis Kebutuhan	79
4.2.2 Analisis Sistem Berjalan.....	82
4.3 Perancangan Sistem.....	82
4.3.1 Analisis Sistem Usulan.....	82
4.3.2 Rancangan Sistem	83
4.3.3 Rancangan Layar	92
4.4 Implementasi	95
4.4.1 Tampilan Layar.....	95
4.4.2 Pengujian	100
BAB V PENUTUP.....	106
5.1 Kesimpulan.....	106
5.2 Saran	106
DAFTAR PUSTAKA	107
LAMPIRAN.....	109

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Fase Dasar Pengembangan Sistem[9]	7
Gambar 2.2 Model Waterfall[11].....	11
Gambar 2.3 Contoh Use Case Diagram[14]	14
Gambar 2.4 Contoh Activity Diagram[14]	15
Gambar 2.5 Contoh Class Diagram[14].....	17
Gambar 2.6 Contoh Sequence Diagram[15]	18
Gambar 2.7 Contoh Package Diagram[15]	18
Gambar 2.8 Contoh State Diagram[14]	19
Gambar 2.9 Contoh Communication Diagram[14].....	20
Gambar 2.10 Contoh Composite Structur Diagram[15]	20
Gambar 2.11 Contoh Object Diagram[14].....	21
Gambar 2.12 Contoh Timing Diagram[15].....	22
Gambar 2.13 Contoh Component Diagram[14].....	23
Gambar 2.14 Contoh Deployment Diagram[14].....	23
Gambar 2.15 Contoh Interaction Overview Diagram[14]	24
Gambar 2.16 Proses Embedding Citra[7]	28
Gambar 2.17 Proses Ekstrasi Citra[7].....	28
Gambar 2.18 Proses Enkripsi AES-256[5]	37
Gambar 2.19 formula Addroundkey AES[5]	38
Gambar 2.20 Substitusi S-Box[5]	38
Gambar 2.21 Transformasi ShiftRow[5]	39
Gambar 2.22 Transformasi mixcolumns[5]	39
Gambar 2.23 Perkalian Matriks[5].....	40
Gambar 2.24 Proses Dekripsi AES-256[5]	40
Gambar 2.25 Transformasi InvShiftRows[5].....	41
Gambar 2.26 Tabel Inverse S-Box[5]	41
Gambar 2.27 Matrik InvMixColumns[5].....	42

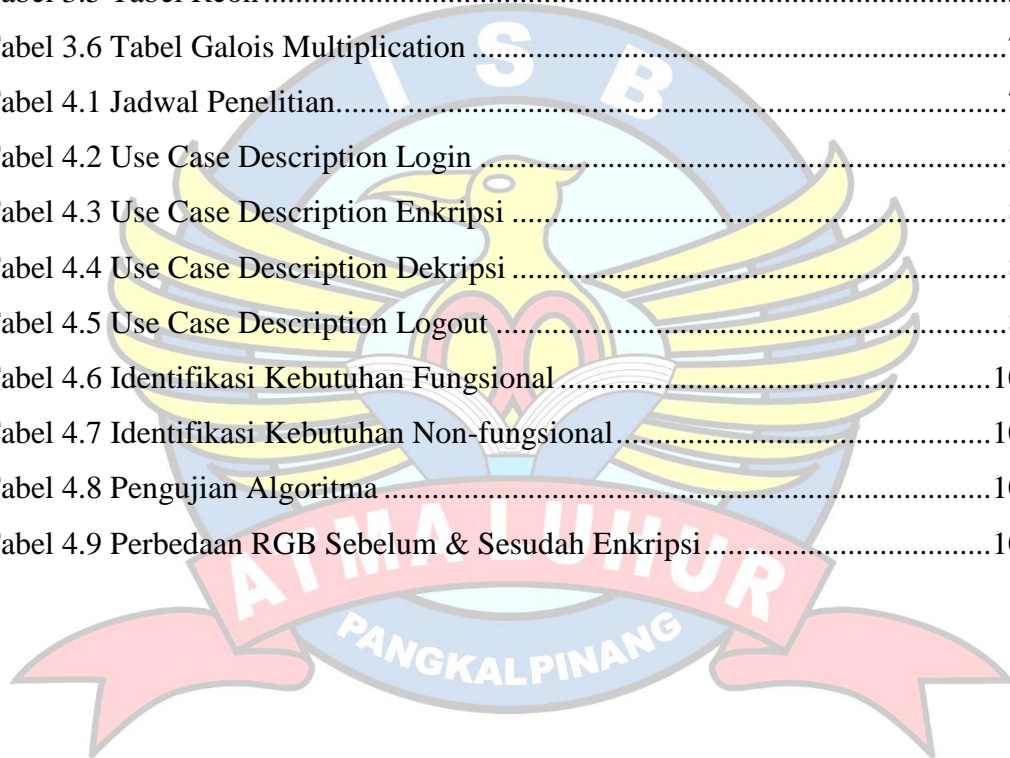
Gambar 2.28 Hasil Perkalian Matrik InvMixColumns[5]	42
Gambar 2.29 Lingkungan Pemrograman Java[24]	46
Gambar 3.1 Rotasi Kolom Terakhir	57
Gambar 3.2 Hasil SubBytes	58
Gambar 3.3 Hasil XOR Rcon ke-1	59
Gambar 3.4 Penjelasan Hasil Round-2 dan Round-3.....	59
Gambar 3.5 Proses RoundKey Kunci Round 0 dan Round 1	60
Gambar 3.6 Hasil Proses Ekspansi Key	
ISBATMALUHURKAMPUSBANGKABELITUNG	61
Gambar 3.7 Addroundkey Round-1	62
Gambar 3.8 Transformasi S-Box	62
Gambar 3.9 Proses Shiftrows	63
Gambar 3.10 Proses MixColumns Round-1 kolom 1 baris 1	63
Gambar 3.11 Proses MixColumns kolom 1 baris 2	64
Gambar 3.12 Hasil Proses Enkripsi AES 256.....	65
Gambar 3.13 Bukti Kecocokan Enkripsi AES 256 Menggunakan AES converter online.....	66
Gambar 3.14 Bukti kecocokan Hex dan Base64.....	66
Gambar 3.15 Proses InvAddroundkey	67
Gambar 3.16 Proses InvShiftRows	67
Gambar 3.17 Proses InvSubBytes.....	68
Gambar 3.18 Tabel Inv S-Box	68
Gambar 3.19 Proses InvMixColumns	69
Gambar 3.20 Hasil Proses InvMixColumns round-13.....	76
Gambar 3.21 Hasil Keseluruhan Proses Dekripsi AES 256	77
Gambar 4.1 Activity Diagram Proses Sistem Berjalan	82
Gambar 4.2 Activity Diagram Analisis Sistem Usulan	83
Gambar 4.3 Use Case Diagram Aplikasi	84
Gambar 4.4 Activity Diagram Enkripsi Pesan.....	87
Gambar 4.5 Activity Diagram Dekripsi Penerima.....	88
Gambar 4.6 Sequence Diagram Form Login	89

Gambar 4.7 Sequence Diagram Form Utama	90
Gambar 4.8 Sequence Diagram Form Encode	91
Gambar 4.9 Sequence Diagram Form Decode	92
Gambar 4.10 Rancangan Layar Login	92
Gambar 4.11 Rancangan Layar Menu Utama	93
Gambar 4.12 Rancangan Layar Encode	93
Gambar 4.13 Rancangan Layar Decode	94
Gambar 4.14 Tampilan Layar Login	95
Gambar 4.15 Tampilan Layar login(2)	96
Gambar 4.16 Tampilan Layar login(3)	96
Gambar 4.17 Tampilan Layar Halaman Menu Utama	96
Gambar 4.18 Menu Bantuan Halaman Utama	97
Gambar 4.19 Tampilan Layar Encode Steganography	97
Gambar 4.20 Menu Open Image	98
Gambar 4.21 Menu Bantuan Encode Steganography	99
Gambar 4.22 Tampilan Layar Menu Decode Steganography	99
Gambar 4.23 Menu Bantuan Decode Steganography	100
Gambar 4.24 Output NetBeans 8.1 Bagian Encode Image	102




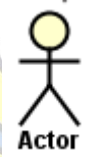
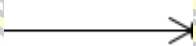



DAFTAR TABEL

	Halaman
Tabel 2.1 Perbandingan AES[5]	36
Tabel 2.2 Tinjauan Penelitian Terdahulu	47
Tabel 3.1 Blok Kunci	56
Tabel 3.2 Konversi Nilai ASCII.....	56
Tabel 3.3 Konversi Blok Kunci	57
Tabel 3.4 Tabel S-Box	58
Tabel 3.5 Tabel Rcon	59
Tabel 3.6 Tabel Galois Multiplication	70
Tabel 4.1 Jadwal Penelitian.....	78
Tabel 4.2 Use Case Description Login	84
Tabel 4.3 Use Case Description Enkripsi	85
Tabel 4.4 Use Case Description Dekripsi	85
Tabel 4.5 Use Case Description Logout	86
Tabel 4.6 Identifikasi Kebutuhan Fungsional	101
Tabel 4.7 Identifikasi Kebutuhan Non-fungsional.....	101
Tabel 4.8 Pengujian Algoritma	102
Tabel 4.9 Perbedaan RGB Sebelum & Sesudah Enkripsi.....	103



DAFTAR SIMBOL

1. Simbol *Use Case Diagram*

<p><i>Use case</i></p> 	<p>Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau <i>actor</i>, biasanya dinyatakan dengan kata kerja di awal <i>frase</i> nama <i>use case</i>.</p>
<p><i>Actor</i></p> 	<p>Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang dibuat itu sendiri, jadi walaupun simbol dalam <i>actor</i> adalah gambar, tetapi <i>actor</i> belum tentu merupakan orang. Biasanya dinyatakan menggunakan kata benda di awal <i>frase</i> nama aktor.</p>
<p>Asosiasi (<i>Association</i>)</p> 	<p>Komunikasi antar aktor dan use case yang berpartisipasi pada use case atau use case memiliki interaksi dengan aktor.</p>
<p>Ekstensi (<i>Extend</i>)</p> 	<p>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 <i>inheritance</i> pada pemrograman berorientasi objek, biasanya use case tambahan memiliki nama depan yang sama dengan nama use case yang ditambahnya.</p>
<p>Generalisasi (<i>Generalization</i>)</p> 	<p>Hubungan generalisasi dan spesialisasi (umum-khusus) antara dua buah use case di mana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.</p>
<p><i>Include</i></p> 	<p>Relasi use case tambahan ke use case di</p>



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.

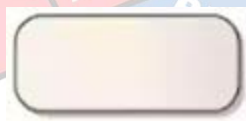
2. Simbol Activity Diagram

Status Awal (*Initial State*)



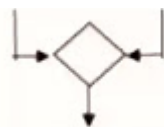
Status awal aktifitas sebuah sistem.

Aktifitas



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

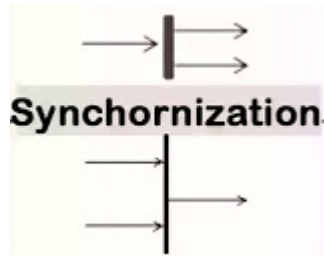
Decision



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.

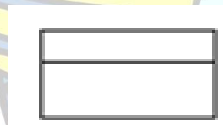
Swimlane



Memisahkan aktifitas yang satu dengan aktifitas yang lainnya.

3. **Simbol Class Diagram**

Kelas (*class*)



Kelas pada struktur sistem



Antarmuka (*Interface*)

Sama dengan prinsip *interface* dalam pemrograman berorientasi objek.



Asosiasi (*Association*)

Relasi antar kelas dengan makna umum, asosiasi biasanya juga disertai dengan *multiplicity*.



Asosiasi berarah (*Directed Association*)


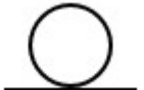
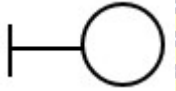



Relasi antar kelas dengan makna kelas yang satu digunakan oleh kelas yang lain, asosiasi berarah biasanya juga disertai dengan *multiplicity*.



Relasi antar kelas dengan makna generalisasi-spesialisasi (umum-

Generalisasi (<i>Generalization</i>)	----->	Relasi antar kelas dengan makna khusus).
Kebergantungan (<i>Dependency</i>)	----->	Relasi antar kelas dengan makna kebergantungan antar kelas.
Agregasi (<i>Aggregation</i>)	----->◇	Relasi antar kelas dengan makna semua bagian (whole-part).

4. Simbol *Sequence Diagram*

<i>Actor</i>		Menggambarkan orang yang berinteraksi dengan sistem.
<i>Entity Class</i>		Menggambarkan hubungan kegiatan yang akan dilakukan.
<i>Boundary Class</i>		Menggambarkan sebuah penggambaran dari sebuah <i>form</i> .
<i>Control Class</i>		Menggambarkan hubungan antar <i>boundary</i> dengan tabel.
<i>Lifeline</i>		Menggambarkan tempat mulai dan berakhirnya sebuah pesan.
<i>Line Message</i>		Menggambarkan pengiriman pesan.