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	**Dosen Pembimbing**
Anggota	
Dwi Yuny Sylfania, M.Kom	**Laurentinus, M.Kom**
NIDN. 0207069301	**NIDN. 0201079201**
Kaprodi Teknik Informatika	**Ketua Penguji**
Chandra Kirana, M.Kom	**Rahmat Sulaiman, M.Kom**
NIDN. 0228108501	**NIDN. 0208019401**

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

DEKAN FAKULTAS TEKNOLOGI INFORMASI
ISB ATMA LUHUR

Elya Helmud, M.Kom
NIDN. 0201027901

ii

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 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

DAFTAR GAMBAR

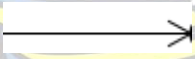
Halaman

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

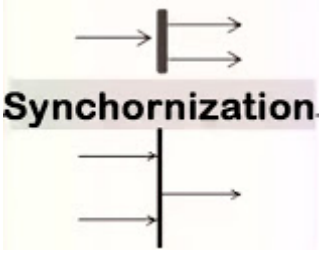
1. Simbol *Use Case Diagram*

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 walapun 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 ditambahkannya.
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 	*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 ditambahan telah dijalankan. Kedua interprestasi di atas dapat di anut salah satu atau keduanya tergantung pada pertimbangan interprestasi 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 mengambarkan gabungan (join) maupun percabangan (fork) aktifitas.



Status akhir (*Final state*)

Status akhir yang dilakukan sebuah sistem.

Swimlane

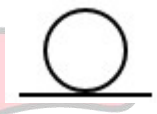
Memisakan aktifitas yang satu dengan aktifitas yang lainnya.

3. Simbol *Sequence Diagram*

Actor

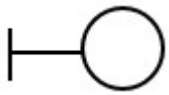
Menggambarkan orang yang berinteraksi dengan sistem.

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 pemgiriman pesan.