# Perancangan dan Desain Aplikasi Anti-forensic untuk Penyembunyian Pesan didalam Media Digital

**I Wayan Ardiyasa**
(STMIK) STIKOM Bali
Jalan Raya Puputan, No. 86 Renon Denpasar Bali, (0361) 244445, (STMIK) STIKOM Bali
e-mail:ardi@stikom-bali.ac.id

***Abstrak***

*Keamanan suatu informasi sangat penting, mengingat teknologi semakin canggih serta minimnya pengetahuan pengguna tentang privasi suatu informasi. Kejahatan cyber semakin hari semakin meningkat, ini pula menjadi suatu permasalahan yang sangat serius. Dampak dari meningkatnya akan kebutuhan informasi dan penggunaan teknologi. Maka dibutuhkan suatu teknik atau cara yang menghasilkan suatu aplikasi yang mampu mengamankan suatu pesan yang sifatnya rahasia yang mana tidak menyalahi suatu aturan hukum dan melindungi hak privasi pengguna di jaringan internet. Penerapan Teknik Anti Forensic didalam penyembunyian pesan bertujuan agar pesan yang dikirimkan aman, sehingga tidak diketahui oleh orang yang tidak bertanggung jawab. Salah satu Teknik Anti forensic yang digunakan adalah dengan menerapkan kriptografi dengan steganography.*

***Kata kunci:*** *Kriptografi, Steganografi, Anti-Forensic, cyber.*

## 1. Pendahuluan

### 1.1 Latar Belakang

Perkembangan internet saat ini mengalami peningkatan yang signifikan. Dilihat dari penggunaan internet, hampir setiap masyarakat sudah membutuhkan internet untuk mengakses suatu informasi. Dilihat dari hal itu, Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. [1]

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam *development,* algoritma-algoritma dan teknik-teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima. [1]

Keamanan suatu informasi sangat penting, mengingat teknologi semakin canggih serta minimnya pengetahuan pengguna tentang privasi suatu informasi. Kejahatan *cyber* semakin hari semakin meningkat, ini pula menjadi suatu permasalahan yang sangat serius. Dampak dari meningkatnya akan kebutuhan informasi dan penggunaan teknologi. Maka dibutuhkan suatu teknik atau cara yang menghasilkan suatu aplikasi yang mampu mengamankan suatu pesan yang sifatnya rahasia yang mana tidak menyalahi suatu aturan hukum dan melindungi hak privasi pengguna di jaringan internet.

Teknik anti f*orensic* merupakan salah satu ilmu yang bertujuan untuk menjaga kerahasiaan data (confidentiality) atau menjaga privasi, agar suatu data digital yang bernilai penting tidak dapat ditemukan atau diketahui oleh pihak lain. [2] Penerapan Teknik Anti-*Forensic* didalam penyembunyian pesan bertujuan agar pesan yang dikirimkan aman, sehingga tidak diketahui oleh orang yang tidak bertanggung jawab. Salah satu Teknik Anti *forensic* yang digunakan adalah dengan menerapkan kriptografi dan *steganography*. Kriptografi meupakan suatu ilmu seni penyandian pesan sedangkan *Steganography* merupakan teknik penyembunyian pesan didalam sebuah media gambar. Dengan penerapan teknik anti-*forensic* untuk pengamanan pesan dalam media gambar bisa menjadi pilihan untuk mengurangi tindak kejahatan *cyber* yang merugikan pengguna dalam hal ini adalah keamanan suatu pesan.

### 1.2 Rumusan Masalah

Adapun rumusan masalah dari latar belakang diatas adalah sebagai berikut:

Bagaimana perancangan aplikasi Anti-*Forensic* untuk mengamankan suatu pesan dengan menggunakan kriptografi *Triple* DES dan steganograpi metode *Least Significant Bit* (LSB) untuk melakukan penyandian pesan dan penyembunyian pesan dalam media digital?

## 2. Tinjauan Pustaka

### 2.1 Anti-*Forensic*

*Computer* Anti-*Forensic* (Liu dan Brown, 2006) adalah "*Application of the scientific method to digital media in order to invalidate factual information for judicial review* ". Komputer Forensik menitik beratkan kepada tindakan mencari, menemukan dan menjaga integritas data digital, maka Anti-*Forensic* justru berfokus sebaliknya, yaitu menjaga agar data tetap aman dan tidak dapat diakses (kecuali oleh pemilik data aslinya). Anti-*Forensic* merupakan bidang TI yang legal, karena dari segi manfaat dan tujuannya membantu meningkatkan keamanan data dan menjaga privasi. Tujuan utama dari Anti-*Forensic* adalah mengagalkan investigasi atau menyulitkan *investigator* dalam mencari dan menemukan bukti digital (*digital evidence*).

### 2.2 Teknik Anti-*Forensic*

Dr. Marcus K. Rogers, mengelompokan anti forensik berdasarkan jenis dan tujuannya. Anti Forensik dikelompokan berdasarkan tujuan teknik tersebut seperti Menyembunyikan Data (dengan teknik enkripsi, steganografi, *anomizer, split*), Penghapusan Jejak (*history*), dan Merubah Integritas Data. Adapun teknik anti *forensic* adalah sebagai berikut:

a. Data *Hidding*
   Tujuan dari proses pengamanan dengan menyembunyikan data agar tidak dapat ditemukan oleh investigator pada saat melakukan proses pencarian (investigasi).
b. Steganografi
   *Steganografi* (*Steganography*) berasal dari bahasa Yunani *steganos* (*hidden*) dan *gráphein* (*writing*). Jadi, *steganografi* berarti *hidden writing* (tulisan tersembunyi). Steganografi adalah seni dan ilmu menyembunyikan pesan ke dalam sebuah media dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa sebenarnya ada suatu pesan rahasia. Pada steganografi modern, arti steganografi berkembang menjadi penyembunyian informasi pada sebuah media file digital, bisa berupa media gambar, suara ataupun video. [4]
c. Kriptografi
   Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Kriptografi (*Cryptography*) berasal dari bahasa Yunani yaitu "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Terdapat 2 jenis algoritma dalam kriptografi, yaitu algoritma kriptografi Simetris dan Asimetris. Algoritma kriptografi simetris adalah algoritma yang menggunakan kunci yang sama baik untuk proses enkripsi maupun untuk proses dekripsi. Sedangkan algoritma kriptografi asimetris, kunci yang digunakan untuk proses enkripsi berlainan dengan kunci untuk melakukan proses dekripsi. Untuk jenis algoritma yang terakhir, kunci- kunci yang digunakan disebut dengan kunci *public* dan kunci *private*. [3]

### 2.3 *Least Significant Bit*

*Least Significant Bit* (LSB) *Coding*. Metoda ini merupakan metoda yang sederhana. Metoda ini akan mengubah nilai *Least Significant Bit* komponen luminansi atau warna menjadi bit yang bersesuai dengan bit label yang akan disembunyikan. Memang metoda ini akan menghasilkan video rekontruksi yang sangat mirip dengan aslinya, karena hanya mengubah nilai bit terakhir dari data. Metoda ini paling mudah diserang, karena bila orang lain tahu maka tinggal membalikkan nilai dari LSB-nya maka data label akan hilang seluruhnya. [6]

### 2.4 *Triple DES*

Pada Algoritma *Triple* DES, teks dienkrip dalam blok-blok 64-bit dengan menggunakan 56-bit kunci internal. Kunci internal berasal dari kunci eksternal yang panjangnya 64-bit. Blok-blok teks input tersebut ditransformasikan kedalam blok-blok *output* 64-bit juga dengan menggunakan beberapa tahapan. [3]
Tiga tahapan besar dalam DES yaitu:
a. *Plaintext* yang berukuran 64 bit dipermutasi dengan *matriks* permutasi awal.
b. Hasil permutasi awal kemudian di-*enciphering* sebanyak 16 kali (16 putaran).
c. Setiap putaran menggunakan kunci internal yang berbeda.

c. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok *cipherteks*.

Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES. Sehingga menghasilkan pra-*cipherteks* pertama. Tahap kedua, pra-cipherteks pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma DES. Sehingga menghasilkan prs-cipherteks kedua. Tahap terakhir, pra-cipherteks kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan cipherteks (C).

## 3. Metode Penelitian

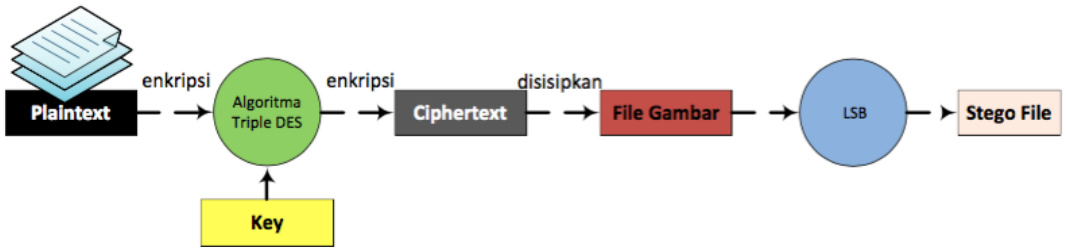
Adapun metode penelitian yang digunakan adalah sebagai berikut :


Gambar 1. Metode Penelitian

## 3. Hasil dan Pembahasan

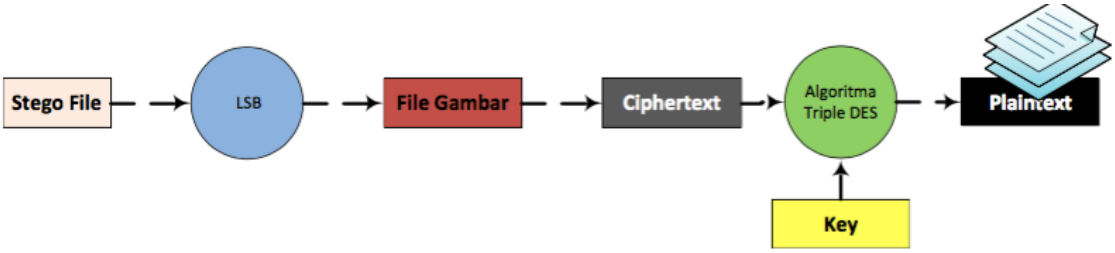
### 3.1 Arsitektur Sistem

Teknik *Anti-Forensic* merupakan teknik yang digunakan untuk mempersulit ahli *forensic* didalam melakukan investigasi untuk mendapatkan barang bukti. Dengan teknik anti-forensic ini, penelitian ini dibuat untuk mengamankan suatu pesan rahasia kedalam sebuah media digital berupa gambar dengan format .bmp. Tujuan digunakan teknik *anti-forensic* yaitu ketika terjadi suatu kegiatan *intercept* maka mampu memberikan sebuah pilihan solusi untuk mengamankan sebuah pesan digital. Berikut ini alur atau artsitektur sistem secara umum :




Gambar 2. Proses Enkripsi dan *hidding* pesan

Pada Gambar 2. Sebuah pesan rahasia akan dilakukan enkripsi menggunakan *Triple DES* dengan menginputkan sebuah *key* dimana *key* disini menjadi penyederhanaan dari 3 *key* yaitu K = K1=K2=K3. Ketika dilakukan enkripsi maka dihasilkan pesan *ciphertext*, pada pesan *ciphertext* ini akan di*hidding* kedalam sebuah gambar dengan metode LSB kemudian dihasilkan sebuah file gambar yang sudah terdapat sebuah pesan rahasia yang sudah terenkripsi dengan hasil file stego.




Gambar 3. Proses Dekripsi dan *extract* pesan

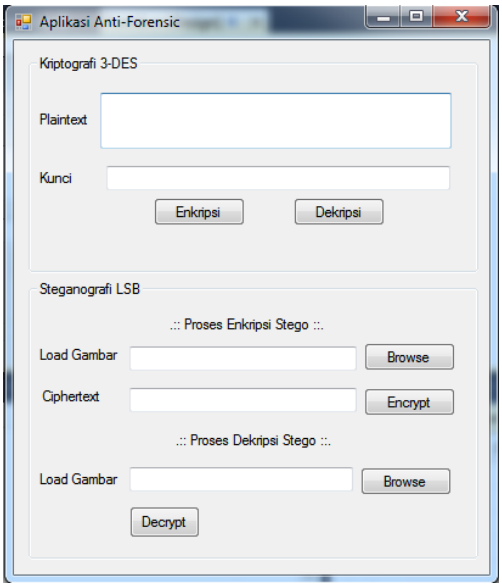
Pada Gambar 3. Dimana tahap melakukan proses dekripsi. Proses dekripsi disini dimulai dari file stego yang memiliki pesan rahasia didekripsi dengan metode LSB dimana bertujuan untuk memisahkan antara file gambar dan pesan *ciphertext*. Setelah didapatkan file ciphertext dilanjutkan dengan melakukan dekripsi dengan mencocokan *key* yang sudah digunakan dengan menggunakan algoritma *Triple DES*.

### 3.2 Hasil

Enkripsi merupakan suatu ilmu seni didalam melakukan penyandian suatu pesan. Pesan yang sifatnya rahasia akan dirubah menjadi *ciphertext* dalam proses enkripsi yang bertujuan untuk mengacak *plaintext* sehingga sulit untuk dipahami makna dari pesan tersebut. Pada kriptografi menggunakan algoritma *Triple DES* untuk penyandian pesan aslinya menjadi ciphertext. Pesan *ciphertext* tersebut akan disisipkan atau disembunyikan kedalam sebuah media digital berupa file gambar dengan format .bmp. Penggunaan dengan gambar format .bmp karena sederhana, tidak dikompresi, sehingga setiap *pixel* menyatakan nilai keabuan secara langsung. Penggunaan metode *Least Significant Bit* (LSB) pada Steganografi digunakan untuk penanaman pesan kedalam sebuah citra gambar, dimana seluruh *byte* dari gambar akan dirumah menjadi bit dari suatu pesan rahasia. Hasil dari penelitian ini adalah rancangan dan desain awal dari aplikasi dan penerapan Algoritma *Triple* DES dan *Least Significant Bit* untuk penyembunyian pesan didalam sebuah media digital berupa gambar. Dengan begitu, hasil dari penelitian ini bisa digunakan untuk tahap berikutnya yaitu ketahap *coding* dan implementasi.

#### 3.2.1 Prancangan dan Desain Aplikasi

Pada perancangan dan desain aplikasi anti-forensic menggunakan visual C# dengan memiliki dua tahap yaitu tahap pertama pesan rahasia akan dilakukan enkripsi dengan *Triple DES* setelah dihasilkan ciphertext maka dilakukan penyembunyian pesan kedalam sebuah gambar atau *hidding secret message* dengan metode LSB kedalam media digital berupa gambar. Berikut ini adalah desain aplikasi anti-*forensic*:




Gambar 4. Perancangan Anti-*Forensic*

Dengan menggunakan kriptografi dan Steganografi didalam pengamanan sebuah pesan digital membantu untuk mencegah pencurian pesan rahasia. Keamanan algortima berlapis yang dipadukan dengan metode LSB mampu mengurangi resiko ataupun keinginan seseorang yang tidak bertanggung jawab untuk melakukan serangan yang bersifat *destruktif.*

#### 3.2.2 Keunggulan Algoritma

Didalam penelitian ini, terdapat keunggulan yang bisa dipaparkan untuk algoritma Triple DES dan Steganograpi LSB, yaitu:

1. Keunggulan Triple DES
   Algoritma Triple DES menggunakan kunci (*k*) sejumlah tiga kunci dengan panjang kunci 168-bit dengan masing-masing panjang kunci 56-bit. Pada Triple DES menggunakan satu kunci lainnya sama dengan kunci pertama. Dengan penggunaan algoritma Triple DES pengamanan data menjadi lebih aman.
2. Keunggulan Steganograpi dengan metode LSB

Metode LSB adalah suatu teknik dimana mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Dimana, bit yang diganti hanyalah bit yang paling akhir. Sehingga dihasilkan suatu file yang sama dengan media gambar sebelum disisipi dan sesudah disisipi suatu pesan yang disembunyikan.

**4. Kesimpulan**

Adapun Kesimpulan dari penelitian ini adalah sebagai berikut :

1. Perancangan aplikasi dengan Teknik *Anti-forensic* untuk penyembunyian pesan didalam media digital.
2. Penggunaan Kriptografi Triple DES dan Steganografi dengan metode *Least Significant Bit* untuk melakukan enkripsi pesan dan penyembunyian pesan. Dimana pesan akan disisipkan kedalam sebuah gambar dengan format gambar .bmp.
3. Dihasilkannya rancangan dan desain untuk aplikasi anti-*forensic* dengan menggunakan *visual C#*.

**Daftar Pustaka**


[1] Raharjo, Budi. (1998-1999). *Keamanan Sistem Informasi Berbasis Internet.* PT. Insan Komunikasi/Indonesia-Bandung.

[2] Mahardika, Fathoni., Sani, Yuliani. *Anti Forensic Tool dalam Meningkatkan Keamanan Data*. STMIK Sumedang, Magister Teknik Informatika Universitas Langlangbuana.

[3] Br. Bangun, Apulina Emmy., Setiawan, Natawijaya Gamalie. *Perbandingan Metode Modifikasi 3DES Dengan Metode 3DES.* Fakultas Teknik, Institut Teknologi Harapan Bangsa.

[4] Sitorus, Michael. (2015). *Teknik Steganography Dengan Metode Least Significan Bit (LSB)*. Faklutas Teknik. Universitas Satya Negara Indonesia.

[5] Nani, A. Paskalis. *Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode EOF*. Teknik Informatika. Universitas Katolik Widya Mandira.

[6] Gusmayuda, Ayus Rizky. Steganografi Pada Media Video Digital Dengan Metode FFT (Fast Fourier Transform) dan LSB (Least Signifikan Bit). Fakultas Teknik dan Ilmu Komputer. Teknik informatika. Universitas Komputer Indonesia.

[7] Hidayat, Akik. (2016) *Enkripsi Dan Dekripsi Data Dengan Algoritma 3 Des (Triple Data Encryption Standard)*. Jurusan Matematika FMIPA Universitas Padjadjaran.

[8] Utomo, Tri Prasetyo. (2012). *Steganografi Gambar dengan Metode Least Significant Bit untuk Proteksi Komunikasi pada Media Online*. Universitas Islam Negeri Sunan Gunung Djati. Bandung.