Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018
SENSITEK 2018
STMIK Pontianak, 12 Juli 2018

Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada 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

Teknik data hiding merupakan proses pengamanan suatu data dengan menyembunyikan data didalam sebuah media digitali. Teknik data hiding merupakan teknik didalam anti-forensic yang bertujuan untuk menyulitkan ahli forensic didalam investigasi. Meningkatnya perkembangan teknologi menimbulkan paradigma pada keamanan informasi, dikarenakan mudahnya suatu informasi mengalami kebocoran. Atas dasar masalah tersebut, pengamanan pesan dengan teknik data hidding digunakan didalam mengamankan pesan rahasia dengan mengkombinasikan kriptografi dan Stegaganogaphy. Algoritma TripleDES digunakan untuk mengenkripsi pesan rahasia sedangkan Least Significant Bit (LSB) untuk metode menyembunyikan pesan rahasia kedalam sebuah gambar sehingga dihasilkan file stego dengan sebuah gambar yang didalamnya terdapat suatu pesan rahasia. Dihasilkannya aplikasi menggunakan teknik hidding dengan tripleDES dan steganography metode LSB dengan menggunakan Visual Studio C# ini mampu menghasilkan file stego dengan dilakukannya enkripsi pesan plaintext dan di lakukan embed ciphertext kedalam media gambar. Dari hasil pengujian dengan metode blackbox menunjukan, aplikasi ini berjalan dengan baik dan pengujian juga dilakukan menggunakan software HxD untuk melihat patern pada file gambar asli dengan file stego yang menunjukan hasil file stego terdapat perubahan data patern gambar yang sudah disisipkan pesan ciphertext.

***Kata kunci**: Teknik data hiding, Kriptografi, steganography, TripleDES, Least Significant Bit*

1. Pendahuluan

Seiring dengan perkembangan teknologi yang semakin pesat, informasi menjadi suatu peran yang penting ditengah-tengah masyarakat. Dengan teknologi, informasi lebih mudah didalam akses tanpa dibatasi dengan ruang dan waktu. Selain kemudahan akses, hal yang tidak kalah pentingnya adalah keamanan informasi. Keamanan informasi merupakan suatu privasi sebagai hak yang paling mendasar bagi setiap pengguna teknologi dalam melakukan akses suatu informasi serta mengirimkan suatu informasi didalam media jaringan internet agar tidak dengan mudah diketahui oleh pihak yang tidak bertanggung jawab. Semakin berkembangnya teknologi internet, semakin meningkat penggunanyaakan tetapi kurangnya kesadaran didalam mengamankan informasi yang dimilikinya. Hal ini ditunjukan dengan perilaku pengguna yang tidak aware terhadap informasi yang dimilikinya sehingga menjadi sebuah ancaman akan kebocoran suatu informasi. Informasi yang diterima maupun dikirim rawan terhadap serangan *intercept* yang memungkinkan informasi tersebut dimodifikasi sehingga informasi tersebut tidak memiliki integritas dan tidak privasi lagi.

Dari latar belakang diatas, didapatkan permasasalahnnya yakni bagaimana mengamankan suatu informasi agar tidak mudah diketahui oleh pihak yang tidak bertanggung jawab, sehingga informasi menjadi aman dalam hal ini adalah berupa pesan rahasia. Dalam hal ini, di implementasikan aplikasi dengan teknik data hiding menggunakan kriptografi dengan algoritma TripleDES dan *steganography* dengan metode *Least Significant Bit* untuk menyisipkan pesan yang sudah dienkripsi kedalam media gambar digital.

Kriptografi

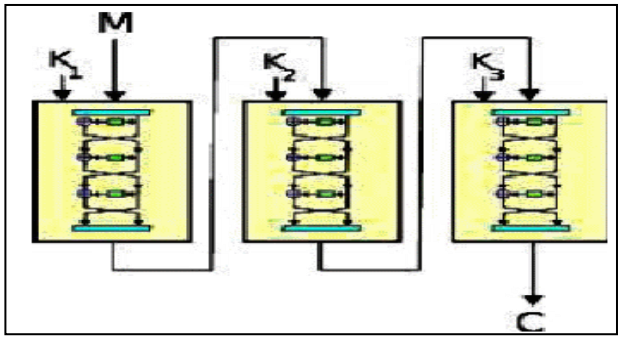
Kriptografi adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *Cryptographer*. Sedangkan *Cryptoanalysis* adalah suatu ilmu dan seni membuka (breaking) chipertext dan orang yang melakukannya disebut *Cryptoanalyst*. *Cryptographic System* atau *Cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke chipertext dan sebaliknya. Dalam sistem ini, seperangkat parameter menentukan transformasi penchiperan tertentu yang disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci Kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengekripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan perlu identik, tergantung pada sistem yang digunakan[14]. Algoritma terdiri dari tiga fungsi dasar yaitu :

1. Enkripsi adalah Proses merubah pesan asli (*plaintext*) menjadi pesan yang sulit dimengerti (*ciphertext*).
2. Dekripsi adalah kebalikan dari enkripsi. Dimana *ciphertext* dikembalikan lagi menjadi *plaintext*.
3. *Key* adalah Kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. *Key* atau kunci dibagi dua yaitu *private* dan *public*

Triple DES

3DES (*Triple Data Encryption Standard*) merupakan suatu algoritma pengembangan dari algoritma DES

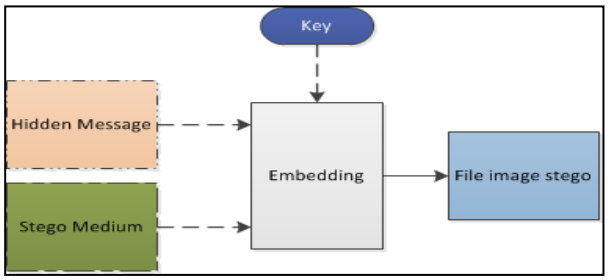
(*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES). Pada algoritma 3DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. 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).



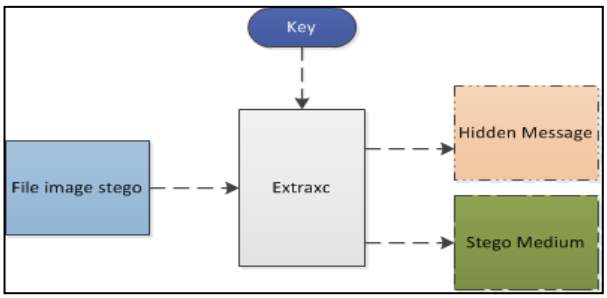
Gambar 1. Algoritma *Triple* DES [15]

Steganografi

Steganografi (*Steganography*) berasal dari bahasa Yunani *steganos* (*hidden*) dan *gráphein* (*writing*). Jadi, steganografi berarti *hidden writing* (tulisan tersembunyi). *Steganography* 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 *steganography* modern, arti steganografi berkembang menjadi penyembunyian informasi pada sebuah media file digital, bisa berupa media gambar, suara ataupun video[4]. Didalam teknik *Steganography* memiliki dua proses yaitu proses *Embedding* atau *Encoding* (menyembunyikan pesan rahasia) dan *Extraction* atau *Decoding* (mengekstrasi pesan yang disembunyikan)[10].

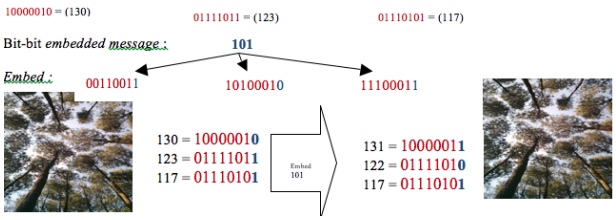


Gambar 2. Proses Embedding Pesan



Gambar 3. Proses Ekstraksi

Least Significant Bit (LSB) adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu mengubah bit redundan *cover image* yang tidak berpengaruh signifikan dengan bit dari pesan rahasia[11]. LSB Merupakan metode *steganography* yang paling populer. Memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar Caranya: Mengganti bit LSB dari *pixel* dengan bit pesan. Mengubah bit LSB hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual atau auditori[12]. Metode yang digunakan untuk penyembunyian pesan rahasia pada metode ini adalah dengan cara menyisipkan pesan ke dalam bit rendah (*Least Significant Bit*) pada data *pixel* yang menyusun file gambar (*image*) yang digunakan sebagai media penampung.
Misal diberikan 1 buah *pixel* dari citra 24-bit (3 x 8 bit) :



Gambar Asli Hasil Stego

Ukuran pesan yang akan disembunyikan bergantung pada ukuran *cover-object*.
Misalkan pada citra *grayscale* (1 byte/pixel) 256 x 256 *pixel* :
-Jumlah pixel = jumlah byte = 256 x 256 = 65536

-Setiap byte dapat menyembunyikan 1 bit pesan di LSB-nya
-Jadi ukuran maksimal pesan = 65536 bit = 8192 byte = 8 KB

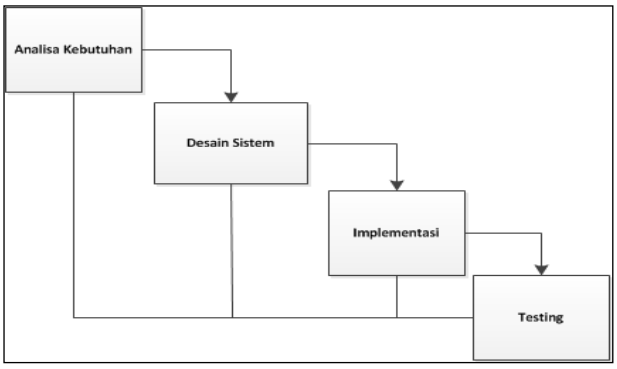
Pada citra berwarna 24-bit berukuran 256 × 256 *pixel*:
-Jumlah *pixel* 256 x 256 = 65536
-Setiap *pixel* = 3 byte, berarti ada 65536 × 3 = 196608 *byte*.
-Setiap *byte* dapat menyembunyikan 1 bit pesan
-Jadi ukuran maksimal pesan = 196608 bit = 24576 *byte* = 24KB

2. Pembahasan

Metode Penelitian

Adapun metode penelitian yang digunakan adalah sebagai berikut :

Gambar 4. Metode Penelitian



Adapun penjelasan dari Gambar 4 diatas adalah sebagai berikut :

a. Analisa Kebutuhan

Pada tahap analisa kebutuhan dimana dilakukan pengumpulan data serta kebutuhan didalam penelitian guna untuk menunjang penelitian ditahap awal.

b. Desain Sistem

Pada tahap desain sistem dilakukan perancangan sistem. Mulai dari perancangan sistem dengan *flowchart*, Use case dan Desain antarmuka sistem.

c. Implementasi

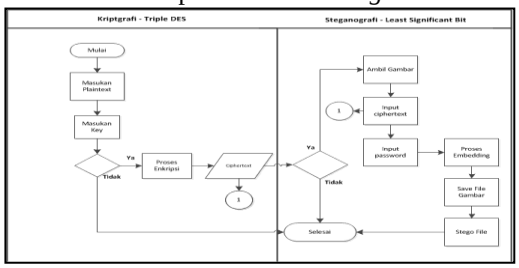
Pada tahap implementasi, dilakukannya tahap desain aplikasi yang selanjutnya diterjemahkan kedalam bahasa pemrograman yang sudah ditentukan atau *coding*.

d. *Testing*

Pada tahap *testing* adalah tahap dimana aplikasi yang sudah selesai dibangun akan diuji secara keseluruhan dengan menggunakan metode *blackbox testing*.

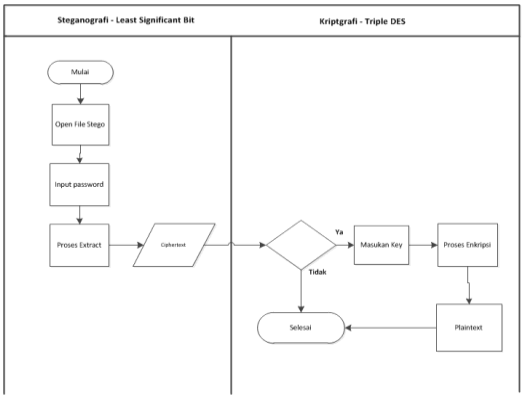
Rancangan Sistem

Flowchart Enkripsi dan *Embedding*



Gambar 5. *Flowchart* Enkripsi dan *Embedding*
Flowchart Dekripsi dan *Ekstraksi* File *Stego*

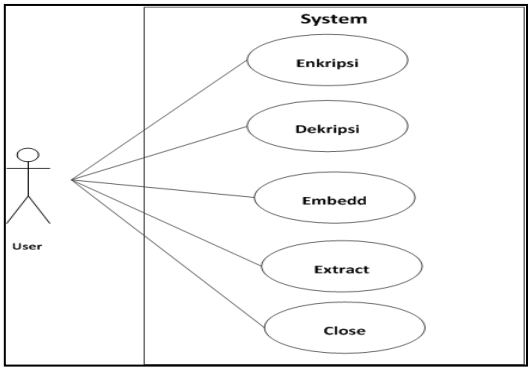
Berikut ini adalah flowchart dekripsi dan ekstraksi file stego adalah :



Gambar 6. *Flowchart* Dekripsi dan Ekstraksi File *Stego*

Use case Diagram

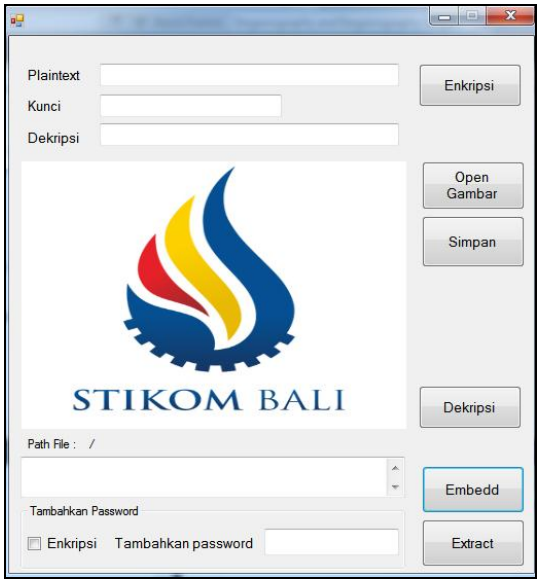
Berikut ini adalah usecase diagram aplikasi sebagai berikut :



Gambar 7. *Use case Diagram* Aplikasi

Implementasi Sistem

Pada tahap ini merupakan tahap implementasi. Pada aplikasi terdapat 6 *button*. Untuk melakukan enkripsi user harus menginputkan pesan *plaintext* dan kunci maka akan dihasilkan *ciphertext*. Untuk melakukan *stego*, pilih *button open* gambar, dan lakukan *embed* dengan menambhkan *password* setelah itu klik *button embed*. Untuk melakukan ekstrak, klik open gambar *stego file*, tambahkan password untuk membuka file tesebut dan klik button ekstrak didapatkan pesan *ciphertext*, dari *ciphertext* tersebut lakukan dekripsi dengan menginputkan kunci dan klik *button* dekripsi.



Gambar 8. User interface Aplikasi

Pada tabel 1 adalah proses dari *steganography*. Gambar_1.jpg merupakan gambar yang akan di *stego* atau gambar awal sedangkan file hasil_stego.bmp merupakan hasil dari *stego* sebagai berikut :

Tabel 1. Hasil Steganografi

No	File	Nama File	Keterangan
1.		Nama File : **Gambar_1.jpg** Size awal : **46.9 KB (48,051 bytes)**	Pada file Gambar_1.jpg merupakan gambar yang belum diproses dengan teknik *stego*.
2.		Nama File : **hasil_stego.bmp** Size Stego : **826 KB (846,578 bytes)**	Pada hasil_stego.bmp merupakan gambar yang sudah melewati proses *stego*, dengan hasil file adalah .bmp.

Dari hasil proses pada tabel 1, didapatkan hasil bahwa ukuran file awal dengan file setelah melewati proses *stego* menjadi lebih besar. Dikarenakan adanya pesan yang diinputkan kedalam file gambar.

Testing Blackbox

Pada tabel 2, merupakan proses *testing* aplikasi menggunakan metode *blackbox testing*. Dimana melakukan serangkaian uji coba inputan terhadap aplikasi tersebut. Sebagai berikut :

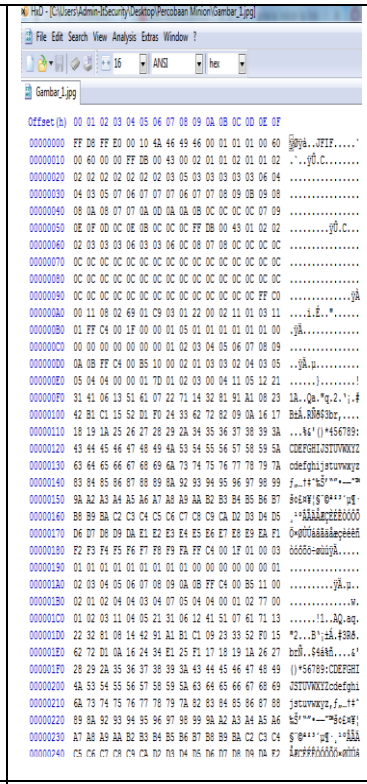
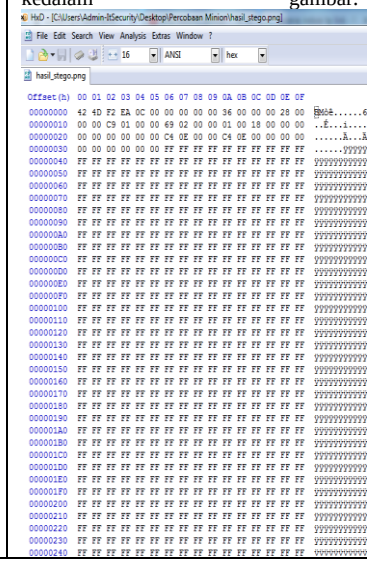
Tabel 2. Hasil *Testing* dengan *blackbox testing*

No	Proses	Keterangan	Hasil
1	Pada Button Enkripsi	Melakukan proses enkripsi dengan cara menginputkan pesan *plaintext*	Proses sesuai
2	Pada Button Deskripsi	Melakukan Proses Dekripsi dengan cara mengambil pesan *ciphertext* dari hasil ekstrak gambar	Proses sesuai
3	Pada Open File Image	Melakukan proses akses file gambar, format yang digunakan adalah .jpg, .bmp	Proses sesuai
4	Pada Save File Image	Melakukan Simpan File, pada proses ini file gambar akan disimpan kedalam format .bmp.	Proses sesuai
5	Pada Embedd Pesan	Melakukan Proses Hiden Pesan, pada proses ini pesan *ciphertext* akan diembedd kedalam sebuah gambar	Proses sesuai
6	Pada Extract Pesan	Melakukan Extraksi pesan didalam gambar, pada proses ini merupakan proses yang digunakan untuk mengambil pesan yang sudah disisipkan kedalam file gambar tersebut.	Proses sesuai

Dari hasil pengujian dengan *blackbox testing* didapatkan hasil semua proses berjalan dengan baik dan sesuai. Pada tabel 3 merupakan pengujian dengan menggunakan HxD tool untuk memeriksa *patern* bit pada suatu file.

Tabel 3. Hasil pengujian dengan HxD Tool

No	Nama Kegiatan	Hasil
1.	Proses analisis terhadap gambar_1.jpg, merupakan gambar asli	Dari hasil analisis dengan menggunakan HxD Tool didapatkan bahwa file **Gambar_1.jpg** yang belum dilakukan proses stego atau file aslinya.

		
2.	Proses analisis terhadap hasil_stego.bmp, merupakan file gambar yang sudah di embed pesan kedalam gambar. 	Sedangkan pada file **hasil_stego.bmp** merupakan file gambar yang sudah dilakukan proses *stego*. Dari hasil analisis dengan menggunakan HxD Tool didapatkan bahwa gambar yang sudah dilakukan proses stego dan sudah diembed suatu pesan menghasilkan file dengan size lebih besar dan pada *patern bit-bit* nya mengalami perubahan dengan berhasilnya pesan diembed kedalam file gambar.

Dari hasil pengujian menggunakan HxD tools didapatkan hasil bahwa, file Gambar_1.jpg merupakan file asli, file tersebut jika di buka dengan HxD didapatkan hasil patern bit tidak mengalami perubahan. Sedangkan untuk file Hasil_stego.bmp merupakan file gambar yang sudah diproses dengan teknik stego dimana hasil dari file tersebut, terlihat bahwa patern bit dari filenya 4berubah dengan bertambahnya patern bit dikarenakan adanya pesan kedalam file gambar.

3. Kesimpulan

Adapun Kesimpulan dari penelitian ini adalah sebagai berikut :

Telah dihasilkan aplikasi teknik data hiding untuk membantu pengamanan pesan rahasia dengan menggunakan kriptografi *Triple Des* dan steganography LSB (*Least significant Bit)* menggunakan menggunakan visual studio C#. Dari hasil pengujian dengan metode Blackbox testing proses enkripsi dan stego file serta dekripsi ciphertext berjalan sesuai dengan yang diharapkan. setelah melakukan uji file dengan menggunakan HxD didapatkan patern pada file berubah serta size file bertambah besar.

Daftar Pustaka

[1]. B. Raharjo. Keamanan Sistem Informasi Berbasis Internet. PT. Insan Komunikasi Indonesia-Bandung., 1998-1999.

[2]. F. Mahardika, Y. Sani, "Anti Forensic Tool dalam Meningkatkan Keamanan Data", STMIK Sumedang, Magister Teknik Informatika Universitas Langlangbuana.

[3]. B. Bangun, E. Apulina, Setiawan, G. Natawijaya, "Perbandingan Metode Modifikasi 3DES Dengan Metode 3DES", Fakultas Teknik, Institut Teknologi Harapan Bangsa, 2015.

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

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

[6]. A.R. Gusmayuda. "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]. A. Hidayat. "Enkripsi Dan Dekripsi Data Dengan Algoritma 3 Des (Triple Data Encryption Standard)".Jurusan Matematika FMIPA Universitas Padjadjaran,2015.

[8]. T.P. Utomo, "Steganografi Gambar dengan Metode Least Significant Bit untuk Proteksi Komunikasi pada Media Online". Universitas Islam Negeri Sunan Gunung Djati. Bandung,2012.

[9]. R. Munir,. *Steganografi dan Watermarking*. ITB, 2004.

[10]. E. Haryanto, "Implementasi Teknik Steganografi Sebagai Anti Forensik Penyisipan Teks Pada Citra". Yogyakarta: Jurnal Informasi Interkatif Vol 1 Nomor 2, 2016.

[11]. https://mti.binus.ac.id/2017/06/08/steganografi-dengan-least-significant-bit-lsb/ diakses pada tanggal 9 Pebruari 2019, Jam 09.15 menit

[12]. R. Munir. 2015. Bahan Kuliah Steganografi. Program Studi Informatika. STEI-ITB. Diambil dari : http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Steganografi%20dan%20Watermarking.pdf

[13]. Andi. *Memahami Model Enkripsi dan Security Data*,Yogyakarta, Andi Offset,2003.

[14]. D. Ariyus. *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi Offset. Yogyakarta. 2016.

[15]. http://3.bp.blogspot.com/-BbPPuMRqcw0/T-bu1K9lNwI/AAAAAAAAAGU/j7qmHMEQNIs/s1600/3.gif diakses tanggal 9 Pebruari 2018 jam 13.00 wita

[16]. http://scdc.binus.ac.id/himsisfo/2016/10/perbedaan-white-box-testing-dan-black-box-testing/ diakses tanggal 9 Pebruari 2018 pukul 20.15 wita