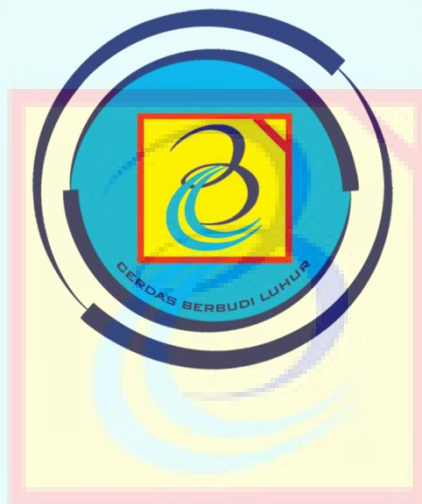


**PENGAMANAN DATA WELL LOG IMAGE MENGGUNAKAN
METODE *LSB* DAN ALGORITMA *TRIPLE DATA ENCRYPTION
STANDARD (3DES)* DENGAN *SHA-1 HASH FUNCTION* PADA MEDIA
IMAGE : STUDI KASUS PT PERTAMINA EP ASSET 2 PRABUMULIH**

TESIS



Oleh:

**Pradhipta Ramadhinara Haryanto
1411602186**

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017**

**PENGAMANAN DATA *WELL LOG IMAGE* MENGGUNAKAN
METODE *LSB* DAN ALGORITMA *TRIPLE DATA ENCRYPTION
STANDARD (3DES)* DENGAN *SHA-1 HASH FUNCTION* PADA MEDIA
IMAGE : STUDI KASUS PT PERTAMINA EP ASSET 2 PRABUMULIH**

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



Oleh:

Pradhipta Ramadhinara Haryanto
1411602186

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017**



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama Mahasiswa : Pradipta Ramadhinara Haryanto
Nomor Induk Mahasiswa : 1411602186
Konsentrasi : Rekayasa Komputasi Terapan
Program Studi : Magister Ilmu Komputer
Fakultas/Program : Pascasarjana / Strata 2

Menyatakan bahwa Tesis yang berjudul :

Pengamanan Data Well Log Image Menggunakan Metode LSB
dan Algoritma Triple Data Encryption Standard (3DES) Dengan
Menggunakan SHA-1 Hash Function Pada Media Image: Studi
Kasus PT Pertamina Asset 2 Probolinggo

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, 1 Agustus 2017

METERAI
TEMPEL
28660AEF146779809
6000
ENAM RIBU RUPIAH
Pradipta Ramadhinara H.



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Pradhipta Ramadhinara Haryanto
Nomor Induk Mahasiswa : 1411602186
Konsentrasi : Rekayasa Komputasi Terapan
Program Studi : Magister Ilmu Komputer
Judul Tesis : Pengamanan Data *Well Log Image* Menggunakan Metode *LSB* dan Algoritma *Triple Data Encryption Standard (3DES)* Dengan Menggunakan *SHA-1 Hash Function* Pada Media *Image* : Studi Kasus PT Pertamina EP Asset 2 Prabumulih

Jakarta, 01 Agustus 2017
Tim Penguji

Tanda Tangan

Ketua,
(Dr. M. Syafrullah, M.Kom, M.Sc)

Anggota,
(Ir. Wendi Usino, MM., M.Sc., Ph.D)

Pembimbing Utama,
(Dr. Ir. Nazori AZ, M.T.)

Ketua Program Studi
Magister Ilmu Komputer

(Dr. M. Syafrullah, M.Kom, M.Sc)

ABSTRAK

Pesatnya perkembangan teknologi informasi telah mendorong penggunaan internet sebagai media pertukaran informasi menjadi sangat signifikan. Dengan karakteristiknya yang memiliki jangkauan luas dan waktu yang singkat ketika melakukan pertukaran data, maka sudah pasti internet menjadi bagian penting dalam kehidupan manusia di era modern ini. Karena karakteristik tersebut, maka privasi di dalam komunikasi digital menjadi sangat penting ketika seseorang atau suatu organisasi ingin melakukan pertukaran informasi yang bersifat rahasia. Namun dibalik semua kemudahan itu terdapat kelemahan yang cukup bahaya apabila tidak hati – hati dalam menggunakannya. Seperti pencurian data, pengubahan data oleh orang yang tidak bertanggung jawab, serta kesalahan pengiriman data kepada orang yang tidak dituju. Maka dari itu untuk melindungi data seseorang ataupun organisasi dari hal tersebut perlu diterapkan metode *Least Significant Bit (LSB)* dan algoritma *Triple Data Encryption Standard (3DES)* dengan penambahan *Secure Hash Algorithm 1 (SHA-1) hash function* sebagai suatu solusi yang penulis usulkan sebagai suatu sistem pengamanan data di dalam tesis ini. Dengan penggabungan beberapa teknik tersebut, data rahasia dienkripsi dengan algoritma *3DES* dan *SHA-1 hash function*, kemudian disisipkan ke bit yang tidak signifikan dalam sebuah *cover image* sebagai media pembawa yang akan dikirimkan sebagai suatu *stego image*. *Stego image* inilah yang nantinya dijadikan sebagai suatu media pengiriman. Dari hasil pengujian yang telah dilakukan pada kedua *cover image* sebagai media penampung, yaitu *cover_file_1.jpg* dan *cover_file_2.png* dengan ke-20 data sampel sebagai *message file*, algoritma *3DES SHA-1* lebih unggul saat dibandingkan dengan *3DES MD5* diukur dari aspek ukuran file yang dihasilkan sebesar 0,0021%, waktu proses *hide data* sebesar 2,41% dan waktu proses *extract data* sebesar 21,22%. Lalu dari aspek keamanan algoritma tersebut juga terbukti aman. Hal ini terlihat dari pengukuran kualitas gambar *stego image* yang dihasilkan berdasarkan nilai *MSE* yang kecil dan nilai *PNSR* yang besar.

Kata kunci: Pengamanan Data, *Least Significant Bit (LSB)*, *Triple Data Encryption Standard (3DES)*, *Secure Hash Algorithm 1(SHA-1)*, Steganografi, Kriptografi.

KATA PENGANTAR

Puji dan Syukur yang sedalam-dalamnya kepada Allah SWT, karena hanya dengan rahmat dan karunia-Nya-lah naskah tesis yang berjudul “Pengamanan Data *Well Log Image* Menggunakan Metode LSB dan Algoritma *Triple Data Encryption Standard (3DES)* dengan *SHA-1 Hash Function* Pada Media Image : Studi Kasus PT Pertamina EP Asset 2 Prabumulih” dapat diselesaikan.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang tulus kepada:

1. Bapak dan Ibu yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
2. Bapak Prof. Dr. Sc. Agr. Ir. Didik Sulistyanto selaku Rektor Universitas Budi Luhur.
3. Bapak Dr. Suhartono, M.A, MBA selaku Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak Dr. M. Syafrullah, M.Kom., M.Sc selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan pembimbing tesis yang banyak memberikan bimbingan dan arahan.
5. Seluruh Dosen Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
6. Serta semua pihak yang tidak dapat dituliskan.

Penulis menyadari bahwa penulisan tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, 15 April 2017

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PERNYATAAN	Error! Bookmark not defined.
LEMBAR PENGESAHAN	Error! Bookmark not defined.
ABSTRAK	iv
KATA PENGANTAR.....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
BAB I : PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	3
1.2.1 Identifikasi Masalah	3
1.2.2 Batasan Masalah.....	3
1.2.3 Rumusan Masalah	4
1.3 Tujuan Penelitian dan Manfaat Penelitian.....	4
1.4 Tata Urut Penulisan	5
1.5 Daftar Pengertian.....	6
BAB II : LANDASAN TEORI	7
2.1 Tinjauan Pustaka	7
2.1.1 Teori Citra Digital	7
2.1.2 Steganografi	9
2.1.3 Metode <i>Least Significant Bit (LSB)</i>	14
2.1.4 Kriptografi	17
2.1.5 Algoritma <i>Data Encryption Standard (DES)</i>	18
2.1.6 Algoritma <i>Triple Data Encryption Standard (3DES)</i>	20
2.1.8 <i>Well Logging</i>	24
2.2 Tinjauan Studi	25
2.3 Tinjauan Objek Penelitian	29
2.3.1 Perangkat Keras	29
2.3.2 Perangkat Lunak	29
2.3.3 Pola Pikir	30
2.4 Hipotesis	31
BAB III : METODELOGI DAN RANCANGAN PENELITIAN	32
3.1 Metode Penelitian.....	32
3.2 Metode Pengumpulan Data	32
3.3 Instrumentasi	33
4.1.1 Instrumen studi dokumentasi yang berhubungan dengan penelitian ini.....	33
4.1.2 Instrumen uji coba penelitian	33
3.4 Langkah – Langkah Penelitian.....	33
3.4.1 Perumusan Masalah.....	34

3.4.2	Studi Pustaka	34
3.4.3	Formulasi Hipotesis.....	34
3.4.4	Perancangan dan Pengembangan Sistem	34
3.4.5	Pengujian dan Analisis	42
3.4.6	Penarikan Kesimpulan.....	42
3.5	Jadwal Penelitian	43
BAB IV : PEMBAHASAN HASIL PENELITIAN		44
4.1	Implementasi Sistem	44
4.2.1	Spesifikasi Perangkat Keras	44
4.2.2	Spesifikasi Perangkat Lunak	45
4.2.3	Implementasi Program	45
4.2	Pengujian Sistem	53
4.2.1	<i>Cover File</i> yang digunakan	53
4.2.2	<i>Message File</i> yang digunakan.....	54
4.2.3	Hasil Pengujian Uji Kualitatif	55
BAB V : PENUTUP		66
5.1	Kesimpulan.....	66
5.2	Saran	66
DAFTAR PUSTAKA		67
RIWAYAT HIDUP SINGKAT		69

DAFTAR GAMBAR

Gambar II-1	: Citra Biner.....	7
Gambar II-2	: Array Citra Biner.....	8
Gambar II-3	: Ruang Warna RGB.....	9
Gambar II-4	: Proses Steganografi.....	12
Gambar II-5	: MSB dan LSB.....	14
Gambar II-6	: Proses Enkripsi <i>Data Encryption Standard (DES)</i>	19
Gambar II-7	: Proses Setiap Putaran Enkripsi <i>Data Encryption Standard (DES)</i>	20
Gambar II-8	: Proses Enkripsi <i>Triple Data Encryption Standard (3DES)</i> Mode EDE.....	21
Gambar II-9	: Proses Dekripsi <i>Triple Data Encryption Standard (3DES)</i> Mode EDE.....	22
Gambar II-10	: Proses Enkripsi <i>Triple Data Encryption Standard (3DES)</i> Mode EEE.....	23
Gambar II-11	: Proses Dekripsi <i>Triple Data Encryption Standard (3DES)</i> Mode EEE.....	23
Gambar II-12	: Pola Pikir Teknik Steganografi dan Kriptografi.....	30
Gambar III-1	: Langkah – langkah Penelitian.....	33
Gambar III-2	: Alur Proses <i>Hide Data</i>	35
Gambar III-3	: Alur proses Extract Data.....	36
Gambar III-4	: <i>Use Case Diagram</i>	36
Gambar III-5	: <i>Activity Diagram</i> Aplikasi Steganografi dan Kriptografi.....	38
Gambar III-6	: <i>Sequence Diagram</i> <i>Hide Data</i> Aplikasi Steganografi dan Kriptografi.....	39
Gambar III-7	: <i>Sequence Diagram</i> <i>Extract Data</i> Aplikasi Steganografi dan Kriptografi.....	39
Gambar III-8	: Rancangan Layar <i>Hide Data</i> Aplikasi Steganografi dan Kriptografi.....	40
Gambar III-9	: Rancangan Layar <i>Extract Data</i> Aplikasi Steganografi dan Kriptografi.....	41
Gambar IV-1	: Tampilan <i>Tab Hide Data</i>	46
Gambar IV-2	: Tampilan <i>Browse Message File</i>	47
Gambar IV-3	: Tampilan <i>Browse Cover File</i>	48
Gambar IV-4	: Tampilan <i>Browse Output Stego File</i>	49
Gambar IV-5	: Tampilan <i>Loading Process</i>	50

Gambar IV-6	: Tampilan <i>Windows Success Hide Data</i>	50
Gambar IV-7	: Tampilan <i>Tab Extract Data</i>	51
Gambar IV-8	: Tampilan <i>Browse Input Stego File</i>	52
Gambar IV-9	: Tampilan <i>Windows Success Extract Data</i>	53
Gambar IV-10	: Tampilan <i>Invalid Password</i>	53
Gambar IV-11	: Diagram Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Ukuran <i>Stego File</i>	62
Gambar IV-12	: Diagram Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Waktu <i>Hide Data</i>	62
Gambar IV-13	: Diagram Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Waktu <i>Extract Data</i>	63



DAFTAR TABEL

Tabel I-1	: Daftar Pengertian Istilah.....	6
Tabel II-1	: Ringkasan Penelitian Terkait.....	27
Tabel III-1	: <i>Use Case Description Hide Data</i>	37
Tabel III-2	: <i>Use Case Description Extract Data</i>	37
Tabel III-3	: Jadwal Penelitian.....	43
Tabel IV-1	: Spesifikasi Perangkat Keras.....	44
Tabel IV-2	: Spesifikasi Perangkat Lunak.....	45
Tabel IV-3	: Informasi Data <i>Cover File</i>	54
Tabel IV-4	: Informasi Data <i>Message File</i>	55
Tabel IV-5	: Hasil Pengujian Algoritma <i>3DES MD5 hash function</i> Pada File <i>cover_file_1.jpg</i>	55
Tabel IV-6	: Hasil Pengujian Algoritma <i>3DES MD5 hash function</i> Pada File <i>cover_file_2.png</i>	56
Tabel IV-7	: Hasil Pengujian Algoritma <i>3DES SHA-1 hash function</i> Pada File <i>cover_file_1.jpg</i>	57
Tabel IV-8	: Hasil Pengujian Algoritma <i>3DES SHA-1 hash function</i> Pada File <i>cover_file_2.png</i>	58
Tabel IV-9	: Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Ukuran dan Waktu Pada File <i>cover_file_1.jpg</i>	59
Tabel IV-10	: Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Ukuran dan Waktu Pada File <i>cover_file_2.png</i>	60
Tabel IV-11	: Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Nilai <i>MSE</i> dan <i>PNSR</i> Pada File <i>cover_file_1.jpg</i>	63
Tabel IV-12	: Hasil Perbandingan Algoritma <i>3DES MD5</i> dan <i>3DES SHA-1</i> Berdasarkan Nilai <i>MSE</i> dan <i>PNSR</i> Pada File <i>cover_file_2.png</i>	64

DAFTAR PUSTAKA

Agani, N., Farisi, A. dan Aryasanti, A. 2013, Implementation and Analysis Steganography Technique of Least Significant Bit (LSB) on Image and Audio File, *ICIBA2013, the Second International Conference on Information Technology and Business Application Palembang*, Indonesia.

Assare, M. T. dan Missah, Y. M., 2016, An Enhanced Triple Data Encryption Standard (TDES) Algorithm to Secure Health Level Seven (HL7) Data Transfer, *International Research Journal of Engineering and Technology (IRJET)*, Vol. 3 Issue 10, PP 16-27.

Dony, A. 2009, *Pengantar Ilmu Kriptografi, Algoritma Kriptografi Modern*, Andi Publisher, Jakarta.

Ellis, D. V., dan Singe, M. J., 2008, *Well Logging for Earth Scientists* 2nd Edition, Springer, Netherlands.

Hariato, A. 2013, *Studi Perbandingan Eknripsi Steganografi LSB dengan EOF* Program Studi Teknik Informatika, Universitas Tanjungpura, Pontianak.

Karthik, S., dan Muruganandam, A., 2014, *International Journal of Scientific Engineering and Research (IJSER)*, Vol. 2 Issue 11.

Marques, Oge. 2011, *Practical Image and Video Processing Using Matlab*, John Wiley & Sons, Inc, New Jersey.

Pebrianti, W., 2012, *Pemanfaatan Steganografi Untuk Keamanan Pada Pengiriman Email*.