

**PENERAPAN STEGANOGRAFI, KRIPTOGRAFI DAN
KOMPRESI DATA SEBAGAI UPAYA PENINGKATAN
KEAMANAN LAPORAN KEUANGANKOPERASI :
STUDI KASUS KJKS BMT**

TESIS



**Oleh :
DediDarwis
1311600819**

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

**JAKARTA
2015**

**PENERAPAN STEGANOGRAFI, KRIPTOGRAFI DAN
KOMPRESI DATA SEBAGAI UPAYA PENINGKATAN
KEAMANAN LAPORAN KEUANGAN KOPERASI :
STUDI KASUS KJKS BMT**

TESIS

Diajukan untuk memenuhi Persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



**Oleh :
DediDarwis
1311600819**

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

**JAKARTA
2015**



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

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama Mahasiswa : Dedi Darwis
Nomor Induk Mahasiswa : 13.11.600.819
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputer Terapan
Fakultas/Program : Pascasarjana

Menyatakan bahwa Tesis yang berjudul :

Penerapan Steganografi, Kriptografi dan Kompresi Data Sebagai
Upaya Peningkatan Keamanan Laporan Keuangan Koperasi :
Studi Kasus KKS BMT.

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, 11 Agustus 2015



[Signature]
Dedi Darwis



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

LEMBAR PENGESAHAN

Nama Mahasiswa : Dedi Darwis
Nomor Pokok Mahasiswa : 1311600819
Konsentrasi : Rekayasa Komputasi Terapan
Judul Proposal Tesis : Penerapan Steganografi, Kriptografi dan Kompresi
Data Sebagai Upaya Peningkatan Keamanan
Laporan Keuangan Koperasi : Studi Kasus KJKS
BMT

Jakarta, 11 Agustus 2015

Tim Penguji :

Tanda Tangan

Ketua,
Prof. Dr. Moedjiono, M.Sc.

Anggota,
Dr. Ir. Nazori Az, M.T.

Pembimbing,
Ir. Yan Everhard, M.T.

Ketua Program Studi

Dr. Ir. Nazori Az, M.T.

ABSTRAK

Koperasi Jasa Keuangan Syariah (KJKS) BMT Bandarlampung merupakan koperasi yang kegiatan usahanya bergerak di bidang pembiayaan, investasi, dan simpanan sesuai pola bagi hasil (syariah). Pembuatan laporan keuangan koperasi serta memberikan keamanan merupakan hal penting bagi koperasi karena laporan keuangan yang banyak diminati oleh pihak-pihak yang tidak berkompeten untuk mengetahui laporan keuangan tersebut. Laporan keuangan seharusnya hanya dapat dilihat oleh orang-orang yang berwenang dan berkompeten yaitu manajer dan pimpinan. Salah satu cara untuk menangani keamanan laporan keuangan koperasi ini yaitu menggunakan teknik steganografi, kriptografi dan kompresi data. Penelitian ini membahas bagaimana menerapkan teknik steganografi menggunakan algoritma *GifShuffle*, teknik kriptografi menggunakan algoritma *Data Encryption Standard (DES)*, teknik kompresi data menggunakan algoritma kompresi *Huffman* yang akan dikombinasikan pada aplikasi sebagai upaya peningkatan keamanan laporan keuangan koperasi. Hasil dari penelitian ini berupa aplikasi yang dapat melakukan enkripsi laporan keuangan melalui teknik kriptografi, kompresi data dan steganografi kemudian hasil enkripsi tersebut dapat didekripsi kembali sehingga laporan keuangan dapat dibaca oleh manajer dan pimpinan KJKS BMT.

Kata Kunci : Steganografi, Kriptografi, Kompresi Data, Keamanan Laporan Keuangan, *GifShuffle*, *DES*, *Huffman*.

ABSTRACT

Cooperative Financial Services Sharia (KJKS) Bandarlampung BMT is a cooperative whose business activities engaged in financing, investment, and savings in accordance pattern of results (sharia). Making the cooperative's financial statements and provide security is important for the cooperative because of financial statements are much in demand by parties who are not competent to determine the financial statements. Financial statements should only be seen by those who are authorized and competent managers and leaders. One way to deal with the financial statements of the cooperative security that uses the technique of steganography, cryptography and data compression. This study discusses how to apply the technique of steganography using GifShuffle algorithms, cryptographic technique uses an algorithm Data Encryption Standard (DES), a data compression technique using Huffman compression algorithm that will be combined in an effort to improve application security cooperative financial statements. Results of this research is the application that encrypts financial statements through cryptographic techniques, data compression and encryption steganography then the results can be decrypted back so that the financial statements can be read by managers and leaders KJKS BMT.

Keywords: *Steganography, Cryptography, Data Compression, Security Financial Statements, GifShuffle, DES, Huffman.*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT, karena berkat rahmat, hidayah dan karunia-Nya sehingga penulis dapat menyelesaikan penelitian tesis ini yang judul **“Penerapan Steganografi, Kriptografi dan Kompresi Data Sebagai Upaya Peningkatan Keamanan Laporan Keuangan Koperasi”**

Peneliti menyadari bahwa penulisan tesis ini tidak lepas dari bimbingan serta petunjuk dari berbagai pihak, oleh karena itu pada kesempatan ini penulis menyampaikan ucapan terima kasih sebesar-besarnya kepada :

1. Bapak dan Ibu tercinta yang telah memberikan segalanya yang mereka punya untuk keberhasilan penulis.
2. Keluarga yang senantiasa memberikan doa dan dukungan kepada penulis.
3. Bapak Ir. Yan Everhard, M.T. yang telah banyak memberikan masukan dan saran dalam penyusunan proposal ini.
4. Bapak Prof. Dr. Moedjiono, M.Sc. selaku Direktur Pascasarjana Universitas Budi Luhur.
5. Bapak Dr. Ir. Nazori Az., M.T. selaku Kaprodi MKOM UBL dan para staf kesekretariatan MKOM UBL.
6. Sahabat-sahabat tim Magister dari Lampung, Ferico, Agus, Thyo, Agung, Kisworo, Endar yang selalu berbagi canda dan tawa serta semangat selama perjalanan menempuh pendidikan MKOM di Universitas Budi Luhur.
7. Teman-teman MKOM UBL angkatan 2013.
8. Semua pihak yang telah memberikan bantuan, bimbingan serta pengarahan, sehingga penulis dapat menyelesaikan tesis ini.

Akhir kata, penulis berharap semoga Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu dan semoga laporan tesis ini membawa manfaat bagi pengembangan ilmu.

Jakarta, Agustus 2015

Dedi Darwis

DAFTAR ISI

	Halaman
LEMBAR JUDUL	i
LEMBAR PERNYATAAN	ii
LEMBAR PENGESAHAN TESIS	iii
ABSTRAK	iv
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL.....	xiv
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Masalah Penelitian.....	3
1.2.1 Identifikasi Masalah.....	3
1.2.2 Batasan Masalah	4
1.2.3 Rumusan Masalah.....	4
1.3 Tujuan dan Manfaat Penelitian.....	4
1.3.1 Tujuan Penelitian.....	4
1.3.2 Manfaat Penelitian.....	5
1.4 Sistematika Penulisan.....	5
1.5 Daftar Istilah.....	6
BAB II LANDASAN TEORI	8
2.1 Konsep Steganografi	8
2.1.1 Sejarah Steganografi.....	8
2.1.2 Pengertian Steganografi.....	8
2.1.3 Tipe Media Steganografi	10
2.2 Citra Digital	12
2.2.1 Citra Berformat GIF.....	12
2.2.2 Algoritma <i>GifShuffle</i>	13

2.3	Algoritma Kompresi Data	16
2.3.1	Kompresi <i>Huffman</i>	16
2.3.2	Graf.....	17
2.3.3	Jenis-Jenis Graf	17
2.3.4	Pohon.....	17
2.3.5	Pembentukan Pohon <i>Huffman</i>	18
2.3.6	Proses <i>Encoding Huffman</i>	20
2.3.7	Proses <i>Decoding Huffman</i>	20
2.4	Kriptografi	20
2.4.1	Sejarah Kriptografi	20
2.4.2	Pengertian Kriptografi.....	21
2.4.3	Komponen Kriptografi	22
2.4.4	Standar Enkripsi Data.....	23
2.4.5	Algoritma DES	24
2.4.5.1	Standar Enkripsi Data	25
2.4.5.2	Proses Enkripsi DES	27
2.4.5.3	Proses Dekripsi DES.....	31
2.5	Steganografi dan Kriptografi.....	31
2.6	Aspek-Aspek Keamanan Data.....	32
2.7	Tinjauan Studi	33
2.8	Tinjauan Objek Penelitian.....	38
2.9	<i>Hardware</i> dan <i>Software</i> yang Digunakan	39
2.9.1	<i>Hardware</i>	39
2.9.2	<i>Software</i>	39
2.10	Kerangka Konsep.....	40
2.11	Hipotesis Penelitian	41
BAB III METODOLOGI DAN RANCANGAN PENELITIAN		42
3.1	Metode Penelitian.....	42
3.2	Jenis Data.....	43
3.3	Sumber Data	43
3.3.1	Data Primer	43

3.3.2 Data Sekunder	43
3.4 Metode Pengumpulan Data.....	44
3.5 Langkah Penelitian.....	44
3.6 Jadwal Penelitian	48
 BAB IV HASIL PEMBAHASAN	 50
4.1 Gambaran Umum	50
4.2 Analisis Kebutuhan Sistem.....	51
4.2.1 Analisis Kebutuhan Fungsional.....	51
4.2.2 Analisis Kebutuhan Non Fungsional.....	52
4.3 Analisis Proses Bisnis.....	53
4.4 Klasifikasi Data	54
4.5 Rancangan Sistem dan Algoritma	54
4.5.1 Rancangan Sistem	54
4.5.2 <i>Flowchart</i> Alur Sistem	54
4.5.3 <i>Flowchart</i> Algoritma DES	56
4.5.4 <i>Flowchart</i> Algoritma Kompresi <i>Huffman</i>	58
4.5.5 Algoritma <i>GifShuffle</i>	60
4.5.6 Rancangan Basis Data	63
4.6 <i>User Interface</i>	64
4.6.1 <i>Form</i> Login.....	64
4.6.2 <i>Form</i> Menu Utama	65
4.6.3 <i>Form</i> Anggota	67
4.6.4 <i>Form</i> Daftar Akun	69
4.6.5 <i>Form</i> Data Simpanan.....	69
4.6.6 <i>Form</i> Penarikan	71
4.6.7 <i>Form</i> Data Pinjaman.....	72
4.6.8 <i>Form</i> Angsuran Pinjaman.....	73
4.6.9 <i>Form</i> Cetak Jurnal Umum	74
4.6.10 <i>Form</i> Cetak Buku Besar	75
4.6.11 <i>Form</i> Ubah <i>Password</i>	75

4.6.12	Form Enkripsi DES	76
4.6.13	Form Kompresi <i>Huffman</i>	77
4.6.14	Form Enkripsi Steganografi	77
4.6.15	Form Dekripsi Steganografi	78
4.6.16	Form Dekompresi <i>Huffman</i>	79
4.6.17	Form Dekripsi DES	80
4.7	Simulasi dan Pengujian	81
4.7.1	Mencetak Laporan	81
4.7.2	Simulasi dan Pengujian Enkripsi Kriptografi DES	86
4.7.3	Simulasi dan Pengujian Kompresi <i>Huffman</i>	89
4.7.5	Simulasi dan Pengujian <i>Recoverable</i>	97
4.7.6	Simulasi dan Pengujian Dekompresi <i>Huffman</i>	99
4.7.7	Simulasi dan Pengujian Dekripsi DES	99
4.8	Analisis Hasil Simulasi.....	101
4.9	Implikasi Penelitian	102
4.9.1	Aspek Sistem	102
4.9.2	Aspek Penelitian Lanjut.....	102
BAB V	PENUTUP	104
5.1	Kesimpulan	104
5.1	Saran	104
	DAFTAR PUSTAKA	106
	LAMPIRAN-LAMPIRAN.....	107
	LAMPIRAN-LAMPIRAN.....	116

DAFTAR GAMBAR

Gambar	Halaman
II.1 Contoh Bentuk Pohon	17
II.2 Pembentukan Pohon <i>Huffman</i>	19
II.3 Proses Enkripsi dan Dekripsi	23
II.4 Proses Pembangkitan Kunci-Kunci Internal	27
II.5 Satu Putaran DES	28
II.6 Diagram Komputasi Fungsi F	28
II.7 Skema Perolehan R_i	30
II.8 Perbandingan Steganografi dan Kriptografi	32
II.9 Kerangka Konsep Penelitian	40
III.1 Langkah Penelitian	45
IV.1 Rancangan <i>Use Case Diagram</i>	55
IV.2 <i>Flowchart</i> Alur Sistem	56
IV.3 <i>Flowchart</i> Algoritma DES Proses Enkripsi	57
IV.4 <i>Flowchart</i> Algoritma DES Proses Dekripsi	58
IV.5 <i>Flowchart</i> Algoritma Kompresi <i>Huffman</i>	59
IV.6 <i>Flowchart</i> Algoritma Dekompresi <i>Huffman</i>	60
IV.7 <i>Flowchart</i> Algoritma <i>GifShuffle</i> Proses Enkripsi	62
IV.8 <i>Flowchart</i> Algoritma <i>GifShuffle</i> Proses Dekripsi	63
IV.9 Rancangan Basis Data	64
IV.10 <i>Form</i> Login	65
IV.11 <i>Form</i> Menu Utama	66
IV.12 <i>Form</i> Anggota	68
IV.13 <i>Form</i> Daftar Akun	69
IV.14 <i>Form</i> Simpanan Anggota	70
IV.15 <i>Form</i> Penarikan Simpanan	71
IV.16 <i>Form</i> Data Pinjaman	72
IV.17 <i>Form</i> Angsuran Pinjaman	73

IV.18	Form Cetak Jurnal	74
IV.19	Form Cetak Buku Besar	75
IV.20	Form Ubah Password	75
IV.21	Form Enkripsi DES	76
IV.22	Form Kompresi Laporan Keuangan	77
IV.23	Form Enkripsi Steganografi	78
IV.24	Form Dekripsi Steganografi	79
IV.25	Form Dekompresi Laporan	80
IV.26	Form Dekripsi DES	80
IV.27	Form Pengujian Jurnal Umum	81
IV.28	Export Laporan Format txt	82
IV.29	Proses Menyimpan Jurnal Umum	83
IV.30	Jurnal Umum Dalam Format txt	83
IV.31	Form Pengujian BukuBesar	84
IV.32	Export Laporan Format txt	85
IV.33	Buku Besar Kas dalam Format txt	85
IV.34	Pengujian Proses Enkripsi	86
IV.35	Plainteks Laporan Keuangan	87
IV.36	Chiperteks Laporan Keuangan	87
IV.37	Grafik Perbandingan File Plainteks	89
IV.38	Proses Pengujian Kompresi Huffman	90
IV.39	Proses Kompresi dan Perhitungan Ratio	90
IV.40	Grafik Pengujian Ratio Huffman Proses Kompresi	91
IV.41	Proses Pengujian Enkripsi Steganografi	92
IV.42	Ukuran File Terlalu Besar	93
IV.43	Grafik Hasil Kuisisioner Imperecibility	95
IV.44	Pengujian Recoverable	98
IV.45	Hasil Enkripsi	98
IV.46	Hasil Dekripsi	98
IV.47	Pengujian Dekompresi Huffman	99
IV.48	Proses Pengujian Dekripsi DES	100

IV.49 File Chiperteks	100
IV.50 File Plainteks	101



DAFTAR TABEL

Tabel	Halaman
II.1 Kunci Ekternal 64 bit	25
II.2 Matriks Permutasi Kompresi PC-1	26
II.3 Jumlah Pergeseran bit pada tiap putaran	26
II.4 Matriks Permutasi Kompresi -2 (PC-2)	27
II.5 Matriks Permutasi Ekspansi	28
II.6 S-box	29
II.7 P-box	30
II.8 Matriks Invers Inisial Permutasi	30
II.9 Tinjauan Studi	36
III.1 Jadwal Penelitian.....	49
IV.1 Perbandingan Chiperteks dan Plainteks	88
IV.2 Hasil Kuisioner Pengujian Imperecbility	94
IV.3 Pengujian Fidelity Menggunakan MSE dan PSNR.....	97

DAFTAR LAMPIRAN

Lampiran	Halaman
1 Wawancara kepada Juru Buku	107
2 Wawancara kepada Manajer	109
3 Contoh bentuk Jurnal Umum KJKS BMT	110
4 Contoh bentuk Buku Besar KJKS BMT	111
5 Format Kuisisioner Pengujian <i>Imperecibility</i>	112



CERDAS BERBUDI LUHUR

DAFTAR PUSTAKA

- [Anhar 2010] Anhar, 2010. *Membuat Aplikasi Data Base MySQL*. Gava Media, Yogyakarta
- [Ariyus 2006] Ariyus, Dony, 2006. *Kriptografi Keamanan Data dan Komunikasi*. Graha Ilmu, Yogyakarta.
- [Ariyus 2008] Ariyus, Dony, 2008. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Andi Offset, Yogyakarta.
- [ARB 2013] Ari Wibowo, 2013. *Kompresi Data Menggunakan Metode Huffman*, Teknik Informatika. Politeknik Negeri Batam
- [Ernita 2013] Ernita Sitohang, 2013. *Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma DES*, Pelita Informatika Budi Darma, ISSN 2301-9425
- [Kurniawan 2004] Kurniawan, Yusuf, 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Informatika, Bandung.
- [MFK 2013] Mufida Khairani, Sajadin Sembiring, 2013. *Analisis dan Implementasi Steganografi Pada Citra GIF Menggunakan Algoritma GifShuffle*, SNASTIKOM, ISBN 978-602-19837-3-7.
- [Morkel 2005] Morkel, T., Eloff, J.H.P., Olivier, M.S., 2005. *An Overview of Citra Steganography*.
- [MRA 2013] Maria Roslin Apriana Neta, 2013. *Perbandingan Algoritma Kompresi Terhadap Objek Citra Menggunakan Java*, SEMANTIK 2013, ISBN 979-26-0266-6.
- [Munir 2006] Munir, Rinaldi, 2006. *Diktat Kuliah IF5054 Kriptografi*.
- [Penalosa 2005] Penalosa, 2005. *Steganografi Pada Citra dengan Format GIF Menggunakan Algoritma GifShuffle*, Teknik Informatika. Institut Teknologi Bandung.
- [RP 2011] Rifkie Primartha, 2011. *Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)*, Universitas Sriwijaya, ISSN 2085-1588
- [Sadikin 2012] Sadikin, Rifki, 2012. *Kriptografi untuk Keamanan Jaringan*. Andi Offset, Yogyakarta.