



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk mengubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**IMPLEMENTASI STEGANOGRAFI LSB DAN LIBRARY
ENKRIPSI AES-128 KE BANYAK DOKUMEN PDF**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer (S.Kom.)**



Naldiyanto Sofian

14110110023

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG**

2018

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI STEGANOGRAFI LSB DAN LIBRARY ENKRIPSI AES-128 KE BANYAK DOKUMEN PDF

Oleh

Nama : Naldiyanto Sofian

NIM : 14110110023

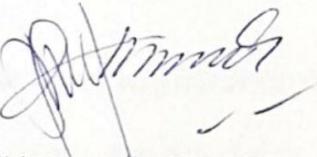
Fakultas : Teknik dan Informatika

Program Studi : Informatika

Tangerang, 13 Agustus 2018

Ketua Sidang

Dosen Pengaji



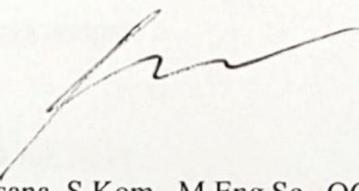
Adhi Kusnadi, S.T., M.Si.



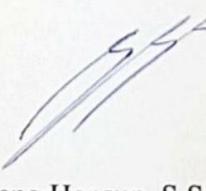
Dennis Gunawan, S.Kom., M.Sc.

Dosen Pembimbing I

Dosen Pembimbing II



Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH

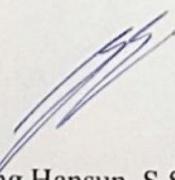


Seng Hansun, S.Si., M.Cs.

Mengetahui

Ketua Program Studi

Informatika



Seng Hansun, S.Si., M.Cs.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya:

Nama : Naldiyanto Sofian

NIM : 14110110023

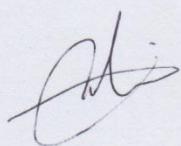
Fakultas : Teknik dan Informatika

Program Studi : Informatika

menyatakan bahwa skripsi yang berjudul "**Implementasi Steganografi LSB dan Library Enkripsi AES-128 ke Banyak Dokumen PDF**" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/ penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 9 Juli 2018



Naldiyanto Sofian

**MULTIMEDIA
NUSANTARA**

**PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Naldiyanto Sofian

NIM : 14110110023

Program Studi: Informatika

Fakultas : Teknik dan Informatika

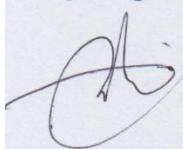
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui dan memberikan izin kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul: **Implementasi Steganografi LSB dan Library Enkripsi AES-128 ke Banyak Dokumen PDF** beserta perangkat yang diperlukan.

Dengan Hak Bebas Royalti Non-eksklusif ini, pihak Universitas Multimedia Nusantara berhak menyimpan, mengalihmedia atau *format-kan*, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mendistribusi dan menampilkan atau memublikasikan karya ilmiah saya di internet atau media lain untuk kepentingan akademis, tanpa perlu meminta izin dari saya maupun memberikan royalty kepada saya, selama tetap mencantumkan nama saya sebagai penulis karya ilmiah tersebut.

Demikian pernyataan ini saya buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Tangerang, 9 Juli 2018



(Naldiyanto Sofian)

KATA PENGANTAR

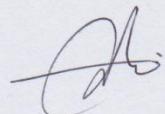
Puji Syukur kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya laporan skripsi dengan judul “Implementasi Steganografi LSB dan Library Enkripsi AES-128 ke Banyak Dokumen PDF” dapat diselesaikan pada waktunya.

Penulis juga mengucapkan terima kasih kepada:

1. Dr. Ninok Leksono, Rektor Universitas Multimedia Nusantara, yang memberi inspirasi bagi penulis untuk berprestasi,
2. Hira Meidia, Ph.D., Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara,
3. Seng Hansun, S.Si., M.Cs., Ketua Program Studi Informatika Universitas Multimedia Nusantara, yang menerima penulis dengan baik untuk berkonsultasi,
4. Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH dan Seng Hansun, S.Si., M.Cs., yang telah membimbing pembuatan skripsi dan yang telah mengajar penulis tata cara menulis karya ilmiah dengan benar,
5. Keluarga yang selalu memberi dukungan dalam penyelesaian laporan, dan
6. Seluruh teman-teman yang tidak dapat disebutkan satu per satu.

Diharapkan laporan ini dapat menambah wawasan dan bermanfaat bagi para pembaca.

Tangerang, 9 Juli 2018



Naldiyanto Sofian

IMPLEMENTASI STEGANOGRAFI LSB DAN LIBRARY

ENKRIPSI AES-128 KE BANYAK DOKUMEN PDF

ABSTRAK

Keamanan menjadi salah satu faktor penting dalam komunikasi di dunia sekarang. Steganografi dibantu dengan kriptografi dapat digunakan untuk menyembunyikan dan mengamankan informasi. Salah satu teknik steganografi yaitu *Least Significant Bit* (LSB). Teknik LSB dapat diterapkan pada *Portable Document Format* (PDF) dengan memanfaatkan *Tj Operator*. Sebuah program yang dapat melakukan steganografi ke banyak dokumen PDF dibuat untuk meningkatkan kapasitas steganografi pada dokumen PDF. Program tersebut diberi nama MPDFStego. MPDFStego dibuat dengan bahasa pemrograman Java, dibantu dengan *library* JavaFX sebagai pembangun tampilannya. *Secret text* yang nantinya disembunyikan ke dalam dokumen PDF, terlebih dahulu dienkripsi menggunakan enkripsi *Advanced Encryption Standard* dengan *key* berukuran 128 bit (AES-128) mode *Cipher Block Chaining* (CBC), yang berasal dari *library* javax.crypto. Rekompresi dan dekompresi dokumen PDF dilakukan terpisah dari MPDFStego menggunakan *tool* QPDF. Hasil uji coba yang dilakukan pada MPDFStego menunjukkan bahwa enkripsi AES-128 CBC yang diimplementasikan sudah sesuai. MPDFStego juga terbukti mampu menyembunyikan *secret text* ke banyak dokumen PDF. *Peak Signal-to-Noise Ratio* (PSNR) juga dihitung untuk dua *stego file* PDF yang dievaluasi, menghasilkan nilai rata-rata PSNR yang lebih tinggi daripada program banding, yaitu 29,78 untuk *file* pertama, dan 44,16 untuk *file* kedua.

Kata Kunci: *Advanced Encryption Standard*, *Least Significant Bit*, *Portable Document Format*, *Steganography*, *Tj Operator*

UNIVERSITAS
MULTIMEDIA
NUSANTARA

IMPLEMENTATION OF LSB STEGANOGRAPHY AND AES-128

ENCRYPTION LIBRARY TO MULTIPLE PDF DOCUMENTS

ABSTRACT

Security has become one of important factors in communication in the world now. Steganography with help of cryptography can be used to hide and secure information. One of the steganography technique is Least Significant Bit (LSB). LSB technique can be applied to Portable Document Format (PDF) file by changing the Tj Operator values. A program which can do steganography to multiple PDF documents is built and named MPDFStego to increase steganography capacity in PDF documents. MPDFStego is built using Java programming language, and JavaFX for its Graphical User Interface library. Secret text is encrypted using Advanced Encryption Standard with 128-bit size key (AES-128) and Cipher Block Chaining (CBC) mode from javax.crypto library before it is hidden inside PDF documents. Recompression and decompression of PDF documents is done separately from MPDFStego, using QPDF. Tests which are done to MPDFStego show that AES-128 CBC encryption is correctly implemented. It is proven that MPDFStego is capable of hiding secret text into multiple PDF documents. Peak Signal-to-Noise Ratio (PSNR) is calculated for the two evaluated stego file PDF, resulting in average PSNR value of 29.78 for the first file, and 44.16 for the second file. These values are higher compared to the other program.

Keywords: Advanced Encryption Standard, Least Significant Bit, Portable Document Format, Steganography, Tj Operator

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR ISI

HALAMAN JUDUL.....	i
LEMBAR PENGESAHAN SKRIPSI	ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	iii
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS.....	iv
KATA PENGANTAR.....	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan Laporan Penelitian.....	5
BAB II LANDASAN TEORI	7
2.1 Steganografi.....	7
2.1.1 Least Significant Bit.....	7
2.2 Advanced Encryption Standard	8
2.2.1 AES Key Expansion.....	17
2.2.2 Cipher Block Chaining	19
2.2.3 javax.crypto.....	21
2.3 PDF.....	22
2.3.1 Tj Operator.....	24
2.4 Peak Signal-to-Noise Ratio	25
BAB III METODOLOGI DAN PERANCANGAN PROGRAM	26
3.1 Metodologi Penelitian	26
3.2 Perancangan Program	27
3.2.1 Flowchart	27
3.2.2 Desain Antarmuka.....	36
BAB IV IMPLEMENTASI DAN UJI COBA	42
4.1 Implementasi Program.....	42
4.1.1 Lingkup Implementasi	42
4.1.2 Hasil Implementasi	43
4.2 Pengujian Program	49
4.2.1 Proses Pengujian.....	49
4.3 Evaluasi Hasil	64
BAB V SIMPULAN DAN SARAN	70
5.1 Simpulan.....	70
5.2 Saran	70
DAFTAR PUSTAKA	72
DAFTAR LAMPIRAN	75

DAFTAR GAMBAR

Gambar 2.1 Enkripsi dan Dekripsi AES	10
Gambar 2.2 Substitution Box (S-Box) yang Digunakan pada Enkripsi AES	11
Gambar 2.3 Perkalian 87 dengan 131 pada operasi AES	12
Gambar 2.4 Binary XOR Long Division	13
Gambar 2.5 Matrix Multiplication AES dalam Decimal	13
Gambar 2.6 Rincian Matrix Multiplication AES	14
Gambar 2.7 Inverse S-box.....	16
Gambar 2.8 Matriks yang Digunakan pada InvMixColumns dalam Hexadecimal	17
Gambar 2.9 Key Expansion Algorithm.....	18
Gambar 2.10 Round Constant untuk Putaran 1 sampai 10	19
Gambar 2.11 Enkripsi pada Mode CBC.....	20
Gambar 2.12 Dekripsi pada Mode CBC	20
Gambar 2.13 Contoh dari Tj Operator	24
Gambar 2.14 Peak Signal-to-Noise Ratio	25
Gambar 2.15 Mean-squared Error.....	25
Gambar 3.1 Tahapan Metodologi Penelitian.....	26
Gambar 3.2 Flowchart Utama (main)	28
Gambar 3.3 Flowchart Tab Hide (hideTab)	29
Gambar 3.4 Flowchart Tab Hide Lanjutan (hideTab)	31
Gambar 3.5 Flowchart Tab Extract (extractTab)	33
Gambar 3.6 Flowchart Tab Extract Lanjutan (extractTab)	35
Gambar 3.7 Rancangan Antarmuka Tab Hide	36
Gambar 3.8 Rancangan Antarmuka Sebelum Memulai Proses Hiding	37
Gambar 3.9 Rancangan Antarmuka Minta File Selanjutnya saat Proses Steganografi	37
Gambar 3.10 Rancangan Antarmuka saat Proses Steganografi Selesai.....	38
Gambar 3.11 Rancangan Antarmuka Tab Extract	38
Gambar 3.12 Rancangan Antarmuka Sebelum Memulai Proses Ekstraksi Data ...	39
Gambar 3.13 Rancangan Antarmuka Minta File Selanjutnya saat Proses Ekstraksi	39
Gambar 3.14 Rancangan Antarmuka saat Proses Ekstraksi Selesai	40
Gambar 3.15 Rancangan Antarmuka Tab How To	40
Gambar 3.16 Rancangan Antarmuka Tab About	41
Gambar 4.1 Tampilan Antarmuka Tab Hide	43
Gambar 4.2 Tampilan Antarmuka Meminta File Selanjutnya pada Proses Hiding	44
Gambar 4.3 Tampilan Antarmuka Setelah Proses Hiding Selesai	45
Gambar 4.4 Tampilan Antarmuka Tab Extract	46
Gambar 4.5 Tampilan Antarmuka Proses Ekstraksi Meminta File Selanjutnya	47
Gambar 4.6 Tampilan Antarmuka Setelah Proses Extracting Selesai	47
Gambar 4.7 Tampilan Antarmuka Tab How to Use	48
Gambar 4.8 Tampilan Antarmuka Tab About	49
Gambar 4.9 Tampilan Tab Hiding sebelum Steganografi Dimulai	50
Gambar 4.10 Log Hasil Steganografi Program.....	51

Gambar 4.11 Tool Enkripsi dengan Masukan dan Keluarannya	51
Gambar 4.12 Hasil Dekripsi dengan Tool Enkripsi Online	52
Gambar 4.13 Hasil Plaintext setelah Program Menjalankan Fungsi Extract	52
Gambar 4.14 Log Hasil Proses Ekstraksi Program	53
Gambar 4.15 Log Steganografi Skenario Pertama	56
Gambar 4.16 Hasil Ekstraksi Secret Text Skenario Pertama	56
Gambar 4.17 Tj Operator pada Dokumen PDF sebelum Steganografi.....	57
Gambar 4.18 Tj Operator pada Dokumen PDF Setelah Steganografi	59
Gambar 4.19 Tampilan Pesan Error dari Program pdf_hide	60
Gambar 4.20 Hasil Ekstraksi Secret Text Skenario Ketiga	61
Gambar 4.21 Hasil Ekstraksi Secret Text Skenario Keempat.....	62
Gambar 4.22 Command Enkripsi menggunakan QPDF	63
Gambar 4.23 Penjelasan Parameter encrypt pada QPDF	63
Gambar 4.24 Tampilan Error MPDFStego untuk Cover File PDF Terenkripsi	64



DAFTAR TABEL

Tabel4.1 Tabel Masukan dan Keluaran Pengujian Enkripsi Kedua	53
Tabel4.2 Tabel Masukan dan Keluaran Pengujian Enkripsi Ketiga	54
Tabel4.3 Tabel Masukan dan Keluaran Skenario Pertama	55
Tabel4.4 ASCII dan Biner dari Secret Text	57
Tabel4.5 Nilai Tj Operator Sebelum dan Sesudah Hiding	58
Tabel4.6 Tabel Masukan dan Keluaran Skenario Ketiga.....	60
Tabel4.7 Tabel Masukan dan Keluaran Skenario Keempat	62
Tabel4.8 Tabel Masukan untuk MPDFStego	64
Tabel4.9 Tabel Daftar Cover File PDF dan Plaintext	67
Tabel4.10 Ukuran Stego File nLines.pdf	67
Tabel4.11 Ukuran Stego File latexExample.pdf	68

