

**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD*  
(AES) DAN TEKNIK STEGANOGRAFI *BIT PLANE COMPLEXITY*  
*SEGMENTATION* (BPCS) DALAM ESKALASI KEAMANAN FILE TEKS**

**SKRIPSI**

**AFTHAR KAUTSAR**

**0701212239**



**PROGRAM STUDI ILMU KOMPUTER  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA  
MEDAN  
2024**

**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD*  
(AES) DAN TEKNIK STEGANOGRAFI *BIT PLANE COMPLEXITY*  
*SEGMENTATION* (BPCS) DALAM ESKALASI KEAMANAN FILE TEKS**

**SKRIPSI**

*Diajukan Untuk Memenuhi Syarat Mencapai Gelar Sarjana Komputer*

**AFTHAR KAUTSAR**

**0701212239**



**PROGRAM STUDI ILMU KOMPUTER  
FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA  
MEDAN  
2024**

## PERSETUJUAN TUGAS AKHIR

Hal : Surat Persetujuan Tugas Akhir  
Lamp : -

Kepada Yth.,  
Dekan Fakultas Sains dan Teknologi  
Universitas Islam Negeri Sumatera Utara

*Assalamu'alaikum Wr. Wb.*

Setelah membaca, meneliti, memberikan petunjuk, dan mengoreksi serta mengadakan perbaikan, maka kami selaku pembimbing berpendapat bahwa Tugas Akhir saudara,

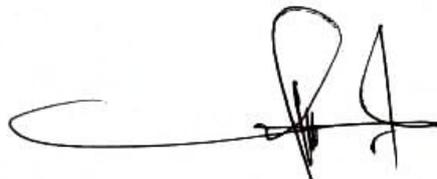
Nama : Afthar Kautsar  
NIM : 0701212239  
Program Studi : Ilmu Komputer  
Judul : Implementasi Algoritma *Advanced Encryption Standard* (AES) Dan Teknik Steganografi *Bit Plane Complexity Segmentation* (BPCS) Dalam Eskalasi Keamanan File Teks

dapat disetujui untuk segera dikolokiumkan. Atas perhatiannya kami ucapkan terimakasih.

*Wassalamu'alaikum Wr. Wb.*

Medan, 06 Februari 2025 M  
07 Sya'ban 1446 H

Pembimbing



**Muhammad Ikhsan, ST., M.Kom**  
NIP. 198304152011011008

## SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertanda tangan di bawah ini,

Nama : Afthar Kautsar

NIM : 0701212239

Program Studi : Ilmu Komputer

Judul : Implementasi Algoritma *Advanced Encryption Standard*  
(AES) Dan Teknik Steganografi *Bit Plane Complexity*  
*Segmentation* (BPCS) Dalam Eskalasi Keamanan File Teks

menyatakan bahwa Tugas Akhir ini adalah hasil karya saya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya. Apabila di kemudian hari ditemukan plagiat dalam Tugas Akhir ini maka saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi lainnya sesuai dengan peraturan yang berlaku.

Medan, 6 Februari 2025



Afthar Kautsar  
NIM. 0701212239



KEMENTERIAN AGAMA REPUBLIK INDONESIA  
UNIVERSITAS ISLAM NEGERI SUMATERA UTARA MEDAN  
FAKULTAS SAINS DAN TEKNOLOGI

Jl. Lap. Golf No 120, Desa Durian Jangak, Kec. Pancur Batu, Kode Pos 20235  
Telp. (061) 6615683-6622925, Fax. (061) 6615683  
Url: www.saintek.uinsu.ac.id, E-mail: saintek@uinsu.ac.id

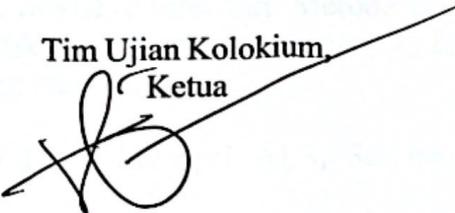
**PENGESAHAN TUGAS AKHIR**  
Nomor : B.160/ST.ST.V2/PP/01/01/04/2025

Judul : Implementasi Algoritma *Advanced Encryption Standard* (AES) Dan Teknik Steganografi *Bit Plane Complexity Segmentation* (BPCS) Dalam Eskalasi Keamanan File Teks  
Nama : Afthar Kautsar  
NIM : 0701212239  
Program Studi : Ilmu Komputer  
Fakultas : Sains dan Teknologi

Telah dipertahankan dihadapan Dewan Penguji Tugas Akhir Program Studi Ilmu Komputer Fakultas Sains dan Teknologi UIN Sumatera Utara Medan dan dinyatakan **LULUS**.

Pada Hari/Tanggal : Rabu/ 16 April 2025  
Tempat : Ruang Sidang Fakultas Sains dan Teknologi

Tim Ujian Kolokium,  
Ketua



Ilka Zufria, M.Kom  
NIP. 198506042015031006

Dewan Penguji,

Penguji



Abdul Halim Hasugian, M.Kom  
NIP. 198803272023211020

Pembimbing



Muhammad Ikhsan, S.T., M.Kom  
NIP. 198304152011011008

Mengesahkan,  
Wakil Dekan Bidang Akademik & Kelembagaan  
Fakultas Sains dan Teknologi  
UIN Sumatera Medan



Dr. M. Ridwan M. Ag  
NIP. 197608202003121004

## ABSTRAK

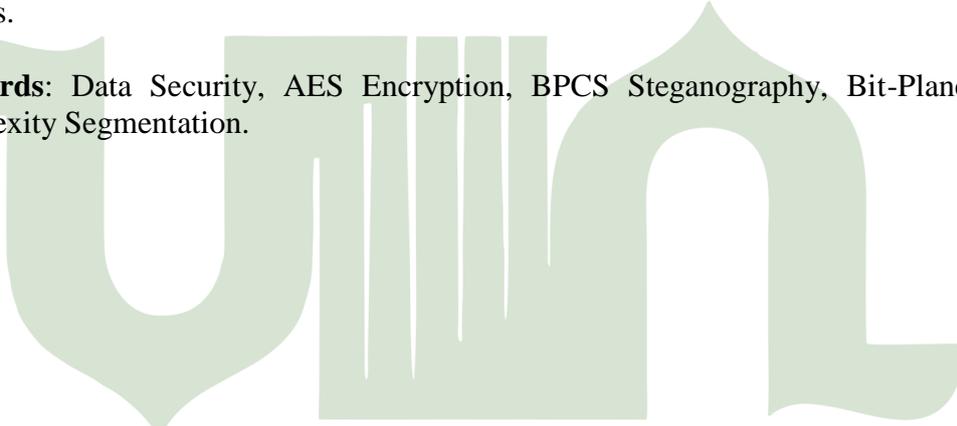
Di zaman sekarang, menjaga keamanan data sangat penting karena hampir semua informasi dikirim dan disimpan secara digital. Salah satu cara untuk melindungi data adalah dengan mengenkripsi informasi menggunakan Advanced Encryption Standard (AES), yang dikenal sebagai metode enkripsi yang aman dan banyak digunakan. Namun, hanya mengenkripsi data saja belum cukup karena informasi yang terenkripsi masih bisa menarik perhatian pihak yang tidak berwenang. Oleh karena itu, teknik steganografi Bit-Plane Complexity Segmentation (BPCS) digunakan untuk menyembunyikan data dalam gambar digital agar lebih sulit dideteksi. Penelitian ini bertujuan untuk meningkatkan keamanan data dengan menggabungkan enkripsi AES dan steganografi BPCS. Data teks pertama-tama dienkripsi menggunakan AES agar tidak bisa dibaca oleh siapa pun tanpa kunci yang benar. Setelah itu, hasil enkripsi disisipkan ke dalam gambar menggunakan teknik BPCS, yang memilih bagian gambar dengan pola kompleks untuk menyimpan data tanpa mengubah tampilan gambar secara mencolok. Hasil penelitian menunjukkan bahwa metode ini dapat menjaga keamanan data dengan baik. Data yang telah disisipkan dalam gambar tetap bisa diekstraksi kembali dengan akurasi tinggi, sementara kualitas gambar tidak mengalami perubahan yang mencolok. Kesimpulannya, menggabungkan enkripsi AES dan steganografi BPCS memberikan perlindungan ganda: data dienkripsi agar tidak bisa dibaca dan disembunyikan agar tidak mudah ditemukan. Metode ini dapat diterapkan dalam berbagai bidang, baik untuk keperluan pribadi maupun bisnis, yang memerlukan sistem keamanan data yang lebih kuat.

**Kata Kunci:** Keamanan Data, Enkripsi AES, Steganografi BPCS, Bit-Plane Complexity Segmentation.

## ABSTRACT

Nowadays, ensuring data security is crucial as most information is transmitted and stored digitally. One effective way to protect data is by encrypting it with Advanced Encryption Standard (AES), a widely used and highly secure encryption method. However, encryption alone is not enough, as encrypted data might still attract the attention of unauthorized parties. To further enhance security, the Bit-Plane Complexity Segmentation (BPCS) steganography technique is used to conceal encrypted data within digital images, making it harder to detect. This study aims to enhance data security by integrating AES encryption with BPCS steganography. First, text data is encrypted using AES, ensuring that it cannot be read without the correct key. Then, the encrypted data is embedded into an image using the BPCS technique, which selects complex patterns within the image to store the data discreetly without significantly altering its appearance. The results indicate that this method effectively secures data. The embedded information can be accurately extracted, and the image quality remains visually unchanged. In conclusion, combining AES encryption with BPCS steganography provides dual-layer protection: encrypting data to make it unreadable and hiding it to prevent detection. This approach can be applied in various fields, both personal and business-related, requiring stronger data security systems.

**Keywords:** Data Security, AES Encryption, BPCS Steganography, Bit-Plane Complexity Segmentation.



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## KATA PENGANTAR

*Assalamu'alaikum warahmatullahi wabarakatuh...*

Segala puji dan syukur kita panjatkan kepada Allah Subhanahu wa Ta'ala yang telah melimpahkan rahmat, taufik, dan hidayah-Nya, serta shalawat dan salam kita hadiahkan kepada junjungan kita yaitu Baginda Nabi besar Muhammad SAW semoga kita mendapatkan syafaatnya di hari kelak, sehingga saya dapat menyelesaikan Tugas Akhir yang berjudul " Implementasi Algoritma *Advanced Encryption Standard* (AES) dan Teknik Steganografi *Bit Plane Complexity Segmentation* (BPCS) Dalam Eskalasi Keamanan File Teks ". Penyusunan Tugas Akhir ini merupakan salah satu syarat kelulusan dan untuk memperoleh gelar Sarjana di Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara.

Dalam kesempatan ini, saya ingin mengucapkan terima kasih kepada orang tua saya, ayahanda Suprianto dan ibunda Ellylawati, A.Md, serta keluarga. Yang mana mereka selalu memberikan semangat dan dukungan dalam bentuk materi maupun moril dalam menyelesaikan studi ini.

Dalam proses pengerjaan Tugas Akhir ini, penulis sangat tidak lepas dari bantuan berbagai pihak dan sudah seharusnya penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Ibu Prof. Dr. Nurhayati, M.Ag selaku Rektor Universitas Islam Negeri Sumatera Utara Medan.
2. Bapak Dr. Zulham, S.H.I., M.Hum selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan.
3. Bapak Ilka Zufria, M.Kom selaku Ketua Program Studi Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan.
4. Bapak Dr. M. Fakhriza, S.T, M.Kom selaku Sekretaris Program Studi Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan.

5. Bapak Muhammad Ikhsan, S.T, M.Kom selaku Dosen Pembimbing Program Studi Ilmu Komputer Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Utara Medan.
6. Bapak Mhd. Ikhsan Rifki, S.Tr.T., M.T selaku Dosen Pembimbing Akademik yang telah memberikan banyak masukan serta motivasi dari awal perkuliahan hingga akhir.
7. Seluruh dosen, staf dan karyawan Program Studi Ilmu Komputer, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara Medan.
8. Teman-teman stambuk 2021 terkhususnya kelas Ilmu Komputer 6 yang baik dan selalu memberi semangat selama menjalani perkuliahan yang tidak dapat saya sebutkan satu persatu.
9. Semua pihak yang dengan tulus dan ikhlas memberikan doa dan motivasi kepada saya yang tidak dapat disebutkan satu persatu.
10. Dan saya sendiri yang telah bertahan selama perkuliahan ini.

Dalam penyusunan Tugas Akhir ini saya menyadari bahwa masih terdapat kekurangan dan kesalahan untuk itu saran dan kritik yang sifatnya membangun sangat diharapkan demi kebaikan kedepannya. Akhir kata saya berharap yang dimana semoga hasil dari Tugas Akhir ini dapat bermanfaat dan membantu semua pihak yang membutuhkannya terutama dalam bidang Ilmu Komputer serta dapat bernilai pahala disisi-Nya. Semoga Allah SWT memberikan rahmat dan hidayah-Nya kepada kita semua.

*Wassalamu'alaikum warahmatullahi wabarakatuh...*

UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN  
Medan, 24 September 2024

Penulis

Afthar Kautsar  
NIM. 0701212239

## DAFTAR ISI

### ABSTRAK

### ABSTRACT

<b>KATA PENGANTAR.....</b>	<b>i</b>
<b>DAFTAR ISI.....</b>	<b>iii</b>
<b>DAFTAR GAMBAR.....</b>	<b>vii</b>
<b>DAFTAR TABEL .....</b>	<b>xi</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xii</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian .....	2
1.5 Manfaat Penelitian .....	2
1.6 Kajian Terdahulu.....	2
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>4</b>
2.1 Kriptografi.....	4
2.1.1 Pengertian Kriptografi.....	4
2.1.2 Sejarah Kriptografi.....	4
2.1.3 Tujuan Kriptografi .....	5
2.1.4 Elemen Kriptografi.....	5
2.2 Enkripsi dan Dekripsi.....	6
2.3 <i>Advanced Encryption Standard (AES)</i> .....	6
2.4 Steganografi .....	18
2.5 <i>Bit Plane Complexity Segmentation (BPCS)</i> .....	19
2.6 Citra Digital.....	26
2.7 Eskalasi Keamanan File .....	27
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>29</b>
3.1 Kerangka Penelitian .....	29
3.2 Rencana Pembahasan .....	30
3.2.1 <i>Flowchart</i> Proses Enkripsi dan Dekripsi AES .....	31

3.2.2 <i>Flowchart</i> Proses Penyisipan dengan Steganografi BPCS .....	33
3.3 Lokasi Penelitian .....	35
3.4 Waktu Penelitian .....	35
3.5 Rencana Penerbitan .....	35
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>36</b>
4.1 Pengujian Program .....	36
4.2 Proses Enkripsi .....	38
4.2.1 File TXT .....	39
4.2.2 File PDF .....	39
4.2.3 File DOCX .....	41
4.3 Proses Dekripsi .....	42
4.3.1 File TXT .....	43
4.3.2 File PDF .....	43
4.3.3 File DOCX .....	44
4.4 Analisis Kompleksitas <i>Bit-Plane</i> .....	44
4.5 Proses Penyisipan Pesan .....	46
4.5.1 Penyisipan File TXT .....	47
4.5.2 Penyisipan File PDF .....	48
4.5.3 Penyisipan File DOCX .....	49
4.6 Ekstraksi Pesan .....	50
4.6.1 Ekstraksi File TXT .....	51
4.6.2 Ekstraksi File PDF .....	51
4.6.3 Ekstraksi File DOCX .....	51
4.7 Evaluasi Sistem .....	52
4.8 Perbandingan Waktu Eksekusi Proses .....	54
4.8.1 Waktu Enkripsi .....	54
4.8.2 Waktu Dekripsi .....	55
4.8.3 Waktu Penyisipan Pesan .....	55
4.8.4 Waktu Ekstraksi Pesan .....	56
4.9 Analisis Keamanan Sistem .....	57
4.9.1 Keunggulan Algoritma AES .....	58
4.9.2 Keunggulan Teknik BPCS .....	55

4.9.3 Analisis Keamanan Gabungan AES + BPCS .....	59
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>62</b>
5.1 Kesimpulan .....	62
5.2 Saran.....	62
<b>DAFTAR PUSTAKA .....</b>	<b>64</b>



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

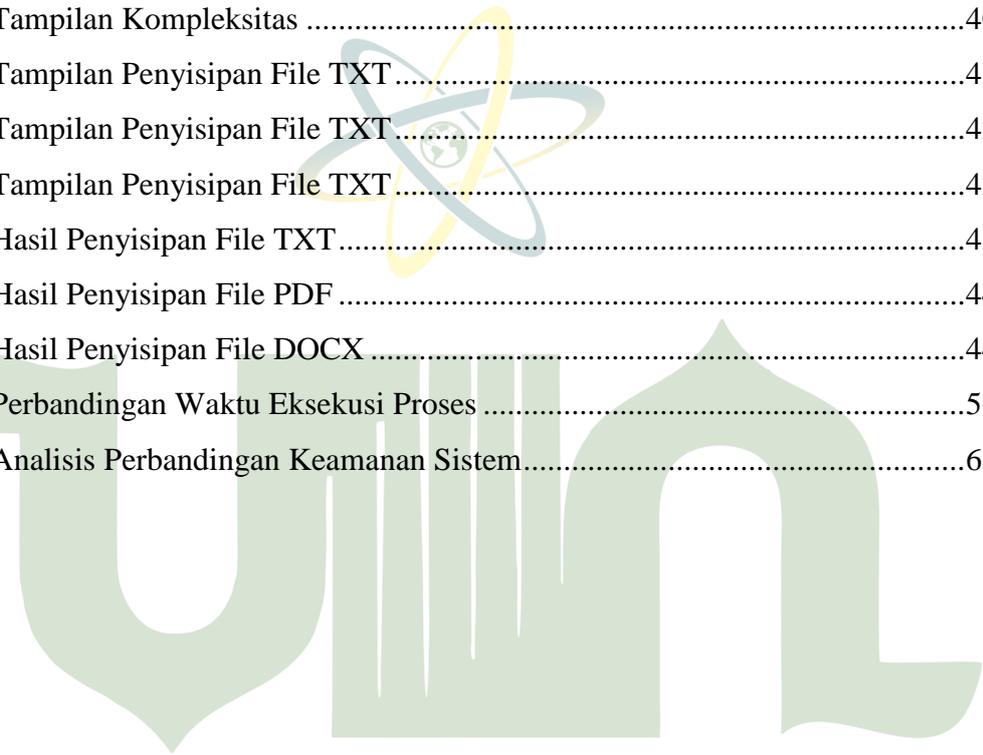
## DAFTAR GAMBAR

<b>Gambar</b>	<b>Judul Gambar</b>	<b>Halaman</b>
2.1	Contoh <i>Plaintext</i> .....	7
2.2	Contoh Kunci .....	7
2.3	Hasil XOR <i>Plaintext</i> dan Kunci .....	7
2.4	Tahap Awal <i>AddRoundKey</i> .....	7
2.5	Tahap <i>SubBytes</i> 1 .....	8
2.6	Tahap <i>ShiftRows</i> 1 .....	8
2.7	Tahap <i>MixColumns</i> 1 .....	8
2.8	Tahap <i>AddRoundKey</i> 1 .....	8
2.9	Tahap <i>SubBytes</i> 2 .....	8
2.10	Tahap <i>ShiftRows</i> 2 .....	8
2.11	Tahap <i>MixColumns</i> 2 .....	8
2.12	Tahap <i>AddRoundKey</i> 2 .....	8
2.13	Tahap <i>SubBytes</i> 3 .....	9
2.14	Tahap <i>ShiftRows</i> 3 .....	9
2.15	Tahap <i>MixColumns</i> 3 .....	9
2.16	Tahap <i>AddRoundKey</i> 3 .....	9
2.17	Tahap <i>SubBytes</i> 4 .....	9
2.18	Tahap <i>ShiftRows</i> 4 .....	9
2.19	Tahap <i>MixColumns</i> 4 .....	9
2.20	Tahap <i>AddRoundKey</i> 4 .....	9
2.21	Tahap <i>SubBytes</i> 5 .....	10
2.22	Tahap <i>ShiftRows</i> 5 .....	10
2.23	Tahap <i>MixColumns</i> 5 .....	10
2.24	Tahap <i>AddRoundKey</i> 5 .....	10
2.25	Tahap <i>SubBytes</i> 6 .....	10
2.26	Tahap <i>ShiftRows</i> 6 .....	10
2.27	Tahap <i>MixColumns</i> 6 .....	10
2.28	Tahap <i>AddRoundKey</i> 6 .....	10

2.29 Tahap <i>SubBytes</i> 7 .....	11
2.30 Tahap <i>ShiftRows</i> 7 .....	11
2.31 Tahap <i>MixColumns</i> 7 .....	11
2.32 Tahap <i>AddRoundKey</i> 7 .....	11
2.33 Tahap <i>SubBytes</i> 8 .....	11
2.34 Tahap <i>ShiftRows</i> 8 .....	11
2.35 Tahap <i>MixColumns</i> 8 .....	11
2.36 Tahap <i>AddRoundKey</i> 8 .....	11
2.37 Tahap <i>SubBytes</i> 9 .....	12
2.38 Tahap <i>ShiftRows</i> 9 .....	12
2.39 Tahap <i>MixColumns</i> 9 .....	12
2.40 Tahap <i>AddRoundKey</i> 9 .....	12
2.41 Hasil <i>SubBytes</i> .....	12
2.42 Hasil <i>ShiftRows</i> .....	12
2.43 Hasil <i>AddRoundKey</i> .....	12
2.44 Tahap Awal <i>Decrypt</i> .....	13
2.45 Tahap <i>InvShiftRows</i> 9 .....	13
2.46 Tahap <i>InvSubBytes</i> 9 .....	13
2.47 Tahap <i>InvAddRoundKey</i> 9 .....	13
2.48 Tahap <i>InvMixColumns</i> 9 .....	13
2.49 Tahap <i>InvShiftRows</i> 8 .....	13
2.50 Tahap <i>InvSubBytes</i> 8 .....	13
2.51 Tahap <i>InvAddRoundKey</i> 8 .....	13
2.52 Tahap <i>InvMixColumns</i> 8 .....	13
2.53 Tahap <i>InvShiftRows</i> 7 .....	14
2.54 Tahap <i>InvSubBytes</i> 7 .....	14
2.55 Tahap <i>InvAddRoundKey</i> 7 .....	14
2.56 Tahap <i>InvMixColumns</i> 7 .....	14
2.57 Tahap <i>InvShiftRows</i> 6 .....	14
2.58 Tahap <i>InvSubBytes</i> 6 .....	14
2.59 Tahap <i>InvAddRoundKey</i> 6 .....	14
2.60 Tahap <i>InvMixColumns</i> 6 .....	14

2.61 Tahap <i>InvShiftRows</i> 5.....	15
2.62 Tahap <i>InvSubBytes</i> 5.....	15
2.63 Tahap <i>InvAddRoundKey</i> 5.....	15
2.64 Tahap <i>InvMixColumns</i> 5.....	15
2.65 Tahap <i>InvShiftRows</i> 4.....	15
2.66 Tahap <i>InvSubBytes</i> 4.....	15
2.67 Tahap <i>InvAddRoundKey</i> 4.....	15
2.68 Tahap <i>InvMixColumns</i> 4.....	15
2.69 Tahap <i>InvShiftRows</i> 3.....	16
2.70 Tahap <i>InvSubBytes</i> 3.....	16
2.71 Tahap <i>InvAddRoundKey</i> 3.....	16
2.72 Tahap <i>InvMixColumns</i> 3.....	16
2.73 Tahap <i>InvShiftRows</i> 2.....	16
2.74 Tahap <i>InvSubBytes</i> 2.....	16
2.75 Tahap <i>InvAddRoundKey</i> 2.....	16
2.76 Tahap <i>InvMixColumns</i> 2.....	16
2.77 Tahap <i>InvShiftRows</i> 1.....	16
2.78 Tahap <i>InvSubBytes</i> 1.....	17
2.79 Tahap <i>InvAddRoundKey</i> 1.....	17
2.80 Tahap <i>InvMixColumns</i> 1.....	17
2.81 Hasil <i>InvShiftRows</i> .....	17
2.82 Hasil <i>InvSubBytes</i> .....	17
2.83 Hasil <i>AddRoundKey</i> .....	18
2.84 Contoh Sebuah Citra 8x8 Piksel.....	20
2.85 Konversi Nilai Bit-Plane 0.....	21
2.86 Konversi Nilai Bit-Plane 1.....	21
2.87 Konversi Nilai Bit-Plane 2.....	21
2.88 Konversi Nilai Bit-Plane 3.....	21
2.89 Konversi Nilai Bit-Plane 4.....	22
2.90 Konversi Nilai Bit-Plane 5.....	22
2.91 Konversi Nilai Bit-Plane 6.....	22
2.92 Konversi Nilai Bit-Plane 7.....	22

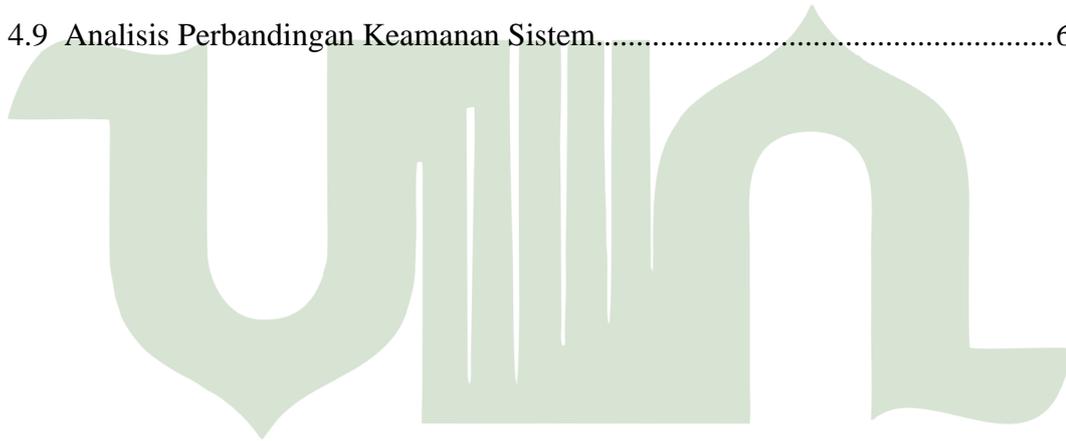
2.93	Bit-plane 0 Sebelum Penyisipan .....	24
2.94	Bit-plane 0 Setelah Penyisipan .....	26
3.1	Kerangka Penelitian .....	29
3.2	Flowchart Proses Enkripsi dan Dekripsi AES .....	31
3.3	Flowchart Proses Penyisipan dengan Steganografi BPCS .....	33
4.3.1	Hasil Dekripsi File TXT.....	39
4.3.2	Hasil Dekripsi File PDF .....	39
4.3.3	Hasil Dekripsi File DOCX .....	40
4.1	Tampilan Kompleksitas .....	40
4.5.1	Tampilan Penyisipan File TXT.....	41
4.5.2	Tampilan Penyisipan File PDF.....	42
4.5.3	Tampilan Penyisipan File DOCX.....	42
4.6.1	Hasil Penyisipan File TXT.....	43
4.6.2	Hasil Penyisipan File PDF .....	44
4.6.3	Hasil Penyisipan File DOCX .....	44
4.8	Perbandingan Waktu Eksekusi Proses .....	56
4.9	Analisis Perbandingan Keamanan Sistem.....	61



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## DAFTAR TABEL

<b>Tabel</b>	<b>Judul Tabel</b>	<b>Halaman</b>
2.1	Konversi Nilai Biner .....	20
3.1	Jadwal Pelaksanaan Penelitian .....	35
3.2	Rencana Penerbitan Rumah Jurnal.....	35
4.1	Kompleksitas Bit-Plane .....	45
4.2	Proses Penyisipan.....	47
4.3	Ekstraksi Pesan .....	50
4.4	<i>Black Box Testing</i> .....	52
4.5	Waktu Enkripsi.....	54
4.6	Waktu Dekripsi .....	55
4.7	Waktu Penyisipan Pesan .....	55
4.8	Waktu Ekstraksi Pesan.....	56
4.9	Analisis Perbandingan Keamanan Sistem.....	60



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN

## DAFTAR LAMPIRAN

Lampiran	Judul Lampiran
1	Hasil Enkripsi File PDF
2	Hasil Enkripsi File DOCX
3	<i>Logbook</i>
4	LOA
5	Jurnal
6	Daftar Riwayat Penulis (CV)
7	Kartu Bimbingan



UNIVERSITAS ISLAM NEGERI  
SUMATERA UTARA MEDAN