

**PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW
DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI
GENERATOR ACAK PADA STEGANOGRAFI LSB**

SKRIPSI

Oleh:

**DELWIN
NIM. 221110202
ALEX ANDER WIJAYA
NIM. 221110286**



**PROGRAM STUDI S-1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2026**

**SECURITY IMPLEMENTATION USING LZW COMPRESSION AND
AES-256-GCM ENCRYPTION WITH ASCON-XOF128 AS A
RANDOM GENERATOR IN LSB STEGANOGRAPHY**

UNDERGRADUATE THESIS

By:

**DELWIN
ID NUMBER. 221110202
ALEX ANDER WIJAYA
ID NUMBER. 221110286**



**UNDERGRADUATE PROGRAM OF COMPUTER SCIENCE
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN
2026**

LEMBARAN PENGESAHAN

**PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW
DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI
GENERATOR ACAK PADA STEGANOGRAFI LSB**

SKRIPSI

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana
Program Studi S-1 Teknik Informatika

Oleh:

ALEX ANDER WIJAYA

NIM. 221110286

DELWIN

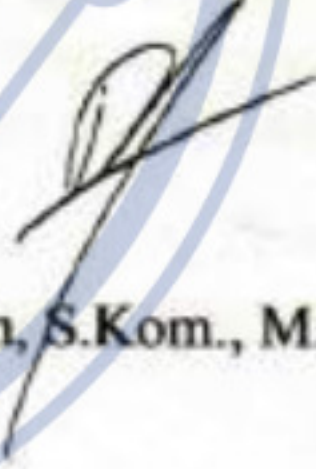
NIM. 221110202

Disetujui Oleh:

Dosen Pembimbing I,


Sunario Megawan, S.Kom., M.Kom.

Dosen Pembimbing II,


Darwin, S.Kom., M.Kom.

Medan, 30 Juni 2026

Diketahui dan Disahkan Oleh:

Ketua Program Studi

S-1 Teknik Informatika,


Carles Juliandy, S.Kom., M. Kom.

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Delwin
NIM : 221110202

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

Judul Skripsi : PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI GENERATOR ACAK PADA STEGANOGRAFI LSB

Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 30 Juli 2026

Saya yang membuat pernyataan,



Delwin

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Alex Ander Wijaya

NIM : 221110286

Saya telah melaksanakan penelitian dan penulisan Skripsi dengan judul dan tempat penelitian sebagai berikut:

Judul Skripsi : PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI GENERATOR ACAK PADA STEGANOGRAFI LSB

Tempat Penelitian : -

Alamat Tempat Penelitian : -

No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Skripsi saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Skripsi saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 30 Juli 2026

membuat pernyataan,



Alex Ander Wijaya

PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI GENERATOR ACAK PADA STEGANOGRAFI LSB

Abstrak

Steganografi berbasis Least Significant Bit (LSB) banyak digunakan untuk menyembunyikan informasi rahasia karena mampu mempertahankan kualitas visual citra. Namun, metode LSB konvensional masih memiliki keterbatasan pada kapasitas penyisipan, keamanan data, serta pola penyisipan yang relatif mudah dideteksi melalui steganalisis statistik. Penelitian ini bertujuan mengembangkan model steganografi hibrida dengan mengintegrasikan kompresi Lempel-Ziv-Welch (LZW), enkripsi AES-256-GCM, dan Ascon-XOF128 sebagai generator bilangan acak kriptografis untuk menentukan pola penyisipan pada metode LSB. Penelitian dilakukan melalui tahapan analisis, perancangan, implementasi, dan pengujian menggunakan citra RGB 24-bit berformat BMP atau PNG. Hasil penelitian menunjukkan bahwa algoritma LZW menghasilkan rasio kompresi rata-rata sebesar 51,943%, sedangkan kualitas stego-image tetap terjaga dengan nilai rata-rata MSE sebesar 2,563, PSNR sebesar 45,6629 dB, dan SSIM sebesar 0,9887. Pengujian Bit Flipping Attack membuktikan bahwa perubahan sekecil apa pun pada Ciphertext menyebabkan proses dekripsi gagal sehingga integritas data tetap terjamin, sementara pengujian Chi-Square menunjukkan metode memiliki ketahanan yang baik terhadap steganalisis pada sebagian besar citra uji. Dengan demikian, integrasi LZW, AES-256-GCM, dan Ascon-XOF128 berhasil meningkatkan kapasitas penyisipan, mempertahankan kualitas visual citra, serta memperkuat keamanan dan integritas data pada steganografi LSB.

Kata kunci: *Steganografi LSB, Kompresi LZW, AES-256-GCM, Ascon-XOF128, Keamanan Data.*

Abstract

Least Significant Bit (LSB)-based steganography is widely used to conceal confidential information due to its ability to maintain the visual quality of the image. However, conventional LSB methods still suffer from limitations regarding embedding capacity, data security, and embedding patterns that are relatively easy to detect through statistical steganalysis. This study aims to develop a hybrid steganography model by integrating Lempel-Ziv-Welch (LZW) compression, AES-256-GCM encryption, and Ascon-XOF128 as a cryptographic random number generator to determine the embedding pattern within the LSB method. The research was conducted through the stages of analysis, design, implementation, and testing using 24-bit RGB images in BMP or PNG formats. The results show that the LZW algorithm yields an average compression ratio of 51.943%, while the stego-image quality is preserved with an average MSE of 2.563, PSNR of 45.6629 dB, and SSIM of 0.9887. Bit Flipping Attack testing proves that even the slightest alteration to the Ciphertext causes the decryption process to fail, thereby ensuring data integrity, while Chi-Square testing indicates that the method possesses good resistance against steganalysis on most test images. Consequently, the integration of LZW, AES-256-GCM, and Ascon-XOF128 successfully enhances embedding capacity, maintains image visual quality, and strengthens data security and integrity in LSB steganography.

Keywords: *LSB Steganography, LZW Compression, AES-256-GCM, Ascon-XOF128, Data Security.*

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul "PENERAPAN KEAMANAN MENGGUNAKAN KOMPRESI LZW DAN ENKRIPSI AES-256-GCM DENGAN ASCON-XOF128 SEBAGAI GENERATOR ACAK PADA STEGANOGRAFI LSB".

Tugas Akhir ini disusun sebagai bagian dari persyaratan kurikulum pada Program Studi S-1 Teknik Informatika, Universitas Mikroskil Medan.

Penulis juga menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Sunario Megawan, S.Kom., M.Kom, selaku Dosen Pembimbing I.
2. Bapak Darwin, S.Kom., M.Kom, selaku Dosen Pembimbing II.
3. Bapak Hardy, S.Kom., M.Sc., Ph.D, selaku Rektor Universitas Mikroskil Medan.
4. Bapak Sunaryo Winardi, S.Kom., M.T selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
5. Bapak Carles Juliandy, S.Kom., M.Kom, selaku Ketua Program Studi S-1 Teknik Informatika Fakultas Informatika Universitas Mikroskil Medan.
6. Bapak dan Ibu Dosen Universitas Mikroskil yang telah memberikan ilmunya selama penulis menempuh pendidikan.
7. Orang tua dan keluarga yang senantiasa memberikan dukungan moral dan materil sepanjang masa studi hingga Tugas Akhir ini terselesaikan
8. Rekan-rekan serta semua pihak yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan bantuan dan dukungan selama proses penyusunan Tugas Akhir ini.

Disadari sepenuhnya bahwa Tugas Akhir ini masih memiliki berbagai kekurangan. Penulis sangat terbuka menerima kritik maupun saran yang konstruktif untuk perbaikan dan pengembangan ke depan. Semoga karya ini dapat memberikan wawasan baru yang bermanfaat bagi pembaca serta mendukung perkembangan teknologi informasi, khususnya dalam ranah steganografi dan keamanan data.

Medan, 30 Juni 2026

Penulis,

Alex Ander Wijaya

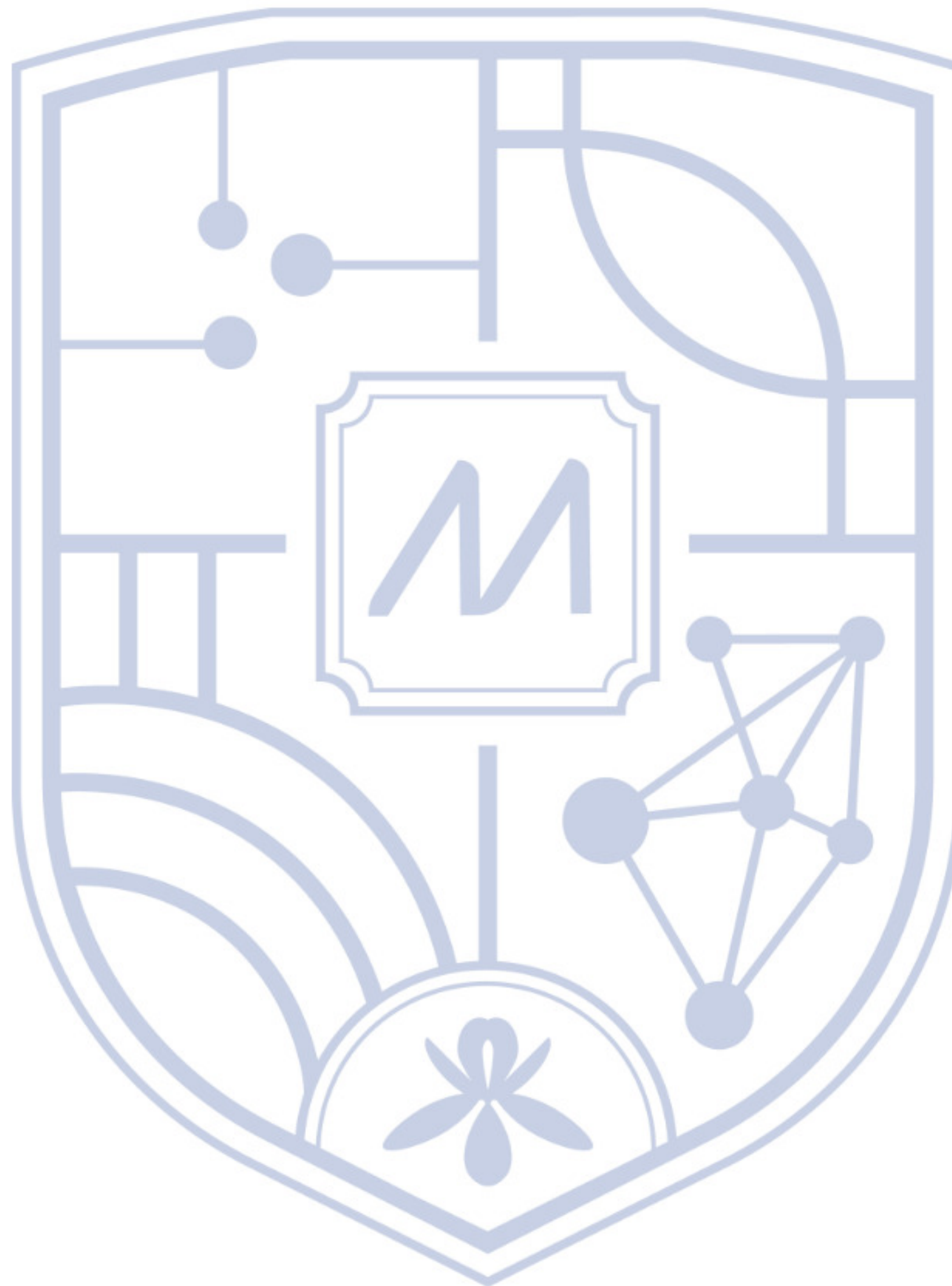
Delwin

DAFTAR ISI

Abstrak	i
KATA PENGANTAR	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	ix
DAFTAR LAMPIRAN	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan	2
1.4 Manfaat	3
1.5 Ruang Lingkup	3
BAB II KAJIAN LITERATUR.....	4
2.1 Kriptografi	4
2.2 Advanced Encryption Standard (AES)	6
2.3 Galois/Counter Mode (GCM).....	11
2.4 AES 256 GCM.....	13
2.5 Steganografi	15
2.6 Least Significant Bit (LSB)	17
2.7 Bilangan Acak.....	18
2.8 Ascon XO128	19
2.9 Citra	22
2.10 Mean Square Error (MSE)	25
2.11 Peak Signal-to-Noise Ratio (PSNR)	26
2.12 Structural Similarity Index Method (SSIM)	26
2.13 Chi-Square	27

2.14 Lempel Ziv Welch (LZW)	28
BAB III TAHAPAN PELAKSANAAN	29
3.1 Analisis	31
3.1.1 Analisis Proses	31
3.1.2 Analisis Kebutuhan	75
3.2 Perancangan Sistem	81
3.2.1 Rancangan <i>Form</i> Halaman Utama	82
3.2.2 Rancangan <i>Form</i> Penyisipan Pesan	83
3.2.3 Rancangan <i>Form</i> Ekstraksi Pesan	85
3.2.4 Rancangan <i>Form</i> Pengujian MSE dan PSNR	88
3.2.5 Rancangan <i>Form</i> Pengujian SSIM	89
3.2.6 Rancangan <i>Form</i> Pengujian Chi-Square	91
3.2.7 Rancangan <i>Form</i> Tentang Kami	92
BAB IV HASIL DAN PEMBAHASAN	94
4.1 Hasil	94
4.1.1 Menu Penyisipan	94
4.1.2 Menu Ekstraksi	97
4.1.3 Menu Pengujian MSE & PSNR	98
4.1.4 Menu Pengujian SSIM	100
4.1.5 Menu Pengujian Chi Square	102
4.2 Pembahasan	104
4.2.1 Pengujian Waktu Eksekusi Berdasarkan Ukuran Data	105
4.2.2 Uji MSE Dan PSNR	108
4.2.3 Uji SSIM	109
4.2.4 Uji <i>Chi-Square</i>	111
4.2.5 Simulasi Bit Flipping Attack pada <i>Payload</i> Stego-Image	113
BAB V PENUTUP	115

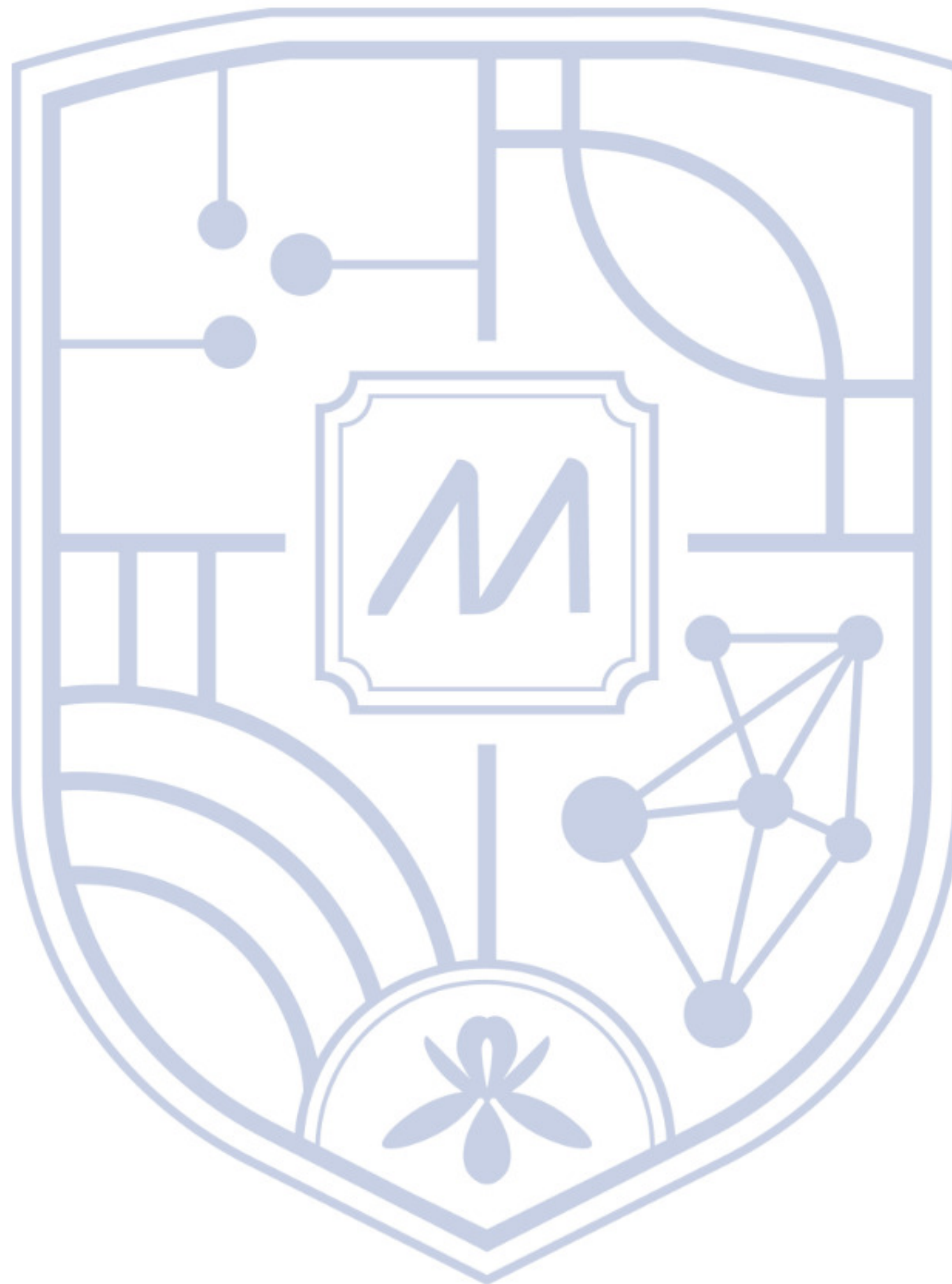
5.1 Kesimpulan	115
5.2 Saran	116
DAFTAR PUSTAKA	117
DAFTAR RIWAYAT HIDUP.....	120



DAFTAR GAMBAR

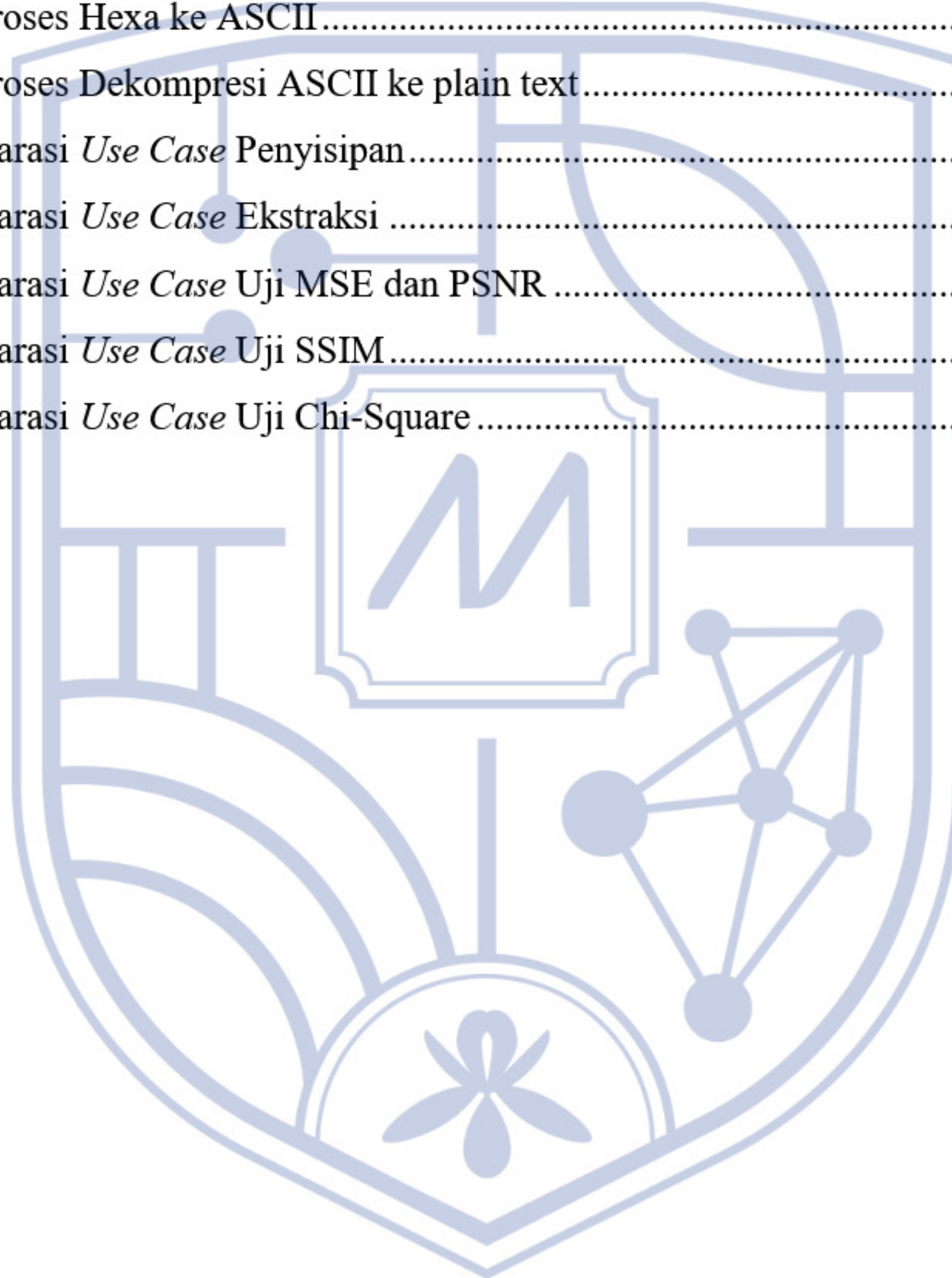
Gambar 2. 1 Enkripsi dan Dekripsi [10].....	4
Gambar 2. 2 Algoritma Simetris [10].....	5
Gambar 2. 3 Algoritma Asimetris [10].....	6
Gambar 2. 4 Penerapan SubBytes() S-box untuk byte pada state [13].....	9
Gambar 2. 5 Penggeseran secara cyclic ShiftRows tiga baris terakhir dalam state [13].....	10
Gambar 2. 6 Ilustrasi MixColumns [13].....	11
Gambar 2. 7 Ilustrasi AddRoundKey [13]	11
Gambar 2. 8 Diagram blok enkripsi terautentikasi GCM [14].....	12
Gambar 2. 9 Alur steganografi	15
Gambar 2. 10 Perbandingan citra sebelum dan sesudah menggunakan metode LSB [5] ...	17
Gambar 2. 11 Constant Addition Layer [8].....	20
Gambar 2. 12 Application of substitution layer ps to Ascon State [8].....	20
Gambar 2. 13 Circuit representation of the 5-bit S-box SBox [8].....	20
Gambar 2. 14 Lookup table representation of SBox [8].....	21
Gambar 2. 15 Application of linear diffusion layer pl to Ascon state [8].....	21
Gambar 2. 16 Contoh Citra Biner [21]	23
Gambar 2. 17 Contoh Citra Keabuan [2].....	24
Gambar 2. 18 Contoh Citra Berwarna [1]	24
Gambar 3. 1 <i>Flowchart</i> Proses <i>Embedding</i>	32
Gambar 3. 2 <i>Flowchart</i> Kompresi LZW	33
Gambar 3. 3 <i>Flowchart</i> Enkripsi AES-256-GCM.....	38
Gambar 3.4 <i>Flowchart</i> Ascon XOF128	50
Gambar 3. 5 <i>Flowchart</i> Penyisipan menggunakan Metode LSB	57
Gambar 3. 6 <i>Flowchart</i> Proses Ekstraksi	62
Gambar 3. 7 Flowchart Mekanisme Pengambilan Payload Menggunakan <i>Ascon XOF128</i>	63
Gambar 3. 8 <i>Flowchart</i> Dekripsi AES-256-GCM	67
Gambar 3. 9 <i>Flowchart</i> Dekompresi LZW	70
Gambar 3. 10 Simbol ASCII	72
Gambar 3. 11 <i>Use Case Diagram</i> Aplikasi	77
Gambar 3. 12 Gambar Halaman Utama	82
Gambar 3. 13 <i>Form</i> Penyisipan Pesan.....	83
Gambar 3. 14 <i>Form</i> Pilih Gambar	84

Gambar 3. 15 <i>Form</i> Pesan Kesalahan Kunci.....	85
Gambar 3. 16 <i>Form</i> Informasi Kapasitas Citra	85
Gambar 3. 17 Tampilan Informasi Proses Penyisipan Berhasil	85
Gambar 3. 18 <i>Form</i> Ekstraksi Pesan	86
Gambar 3. 19 <i>Form</i> Pilih Gambar	87
Gambar 3. 20 <i>Form</i> Pesan Kesalahan Kunci.....	87
Gambar 3. 21 Tampilan Informasi Proses Penyisipan Berhasil	88
Gambar 3. 22 <i>Form</i> Pengujian MSE & PSNR.....	88
Gambar 3. 23 Tampilan Informasi Pengujian MSE dan PSNR Berhasil	89
Gambar 3. 24 <i>Form</i> Pengujian SSIM	90
Gambar 3. 25 Tampilan Informasi Pengujian SSIM Berhasil.....	91
Gambar 3. 26 <i>Form</i> Pengujian Chi-Square	91
Gambar 3. 27 Tampilan Informasi Pengujian Chi-Square Berhasil.....	92
Gambar 3. 28 <i>Form</i> Tentang Kami	93
Gambar 4. 1 Halaman Menu Utama.....	94
Gambar 4. 2 <i>Form</i> penyisipan yang diisi cover image,pesan rahasia kunci	95
Gambar 4. 3 Umpan balik proses berhasil.....	95
Gambar 4. 4 Umpan balik jika pesan lebih besar dari citra.....	96
Gambar 4.5 Penyimpanan Log Excel.....	96
Gambar 4. 6 <i>Form</i> Ekstraksi pesan yang berisi kunci dan stego image.....	97
Gambar 4. 7 Umpan balik Ekstraksi berhasil.....	98
Gambar 4. 8 Hasil ekstraksi pesan.....	98
Gambar 4. 9 <i>Form</i> Pengujian MSE & PSNR yang berisi citra	99
Gambar 4. 10 Umpan balik Proses Pengujian berhasil	99
Gambar 4. 11 Hasil dari proses pengujian MSE & PSNR	100
Gambar 4. 12 <i>Form</i> Pengujian SSIM berisi citra gambar	101
Gambar 4. 13 Umpan balik proses pengujian berhasil.....	101
Gambar 4. 14 Hasil Pengujian SSIM.....	102
Gambar 4. 15 <i>Form</i> Pengujian Chi-Square berisi citra	103
Gambar 4. 16 Umpan balik Proses berhasil	103
Gambar 4. 17 Proses Pengujian Chi-Square Berhasil	104
Gambar 4. 18 <i>Form</i> Penyisipan Pesan.....	106
Gambar 4. 19 <i>Form</i> Pengujian MSE dan PSNR.....	108
Gambar 4. 20 <i>Form</i> Pengujian SSIM	110



DAFTAR TABEL

Table 2. 1 Kombinasi <i>Key</i> Block Round [10]	6
Table 2. 2 Indeks byte dan bit [10]	7
Table 2. 3 S-Box pada AES [13]	9
Table 3. 1 Penambahan Kamus baru	34
Table 3. 2 Konversi ASCII ke Hexadecimal	34
Table 3. 3 Proses Hexa ke ASCII	72
Table 3. 4 Proses Dekompresi ASCII ke plain text	73
Table 3. 5 Narasi <i>Use Case</i> Penyisipan	77
Table 3. 6 Narasi <i>Use Case</i> Ekstraksi	78
Table 3. 7 Narasi <i>Use Case</i> Uji MSE dan PSNR	79
Table 3. 8 Narasi <i>Use Case</i> Uji SSIM	79
Table 3. 9 Narasi <i>Use Case</i> Uji Chi-Square	80



DAFTAR LAMPIRAN

Lampiran 1 Link	119
-----------------------	-----

