PENGAMANAN PESAN
DENGAN METODE STEGANOGRAFI BERBASIS
CONVOLUTIONAL NEURAL NETWORK

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh :

Arya Difo Hasmi
NIM : 09021181823016

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN SKRIPSI

PENGAMANAN PESAN
DENGAN METODE STEGANOGRAFI BERBASIS
CONVOLUTIONAL NEURAL NETWORK

Oleh:

Arya Difo Hasmi
NIM: 09021181823016

Palembang, 13 Januari 2023

Pembimbing I

Al Farissi, S.Kom.,M.Comp.Sc
NIP. 19851215201404001

Pembimbing II,

Osvari Arsalan,S.Kom., M.T.
NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Rabu tanggal 04 Januari 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Arya Difo Hasmi
NIM : 09021181823016
Judul : Pengamanan Pesan Dengan Metode Steganografi Berbasis *Convolutional Neural Network*

dan dinyatakan **LULUS**.

1. Ketua

   Rizki Kurniati, M.T ....
   NIP. 199107122019032016

2. Penguji I

   Mastura Diana Marieska, M.T. .....
   NIP. 198603212018032001

3. Pembimbing I

   Al Farissi, S.Kom.,M.Comp.Sc .....
   NIP. 19851215201404001

4. Pembimbing II

   Osvari Arsalan,S.Kom., M.T. .....
   NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Arya Difo Hasmi
NIM	: 09021181823016
Program Studi	: Teknik Informatika Reguler
Judul	: Pengamanan Pesan Dengan Metode Steganografi Berbasis *Convolutional Neural Network*

Hasil pengecekan *Software iThenticate/Turnitin* : 15%

Menyatakan bahwa Laporan Skripsi saya merupakan hasil karya saya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam Laporan Skripsi ini, maka saya bersedia menerima sanksi dari Akademik Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 13 Januari 2023

Arya Difo Hasmi

NIM. 09021181823016

Motto:

- *Security and convenience are inversely proportional!*
- *If you scared to do it, just do it scared!*

Kupersembahkan karya ini kepada:

- Allah SWT
- Orang Tua dan Keluarga
- Teman Seperjuangan

Secure the Secret Messages Using
Convolutional Neural Network-Based Image Steganography

By:
Arya Difo Hasmi (09021181823016)
Departement of Informatics, Faculty of Computer Science, Sriwijaya University
Email: haryadiifo@gmail.com

ABSTRACT

Image steganography is implemented in order to maintain the confidentiality and security of information so that it is not easily accessed by unauthorized parties and prevent from cyber security incidents. This research aims to build a system that can embed secret image in RGB format into a carrier image in RGB format. This system uses the Convolutional Neural Network (CNN) method by comparing two architectural configurations, such as 16 convolution layers and 4 concatenation function with 30 convolution layers and 5 concatenation function at the CNNEncoder class. The dataset used is CIFAR10 with 5000 training data, 500 testing data and trained as much as 500 epochs. After the comparison is complete, the best architecture is produced by the second network configuration with an average MSE Loss of 0.5, an average PSNR cover image and payload of 41.3 dB and 28.0 dB without compromising the stego image's quality and integrity of the embedded information.

Keywords*: Steganography, Security, Configuration, CNN*

Pengamanan Pesan Dengan Metode Steganografi
Berbasis *Convolutional Neural Network*

Oleh:
Arya Difo Hasmi (09021181823016)
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: haryadiifo@gmail.com

Abstraksi

Steganografi citra diimplementasikan demi menjaga kerahasiaan dan keamanan informasi agar tidak mudah diakses oleh pihak yang tidak berwenang serta mencegah terjadinya insiden keamanan siber. Penelitian ini bertujuan untuk membangun sistem yang dapat menyisipkan citra rahasia berformat RGB kedalam suatu citra pembawa berformat RGB. Sistem ini menggunakan metode *Convolutional Neural Network* (CNN) dengan membandingkan dua konfigurasi arsitektur, yaitu 16 *convolution layer* dan 4 fungsi *concatenation* dengan 30 *convolution layer* dan 5 fungsi *concatenation* pada kelas *CNNEncoder*. Dataset yang digunakan adalah CIFAR10 dengan 5000 *data training* dan 500 *data testing* sebanyak 500 *epoch*. Setelah perbandingan selesai dilakukan, arsitektur terbaik dihasilkan oleh jaringan konfigurasi kedua dengan nilai rata-rata MSE *Loss* sebesar 0,5, rata-rata nilai PSNR citra pembawa dan rahasia sebesar 41,3 dB dan 28,0 dB tanpa mengurangi kualitas citra pembawa dan integritas dari informasi yang disisipkan.

Kata kunci: Steganografi, Keamanan, Konfigurasi, CNN

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT, karena rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir dalam menyelesaikan studi untuk mendapatkan gelar sarjana pada jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya dengan judul skripsi "Pengamanan Pesan Dengan Metode Steganografi Berbasis *Convolutional Neural Network* ".

Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan skripsi ini diantaranya :

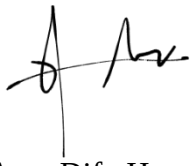
1. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Ibu Alvi Syahrini Utami, S.Si, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Al Farissi, S.Kom., M.Comp.Sc. selaku Pembimbing 1 yang telah meluangkan waktu, tenaga, dan pemikirannya dalam membimbing penulis sehingga dapat menyelesaikan skripsi ini.
4. Bapak Osvari Arsalan, S.Kom., M.T. selaku Pembimbing 2 yang telah membantu, membimbing dalam pembuatan skripsi dan perangkat lunak sehingga penulis dapat menyelesaikan skripsi ini.
5. Bapak M. Fachrurrozi, S.Si., M.T selaku Pembimbing Akademik yang telah membantu dan membimbing penulis selama perkuliahan di Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak dan Ibu dosen Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan penulis ilmu dan mengajar penulis berbagai macam mata kuliah yang bermanfaat selama masa perkuliahan.
7. Abdul Aziz Subayu dan Muhammad Rizal selaku pembimbing program MBKM *Network Security Operation Center (Cyber Blue Team)* dari PT. Mitra Integrasi Informatika yang telah memberikan ilmu yang sangat bermanfaat mengenai *Cyber Security*.

8. Teman-teman perkuliahan di Universitas Sriwijaya yang telah menemani penulis selama perkuliahan dan memberikan masa perkuliahan yang menyenangkan.
9. Terakhir teman-teman seperjuangan dalam melakukan perkuliahan, penelitian, dan penulisan Skripsi yaitu Eka Triani, Pretty Fujianti, Ditya Salsabila, Ferza Reyaldi, Muhammad Febriansyah, Della Octa, Suna Alkayuni, Nur Annisa, Cindy Steffani, Wahyu Ramadhani, Argha Novan, Ednagea Almira, Adi Kurniawan, dan Roni Starko.

Dalam penyusunan laporan ini, penulis menyadari masih banyak kekurangan baik dari segi susunan serta cara penulisan laporan ini, karenanya saran dan kritik yang sifatnya membangun demi kesempurnaan laporan ini sangat penulis harapkan. Akhirnya, semoga laporan ini bisa bermanfaat bagi para pembaca pada umumnya dan juga bermanfaat bagi penyusun pada khususnya.

Palembang, 13 Januari 2023

Penulis,



Arya Difo Hasmi

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN SKRIPSI ii
TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI iii
HALAMAN PERNYATAAN iv
HALAMAN MOTO DAN PERSEMBAHAN v
ABSTRACT vi
ABSTRAKSI vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR GAMBAR xiii
DAFTAR TABEL xv
DAFTAR ISTILAH xvi

BAB I PENDAHULUAN I-1
1.1 Pendahuluan I-1
1.2 Latar Belakang I-1
1.3 Rumusan Masalah I-4
1.4 Tujuan Penelitian I-4
1.5 Manfaat Penelitian I-4
1.6 Batasan Penelitian I-5
1.7 Sistematika Penulisan I-5
1.8 Kesimpulan I-6

BAB II KAJIAN LITERATUR II-1
2.1 Pendahuluan II-1
2.2 Landasan Teori II-1
2.2.1 Kriptografi II-1
2.2.2 Citra RGB II-2
2.2.3 Steganografi II-3

2.2.4 *Convolutional Neural Network* (CNN) II-4
2.2.5 *Mean Square Error* (MSE) II-8
2.2.6 *Peak Signal to Noise Ratio* (PSNR) II-8
2.2.7 *Rational Unified Process* (RUP) II-9
2.3 Penelitian Lain yang Relevan II-10
2.4 Kesimpulan II-13

BAB III METODOLOGI PENELITIAN III-1
3.1 Pendahuluan III-1
3.2 Pengumpulan Data III-1
3.2.1 Jenis Data III-1
3.2.2 Sumber Data III-1
3.2.3 *Sample* Gambar dari *Dataset* III-1
3.3 Tahapan Penelitian III-3
3.3.1 Alur Penelitian III-3
3.3.2 Kriteria Pengujian III-4
3.3.3 Format Data Pengujian III-4
3.3.4 Alat yang Digunakan dalam Pelaksanaan Penelitian III-5
3.3.5 Kerangka Kerja dan Pengujian Penelitian III-5
3.3.6 *Proposed Architecture* III-7
3.3.7 Analisis Hasil Pengujian dan Membuat Kesimpulan III-8
3.4 Metode Pengembangan Perangkat Lunak III-8
3.5 Manajemen Proyek Penelitian III-9

BAB IV PENGEMBANGAN PERANGKAT LUNAK IV-1
4.1 Pendahuluan IV-1
4.2 *Rational Unified Process* (RUP) IV-1
4.2.1 Fase Insepsi IV-1
4.2.2 Fase Elaborasi IV-5
4.2.3 Fase Konstruksi IV-12
4.2.4 Fase Transisi IV-17

4.3 Kesimpulan IV-18

BAB V HASIL DAN ANALISIS PENELITIAN V-1
5.1 Pendahuluan V-1
5.2 Hasil Percobaan / Penelitian V-1
5.2.1 Hasil Percobaan dan Kendala Konsep Penelitian V-1
5.2.2 Konfigurasi Percobaan V-7
5.2.3 Data Hasil *Training* dan *Testing* V-8
5.3 Analisis Penelitian V-18
5.4 Kesimpulan V-24

BAB VI KESIMPULAN DAN SARAN VI-1
6.1 Kesimpulan VI-1
6.2 Saran VI-1
DAFTAR PUSTAKA xvii
LAMPIRAN xx

DAFTAR GAMBAR

Halaman

Gambar II-1 Ruang Warna RGB II-3
Gambar II-2 Proses Steganografi.....II-3
Gambar II-3 Arsitektur *Convolutional Neural Network*.....II-4
Gambar II-4 *Convolutional Layer*.....II-5
Gambar II-5 Operasi pada *Pooling Layer*.....II-6
Gambar II-6 ReLU ……..……. II-7
Gambar II-7 *Fully-connected Layer*.....II-7
Gambar II-8 Fase RUP.....II-10
Gambar III-1 CIFAR10 *Dataset Sample* ……..…….. III-2
Gambar III-2 Kerangka Kerja Penelitian ……...……..... III-6
Gambar III-3 *Proposed Architecture* …….. III-7
Gambar III-4 *Rational Unified Process* (RUP) ……..……..... III-9
Gambar IV-1 Arsitektur CNN yang digunakan IV-4
Gambar IV-2 *Use Case Diagram* IV-5
Gambar IV-3 CNNStego *Website Sequence Diagram* ……..……. IV-9
Gambar IV-4 *Hide Message Sequence Diagram* …..……...……. IV-10
Gambar IV-5 *Hide Message Activity Diagram* ……..…….. IV-11
Gambar IV-6 Model CNN yang digunakan ……..……... IV-13
Gambar IV-7 CNNStego *Dashboard Web Interface* ……...……..…….. IV-14
Gambar IV-8 CNNStego *Help Page Web Interface* …….....……... IV-15
Gambar IV-9 CNNStego *About Page Web Interface* ……..……..... IV-15
Gambar IV-10 *Class Diagram* ……..……...…… IV-16
Gambar V-I Kode program konversi teks dan *image* ke *tensor* ..……..... V-2
Gambar V-2 Hasil konversi *image* ke *tensor* …….……..... V-2
Gambar V-3 Penambahan *padding* dan dimensi pada *tensor string* ……... V-3
Gambar V-4 Kode program konversi teks kedalam *array* 64x64 ….…….. V-4
Gambar V-5 Hasil konversi teks kedalam *array* 64x64 ……..……..... V-4

Gambar V-6 Pesan *error array* 64x64 …….…….... V-4
Gambar V-7 Algoritma konversi teks ke citra RGB …….…….. V-6
Gambar V-8 Konversi teks ke Citra RGB ……..…..…. V-7
Gambar V-9 Hasil penyisipan citra RGB menggunakan CNN ……...……. V-7
Gambar V-10 Perbandingan MSE *Loss* pada CNNStego Konfigurasi Pertama ……....V-19
Gambar V-11 Perbandingan PSNR *Cover Image* pada CNNStego Konfigurasi Pertama ……..……. V-19
Gambar V-12 Perbandingan PSNR *Payload* pada CNNStego Konfigurasi Pertama ……..……. V-19
Gambar V-13 Perbandingan *Test* PSNR pada CNNStego Konfigurasi Pertama ……... V-20
Gambar V-14 *Cover Image, Payload, Stego Image* dan *Decoded Payload* Pada CNNStego Konfigurasi Pertama …….…..…….. V-20
Gambar V-15 Perbandingan MSE *Loss* pada CNNStego Konfigurasi Kedua …….. V-21
Gambar V-16 Perbandingan PSNR *Cover Image* pada CNNStego Konfigurasi Kedua ……..... V-21
Gambar V-17 Perbandingan PSNR *Payload* pada CNNStego Konfigurasi Kedua ……..…..... V-22
Gambar V-18 Perbandingan *Test* PSNR pada CNNStego Konfigurasi Kedua …….. V-22
Gambar V-19 *Cover Image, Payload, Stego Image* dan *Decoded Payload* Pada CNNStego Konfigurasi Kedua ……..……. V-22

DAFTAR TABEL

Halaman

Tabel III-1 Format Tabel Pengujian Kualitas Citra Pembawa ……..…….. III-4
Tabel III-2 Format Tabel Pengujian Kualitas *Payload* ……... III-4
Tabel III-3 Format Tabel Perbandingan Konfigurasi CNN ……... III-4
Tabel III-4 Manajemen Proyek Penelitian ……..…….....…..... III-10
Tabel IV-1 Kebutuhan Fungsional ……..……..... IV-2
Tabel IV-2 Kebutuhan Non-Fungsional ……...……..……. IV-2
Tabel IV-3 Tabel Defenisi Aktor ……...…….. IV-6
Tabel IV-4 Tabel Defenisi *Use Case* …...……...……. IV-6
Tabel IV-5 Tabel Skenario *Use Case Input Cover Image and Secret Image* .. IV-7
Tabel IV-6 Tabel Skenario *Use Case Hide Message* ……..….... IV-8
Tabel IV-7 Implementasi Kelas ……...….. IV-16
Tabel IV-8 Rencana Pengujian ……...….... IV-17
Tabel IV-9 Implementasi dari Rencana Pengujian …..……...….... IV-18
Tabel V-1 Konversi Pesan Menggunakan *Library text-to-image* ……..…….. V-5
Tabel V-2 Tabel Pengujian Kualitas Citra Pembawa ……...…… V-9
Tabel V-3 Tabel Pengujian Kualitas *Payload* ……..……...….... V-11
Tabel V-4 Tabel Pengujian Kualitas Citra Pembawa Konfigurasi Kedua V-14
Tabel V-5 Tabel Pengujian Kualitas *Payload* Konfigurasi Kedua ……..….. V-16
Tabel V-6 Tabel Representasi Perbandingan Kedua Konfigurasi ……..…… V-23

DAFTAR ISTILAH

CNN	:	*Convolutional Neural Network*
RAM	:	*Random Access Memory*
CPU	:	*Central Processing Unit*
RUP	:	*Rational Unified Process*
ReLU	:	*Rectified Linear Unit*
MSE	:	*Mean Square Error*
PSNR	:	*Peak Signal-to-Noise Ratio*
LSB	:	*Least Significant Bit*

BAB I
PENDAHULUAN

1.1 Pendahuluan

Pada bab pendahuluan akan dijelaskan latar belakang, rumusan masalah, tujuan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

1.2 Latar Belakang

Internet menjadi salah satu media komunikasi yang perkembangannya paling pesat didunia karena kemudahan dan teknologi yang ditawarkan. Proses komunikasi data terjadi saat pengguna internet berbagi data dan informasi melalui sistem berbasis *website*, aplikasi, dan komputasi awan. Dengan adanya teknologi tersebut, individu dan organisasi diizinkan untuk menyimpan, memproses, mengakses, dan bertukar data. Sayangnya dengan berkembangnya teknologi, kejahatan di dunia digital semakin meningkat. Berbagai teknik diimplementasikan untuk mengakses informasi yang bukan haknya. Selain itu, beberapa informasi yang tersebar di internet juga tidak bersifat umum, artinya informasi tersebut hanya boleh diketahui oleh satu atau sekelompok orang tertentu. Penyebaran informasi yang bersifat rahasia harus dilakukan secara hati-hati agar informasi tersebut tidak diterima oleh pihak ketiga. Oleh karena itu muncul kebutuhan pengembangan mekanisme dan teknologi baru untuk melindungi data dari pencurian dan penyadapan oleh pihak yang tidak berwenang (Reinel et al, 2021).

Kriptografi dan Steganografi merupakan dua solusi yang dapat digunakan untuk menjaga kerahasiaan dan integritas suatu informasi saat ditransmisikan dari

pengirim kepada penerima pesan. Dalam Kriptografi, algoritma enkripsi tertentu digunakan agar data tidak dapat dipahami oleh orang yang tidak berwenang, namun tetap menarik perhatian *attacker* yang memunculkan kemungkinan data dapat diretas. Dalam Steganografi, informasi rahasia disisipkan pada suatu media pembawa (*cover media*) agar tidak terdeteksi dan tidak menimbulkan kecurigaan pihak ketiga. Media pembawa dan informasi rahasia yang dapat digunakan adalah foto, video, audio, dan teks. Namun, citra *grayscale*, berwarna (RGB/CMYK), dan Bitmap sering digunakan sebagai citra pembawa dalam penelitian Steganografi (Li et al, 2011).

Steganografi memiliki beberapa metode untuk menyisipkan informasi kedalam suatu media pembawa seperti *Least Significant Bit* (LSB). Metode ini memanfatkan nilai *channel* yang bekerja dengan memodifikasi nilai bit terakhir pada suatu citra pembawa secara seragam maupun adaptif untuk meminimalkan pergeseran warna citra pembawa dengan *stego image*. Teknik ini mudah untuk diimplementasikan dan tidak dapat dideteksi jika dilakukan analisis secara visual, namun tingkat keamanannya masih sangat kurang karena piksel-piksel citra pembawa yang dimodifikasi secara terpisah menyebabkan gangguan dalam distribusi LSB piksel *stego image*, sehingga membuat citra tersebut mudah dideteksi menggunakan serangan statistik. Sebagai alternatif, peneliti lain menyarankan untuk mencari citra pembawa yang berkualitas tinggi untuk piksel yang akan dimodifikasi sambil mempertahankan distribusi statistik citra dengan fokus di daerah tekstur, *edge*, dan *brightness* dibandingkan di daerah yang halus (R.J.Rasras, 2019).

Model Steganografi yang digunakan untuk penyisipan informasi dibutuhkan hasil yang sempurna saat mengekstraksi informasi (tanpa kesalahan) agar informasi yang diterima sesuai dengan aslinya. Dalam penelitian yang berjudul *Image Compression Via Auto-Encoding Networks Using* CNN, peneliti membangun arsitektur jaringan yang dibagi menjadi tiga bagian, yaitu *Prep Network* dan *Hidden Network* bertugas untuk menyisipkan *secret image* ke dalam citra pembawa sehingga ukuran dan warna dari *stego image* yang dihasilkan tampak semirip mungkin dengan citra pembawa, serta *Reveal Network* untuk mengekstraksi informasi yang disisipkan. Model yang dikembangkan memberikan kapasitas penyisipan sebesar 24 bpp. Jika dibandingkan dengan dengan metode LSB, umumnya menyematkan 1 bit pesan pada 1 piksel citra pembawa, sehingga jika semua piksel gambar disematkan ke 1 bit pesan maka menghasilkan nilai 1 bpp. Hasil ini membuktikan bahwa penggunaan metode *Deep Learning* dapat meningkatkan kapasitas penyisipan informasi pada citra pembawa (Baluja, 2017 & Setiadi, 2022).

Dalam penelitian ini, peneliti mengimplementasikan *Convolutional Neural Network* dalam proses Steganografi untuk menyisipkan suatu citra rahasia kedalam citra pembawa berformat RGB. Sasaran penelitian ini adalah membangun jaringan CNN dimana sistem harus belajar menyisipkan citra rahasia di berbagai bagian citra pembawa pada *hidden network*, menjamin kualitas *stego image* dan informasi yang diekstraksi serta kapasitas penyisipannya. CNN dikenal memiliki performa yang tinggi dalam pengolahan citra karena dapat mengurangi jumlah parameter dan tingkat komputasi selama pemrosesan tanpa mengurangi kualitas model atau

data yang digunakan, sehingga informasi yang diperoleh memiliki kualitas yang tinggi.

1.3 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Metode steganografi *Least Significant Bit* (LSB) memiliki pola penyisipan yang sederhana sehingga para *attacker* mudah untuk mendeteksi citra pembawa dan *payload* yang disisipkan, serta kapasitas penyisipan yang sangat terbatas.
2. Model CNN yang digunakan untuk steganografi citra pada penelitian sebelumnya terlalu kompleks sehingga dibutuhkan model yang sederhana dan dapat dihandalkan untuk menghindari insiden keamanan digital.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Melakukan pengembangan perangkat lunak yang mengimplementasikan metode *Convolutional Neural Network* dalam proses Steganografi citra.
2. Melakukan perhitungan terhadap aspek kualitas citra pembawa dan rahasia yang meliputi perhitungan pada nilai *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR).

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Memberikan referensi kepada praktisi keamanan siber dalam menganalisis informasi yang disembunyikan pada citra dimana biasanya diterapkan oleh para pelaku kriminal atau *attacker* untuk menyerang suatu instansi,

organisasi atau perorangan.

2. Hasil penelitian juga dapat dipakai sebagai rujukan untuk penelitian-penelitian steganografi selanjutnya.

1.6 Batasan Penelitian

Adapun batasan masalah yang diberikan pada penelitian ini adalah sebagai berikut:

1. Citra pembawa dan rahasia merupakan citra RGB berekstensi (.jpeg).
2. Citra yang digunakan beresolusi 32x32 piksel.
3. Tidak mencakup keamanan saat proses distribusi *stego image*.

1.7 Sistematika Penulisan

Sistematika penulisan laporan ini berdasrkan standar penulisan laporan skripsi Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut:

BAB I. PENDAHULUAN

Pada bab pendahuluan akan dijelaskan latar belakang, rumusan masalah, tujuan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab kajian literatur akan dijelaskan teori dasar penelitian seperti Kriptografi, Citra Digital, Steganografi, *Steganalysis*, MSE, PSNR, *Convolutional Neural Network*, dan *Rational Unified Process*, serta penelitian lain yang relevan

BAB III. METODOLOGI PENELITIAN

Bab ini membahas langkah-langkah yang digunakan dalam penelitian. Setiap rencana tahapan penelitian dirinci dengan menggunakan

kerangka kerja, dilanjutkan dengan perencanaan manajemen proyek dalam melakukan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab pengembangan perangkat lunak meliputi arsitektur, diagram, implementasi CNN pada steganografi citra, dan hasil pengujian perangkat lunak.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab hasil dan analisis akan dijelaskan seluruh hasil penelitian dari bab sebelumnya kedalam bentuk tabel dan grafik serta menjadi dasar kesimpulan yang diambil pada penelitian.

BAB VI. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari semua uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan dapat berguna dalam penerapan CNN pada steganografi citra di masa mendatang.

1.8 Kesimpulan

Pada pendahuluan ini, telah dijelaskan secara umum mengenai penelitian yang akan dilakukan, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

DAFTAR PUSTAKA

Das, A., Wahi, J. S., Anand, M., & Rana, Y. (2021). *Multi-Image Steganography Using Deep Neural Networks*. http://arxiv.org/abs/2101.00350

Kumar, V., Laddha, S., Aniket, & Dogra, N. (2020). *Steganography Techniques Using Convolutional Neural Networks*. *Review of Computer Engineering Studies*, *7*(3), 66–73. https://doi.org/10.18280/rces.070304

Kich, I. (2020). *Image Steganography by Deep CNN Auto-Encoder Networks*. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(4), 4707 – 4716. https://doi.org/10.30534/ijatcse/2020/75942020

Sharifzadeh, M., Agarwal, C., Aloraini, M., & Schonfeld, D. (2017). *Convolutional Neural Network Steganalysis's Application to Steganography*. http://arxiv.org/abs/1711.02581

Bashkirova, D. (2016). *Convolutional Neural Networks for Image Steganalysis*. *BioNanoScience*, *6*(3), 246–248. https://doi.org/10.1007/s12668-016-0215-z

Qadir, A. M., & Varol, N. (2019, June 1). *A Review Paper On Cryptography*. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*. https://doi.org/10.1109/ISDFS.2019.8757514

Bao, Z., Luo, X., Zhang, Y., Yang, C., & Liu, F. (2018). *A Robust Image Steganography on Resisting JPEG Compression with No Side Information*.

IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India), *35*(sup1), 4–13. https://doi.org/10.1080/02564602.2018.1476192

Ren, W., Xu, Y., Zhai, L., Wang, L., & Jia, J. (2020). Issue 5 Article 9 2020 *Fast Carrier Selection of JPEG Steganography Appropriate for Application*. In *Tsinghua Science and Technology* (Vol. 25, Issue 05). https://tsinghuauniversitypress.researchcommons.org/tsinghua-

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). *Image Steganography: A Review of the Recent Advances*. *IEEE Access*, *9*, 23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998

Tan, S., & Li, B. (2014, February 12). *Stacked Convolutional Auto-Encoders For Steganalysis of Digital Images*. *2014 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2014*. https://doi.org/10.1109/APSIPA.2014.7041565

B. Li, J. He, J. Huang, and Y. Q. Shi, "*A Survey on Image Steganography and Steganalysis*," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142–172, 2011.

Al-Balqa' Applied University, Amman, Jordan and R. J. Rasras, "*Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography*," IJATCSE, vol. 8, no. 3, pp. 748–754, Jun. 2019, doi: 10.30534/ijatcse/2019/64832019.

S. Baluja, "*Hiding images in plain sight: Deep steganography*," *in Advances in Neural Information Processing Systems*, 2017, pp. 2069–2079

Couchot, J.-F., Couturier, R., Guyeux, C., & Salomon, M. (2016). *Steganalysis via a Convolutional Neural Network using Large Convolution Filters for Embedding Process with Same Stego Key*. http://arxiv.org/abs/1605.07946

Setiadi, D. R. I. M. (2022). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. *Journal of King Saud University - Computer and Information Sciences*, *34*(2), 104–114. https://doi.org/10.1016/j.jksuci.2019.12.007

Tang, W., Li, B., Tan, S., Barni, M., & Huang, J. (2018). *CNN Based Adversarial Embedding with Minimum Alteration for Image Steganography*. https://doi.org/10.1109/TIFS.2019.2891237

Maia, D., & Trindade, R. (2016). *Face Detection and Recognition in Color Images under Matlab. International Journal of Signal Processing, Image Processing and Pattern Recognition*, 9(2), 13–24. https://doi.org/10.14257/ijsip.2016.9.2.02