

**ANALISIS DAN PENGEMBANGAN METODE PADA TEKNIK
STEGANOGRAFI UNTUK MENGATASI
PERMASALAHAN MANIPULASI *ROBUSTNESS***

DISERTASI

Oleh

DEDI DARWIS



**PROGRAM DOKTOR MIPA
FAKULTAS MATEMATIKA & ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2021**

**ANALISIS DAN PENGEMBANGAN METODE PADA TEKNIK
STEGANOGRAFI UNTUK MENGATASI
PERMASALAHAN MANIPULASI *ROBUSTNESS***

Disertasi untuk memperoleh gelar Doktor
dalam Ilmu MIPA
pada Universitas Lampung

Dipertahankan di hadapan
Dewan Penguji Program Pascasarjana
Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung

Pada tanggal 14 Desember 2021

Oleh

DEDI DARWIS

Tempat dan Tanggal Lahir: Tanjung Bintang, 01 Januari 1988
Lulus Sarjana Komputer STMIK Teknokrat: 2012
Lulus Magister Ilmu Komputer Universitas Budi Luhur: 2015



**PROGRAM DOKTOR MIPA
FAKULTAS MATEMATIKA & ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2021**

Analisis dan Pengembangan Metode pada Teknik Steganografi untuk Mengatasi Permasalahan Manipulasi Robustness

Dipersiapkan dan disusun oleh:

DEDI DARWIS
NPM. 1737061013

Telah disetujui oleh

Prof. Dra. Wamiliana, M.A., Ph.D.

Promotor

Dr.rer.nat. Akmal Junaidi, M.Sc.

Ko-Promotor

Prof. Dr. La Zakaria, M.Sc.

Ko-Promotor

Dr. G. Nugroho Susanto, M.Sc.

Ketua Program Studi Doktor MIPA

Mengesahkan

Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Dr. Eng. Suripto Dwi Yuwono, M.T

NIP. 197407052000031001

Direktur Program Pascasarjana

Prof. Dr. Ahmad Saudi Samosir, S.T., M.T.

NIP. 197104151998031005

Analisis dan Pengembangan Metode pada Teknik Steganografi untuk Mengatasi Permasalahan Manipulasi *Robustness*

Dipersiapkan dan disusun oleh:

DEDI DARWIS

NPM. 1737061013

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 14 Desember 2021

Prof. Dra. Wamiliana, M.A., Ph.D.

Promotor

Dr. rer. nat. Akmal Junaidi, M.Sc.

Ko-Promotor

Prof. Dr. La Zakaria, M.Sc.

Ko-Promotor

Samsuryadi, M.Kom., Ph.D.

Penguji

Dr. Ir. Kurnia Muludi, M.S.Sc.

Penguji

Dr. Eng. Admi Syarif

Penguji

Dr. G. Nugroho Susanto, M.Sc.

Ketua Program Studi Doktor MIPA

Disertasi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Doktor MIPA pada tanggal: 14 Desember 2021

Mengesahkan

Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam



Dr. Eng. Suriplo Dwi Yuwono, M.T


NIP. 197407052000031001

PERNYATAAN ORISINALITAS DISERTASI

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya di dalam disertasi ini tidak terdapat karya ilmiah yang pernah diajukan untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam daftar pustaka.

Bandar Lampung,
Yang Menyatakan




DEDI DARWIS
NPM. 1737061013

PRAKATA

Segala puji hanya milik Allah Rob Seluruh Alam, Alhamdulillah dengan curahan Rahmat dan Karunia-Nya Disertasi yang berjudul “Analisis dan Pengembangan pada Teknik Steganografi untuk Mengatasi Permasalahan Manipulasi *Robustness*” dapat diselesaikan yang merupakan salah satu syarat untuk memperoleh gelar Doktor di Universitas Lampung.

Teriring Shalawat kepada Uswatun Hasanah bagi seluruh umat manusia di muka bumi “Muhammad S.A.W” semoga syafa’at beliau tercurah kepada keluarganya, para sahabatnya dan seluruh umat belai yang selalu konsisten berjalan menjaga dan menjalankan sunnahnya, Aamiin Yarobbal’alamin.

Pada kesempatan ini sebagai penulis mengucapkan terimakasih kepada:

1. Allah S.W.T yang selalu mencurahkan Rahmat dan KaruniaNa kepada penulis.
2. Rektor Universitas Lampung Bapak Prof. Dr. Karomani, M.Si. yang telah memberikan kesempatan bagi penulis untuk mendapatkan ilmu pengetahuan dan teknologi di Unila.
3. Dekan FMIPA Bapak Dr. Eng. Suropto Dwi Yuwono, M.T yang telah menyiapkan pasilitas untuk kelancaran pendidikan dan penelitian penulis di FMIPA Unila
4. Bapak Dr. HM. Nasrullah Yusuf, SE., MBA. Selaku Rektor Universitas Teknokrat Indonesia yang telah mendukung dan membantu penulis dalam hal pendanaan selama menyelesaikan kuliah program Doktor MIPA
5. Ibu Prof. Dra Wamiliana, MA., Ph.D. Selaku Promotor dan Dosen Pembimbing Akademik yang telah banyak memberikan bantuan, bimbingan, arahan dan saran dalam penyusunan Disertasi.

6. Bapak Dr.rer.nat. Akmal Junaidi, M.Sc. selaku Ko-Promotor I yang telah memberikan bimbingan, arahan dan saran dalam proses penyelesaian disertasi .
7. Bapak Prof. Dr. La Zakaria, M.Sc. selaku Ko-Promotor II yang telah banyak memberikan bantuan, saran dan bimbingan sampai selesainya disertasi dengan baik.
8. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc. selaku Penguji atas semua masukan dan saran sehingga disertasi ini lebih baik.
9. Bapak Dr. Eng. Admi Syarif selaku Penguji atas semua masukan dan saran sehingga disertasi ini lebih baik.
10. Bapak Samsuryadi, S.Si., M.Kom., Ph.D. selaku Penguji atas masukan dan sarannya untuk lebih baiknya disertasi ini.
11. Bapak Dr. G. Nugroho Susanto, M.Sc selaku ketua program studi Doktor MIPA atas bimbingan dan arahnya.
12. Ibu Dr. Khoirin Nisa, S.Si., M.Si. selaku Sekretaris Program Studi Doktor MIPA atas bantuan dan arahnya.
13. Seluruh sivitas akademika dari Unila dan Universitas Teknokrat Indonesia yang tidak dapat saya sebutkan satu persatu yang telah memberikan bantuan, semoga Allah membalas amal kebaikan kita semua.

Semoga disertasi ini dapat memberikan manfaat bagi kita semua dalam rangka pengembangan ilmu pengetahuan dan teknologi untuk masa depan, Aamiin.

Bandar Lampung, Desember 2021

DEDI DARWIS

DAFTAR RIWAYAT HIDUP

Nama : **Dedi Darwis**
 Tanggal Lahir : Tanjung Bintang, 01 Januari 1988
 Jabatan : Dosen di Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
 Pendidikan : D1 Komputer Akuntansi, LPBM Teknokrat Lampung
 D3 Komputerisasi Akuntansi, AMIK Teknokrat Lampung
 S1 Teknik Informatika, STMIK Teknokrat Lampung
 S2 Ilmu Komputer, Universitas Budi Luhur

Prestasi di Bidang Tri Dharma Perguruan Tinggi

1) Bidang Pendidikan:

- Perolehan *Certified Data Science Practitioner (CDSP)* dari *CertNexus*, New York, Amerika Serikat yang dibiayai oleh Kemendikbudristek pada tahun 2021

2) Perolehan Hibah Penelitian Kompetitif Nasional dari Kemendikbudristek selama lima tahun berturut-turut (2017 – 2021)

- A New Digital Image Steganography Based on Center Embedded Pixel Positioning (2021).
- Perbandingan Metode Discrete Wavelet Transform dan Singular Value Decomposition pada Steganografi untuk Mengukur Ketahanan Terhadap Gaussian Noise dan Peningkatan Keamanan Data (2020).
- Kombinasi Steganografi, Kriptografi dan Kompresi Data Sebagai Upaya untuk Peningkatan Keamanan Data (2018)
- Analisis Penentu Penerimaan Teknologi Sistem Basis Data Akuntansi (2017)
- Kombinasi Teknik Steganografi Least Significant Bit (LSB) dan Teknik Kompresi Lempel Ziv Welch (LZW) Untuk Pengamanan Data (2017)

3) Perolehan Hibah Pengabdian Masyarakat Kompetitif Nasional dari DRPM Kemenristek selama tiga tahun berturut-turut (2019 – 2021)

- Penerapan Smart School untuk Meningkatkan Produktivitas Guru dan Siswa di Era New Normal pada SMK YP Serdang Tanjung Bintang Kabupaten Lampung Selatan (2021).
- Penerapan IoT Kandang Sapi Modern untuk Meningkatkan Produktivitas Pertumbuhan Sapi bagi Kelompok Peternakan CV Sapi Sport Kecamatan Tanjung Bintang, Lampung Selatan (2021).
- Penerapan Sistem Pembelajaran Dalam Jaringan (SPADA) di SMK Yayasan Pemuda Indonesia Tanjung Bintang Kabupaten Lampung Selatan (2020)
- PKMS Pelatihan dan Pendampingan Pembuatan CD Pembelajaran Interaktif Menggunakan Auto Play Media Studio Untuk Guru SMA Bina Mulya Gading Rejo Kabupaten Pringsewu Provinsi Lampung (2019)
- PKMS Pelatihan dan Pendampingan Pembuatan Game Edukasi Untuk Guru SMP Muhammadiyah 1 Ambarawa Kabupaten Pringsewu(2019)

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN PROMOTOR	ii
HALAMAN PENGESAHAN PENGUJI	iii
PERNYATAAN	vi
PRAKATA	v
RIWAYAT HIDUP	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
ABSTRAK	xii
BAB I PENDAHULUAN	
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	5
1.3 Tujuan Penelitian.....	5
1.4 Manfaat Penelitian.....	5
1.5 Batasan Penelitian	5
1.6 Kebaruan Penelitian (<i>Novelty</i>).....	6
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	
2.1 Tinjauan Pustaka (<i>State of the Art</i>).....	7
2.2 Konsep Steganografi	13
2.3 Konsep Citra Digital.....	14
2.4 Jenis Citra	14
2.4.1 Citra Berwarna	14
2.4.2 Citra Biner	16
2.4.3 Citra Berskala Keabuan	17
2.5 Piksel	17
2.6 <i>Least Significant Bit</i> (LSB)	18
2.7 Metadata Gambar	22
2.8 Kriptografi <i>Fernet</i>	22
2.9 Pengujian Algoritma Steganografi	23
BAB III METODE PENELITIAN	
3.1 Kerangka Penelitian	26
3.2 Tahapan Penelitian	28
3.3 Metode Pengumpulan Data	31
3.4 Kebutuhan <i>Software</i> dan <i>Hardware</i>	32
3.5 Kerangka Pengujian.....	32
BAB IV CENTER SEQUENTIAL TECHNIQUE	
4.1 Metode <i>Center Sequential Technique</i>	35
4.2 Implementasi Metode <i>CST</i>	37
4.2.1 Algoritma Penyisipan Pesan.....	37
4.2.2 Algoritma Ekstraksi Pesan	38
4.3 Pembahasan.....	39
4.3.1 Model Algoritma <i>CST</i>	39

4.4	Hasil Pengujian.....	40
4.4.1	Proses Penyisipan Pesan.....	40
4.4.2	Pengujian <i>Fidelity</i>	42
4.4.3	Pengujian <i>Robustness</i>	43
4.5	Evaluasi Hasil Pengujian	44
BAB V CENTER EMBEDDED PIXEL POSITIONING		
5.1	Metode <i>CEPP</i>	46
5.1.1	Metode Penyisipan Gambar	47
5.1.2	Metode Ekstraksi Pesan	49
5.2	Implementasi Metode <i>CEPP</i>	50
5.2.1	Algoritma Pembacaan Gambar	50
5.2.2	Algoritma Penyisipan Pesan.....	52
5.2.3	Algoritma Ekstraksi Pesan	53
5.3	Pembahasan.....	54
5.3.1	Proses Penyisipan Pesan.....	54
5.3.2	Proses Ekstraksi Pesan	60
5.4	Hasil Pengujian Steganografi <i>CEPP</i>	61
5.4.1	Pengujian <i>Imperceptibility</i>	61
5.4.2	Pengujian <i>Fidelity</i>	62
5.4.3	Pengujian <i>Robustness</i>	63
5.4.4	Pengujian <i>Recovery</i>	66
5.5	Evaluasi Hasil Pengujian Metode <i>CEPP</i>	67
BAB VI STEGANOGRAPHY ON IMAGE METADATA		
6.1	Konsep <i>SIM</i>	69
6.2	Metode Penyisipan Pesan Menggunakan <i>Fernet</i> dan <i>Exif</i>	70
6.3	Metode Ekstraksi Pesan Menggunakan <i>Fernet</i> dan <i>Exif</i>	71
6.4	Implementasi Metode	73
6.4.1	Pembacaan <i>Cover Image</i> dan Enkripsi Pesan	73
6.4.2	Algoritma Penyisipan Pesan.....	73
6.4.3	Algoritma Ekstraksi Pesan	74
6.5	Pembahasan	75
6.6	Pengujian <i>Fidelity</i>	78
6.7	Pengujian <i>Robustness</i>	79
6.7.1	Pengujian <i>Cropping</i>	79
6.7.2	Pengujian <i>Rotate</i> dan <i>Flip</i>	82
6.7.3	Pengujian <i>Resize Image</i>	84
6.7.4	Pengujian Pemberian Efek Kontras Warna	84
6.7.5	Pengujian Ketahanan Pesan pada Metadata	85
6.8	Evaluasi Hasil Pengujian.....	86
6.9	<i>Future Research Steganography</i>	88
BAB VII KESIMPULAN DAN SARAN		
7.1	Kesimpulan	89
7.2	Saran	89

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar	Halaman
2.1	Warna RGB dalam Ruang Berdimensi Tiga 15
2.2	Citra Berwarna dan Representasi Warnanya..... 15
2.3	Hasil Pembacaan Citra Berwarna 16
2.4	Citra Biner..... 17
2.5	Representasi Biner 18
2.6	Kerangka Pengujian Steganografi..... 23
3.1	Kerangka Penelitian 26
3.2	Tahapan Penelitian 28
4.1	Ekuivaken Nilai Piksel dengan Biner 36
4.2	Model Algoritma <i>CST</i> 39
4.3	<i>Cover Image</i> 40
4.4	Perbandingan Nilai Intensitas <i>Stego-Image</i> 41
4.5	Perbandingan Nilai <i>PSNR Stego Image</i> 43
4.6	Hasil Uji <i>Cropping</i> 44
5.1	Alur Penyisipan Gambar 47
5.2	Proses Pencarian Koordinat Kontainer 48
5.3	Alur Ekstraksi Pesan 49
5.4	Panjang Stego Bit Tidak Habis Dibagi 8 49
5.5	Pembacaan Bit Setelah Menemukan Nilai <i>idx</i> 50
5.6	<i>Cover Image</i> Pengujian Tahap Pertama 55
5.7	<i>Cover Image</i> Pengujian Tahap Kedua..... 55
5.8	Pengukuran Koordinat Penyisipan Pesan Rahasia..... 56
5.9	Grafik Perbandingan Pengujian Tahap Pertama 58
5.10	Grafik Perbandingan Pengujian Tahap Kedua 59
5.11	Proses Pembacaan Area Kontainer Pesan 60
5.12	Grafik Hasil Uji <i>Imperceptibility</i> 62
6.1	<i>Flowchart</i> Proses Penyisipan Pesan..... 70
6.2	<i>Flowchart</i> Ekstraksi Pesan..... 72
6.3	<i>Cover Image</i> 75
6.4	Penggunaan <i>Crop Handles</i> untuk <i>Pengujian Cropping</i> 80

DAFTAR TABEL

Tabel	Halaman
2.1	Warna dan Nilai Penyusunan Warna 14
3.1	Format Pertanyaan untuk Pengujian <i>Imperceptibility</i> 33
3.2	Skenario Pengujian <i>Fidelity</i> 33
3.3	Skenario Pengujian <i>Robustness (Cropping)</i> 34
3.4	Skenario Pengujian <i>Robustness (Image Resize)</i> 34
3.5	Skenario Pengujian <i>Robustness (Image Rotation)</i> 34
4.1	Komposisi Perbandingan <i>Cover Image</i> dan <i>Stego Image</i> 41
4.2	Hasil Uji Nilai <i>PSNR</i> 42
4.3	Hasil Uji <i>Cropping</i> 43
5.1	Komposisi Perbandingan <i>Cover Image</i> dan <i>Stego Image (1)</i> 58
5.2	Komposisi Perbandingan <i>Cover Image</i> dan <i>Stego Image (2)</i> 59
5.3	Hasil Uji <i>Imperceptibility</i> 61
5.4	Hasil Uji Tahap Pertama Kualitas <i>Stego Image</i> 62
5.5	Hasil Uji Tahap Kedua Kualitas <i>Stego Image</i> 63
5.6	Hasil Uji <i>Cropping</i> Secara Simetris..... 64
5.7	Hasil Uji <i>Cropping</i> Secara Asimetris..... 65
5.8	Hasil Uji <i>Recovery</i> 66
5.9	Nilai <i>PSNR</i> Penelitian Sebelumnya 67
5.10	Ketahanan Manipulasi <i>Cropping</i> Penelitian Sebelumnya..... 68
6.1	Hasil Uji Penyisipan Pesan 76
6.2	Perbandingan <i>Histogram Cover Image</i> dan <i>Stego Image</i> 76
6.3	Hasil Uji <i>Fidelity</i> 79
6.4	Hasil Uji <i>Cropping</i> Secara Simetris..... 81
6.5	Hasil Uji <i>Cropping</i> Secara Asimetris..... 82
6.6	Hasil Uji Manipulasi <i>Rotate</i> 83
6.7	Hasil Manipulasi <i>Flip</i> 83
6.8	Hasil Uji <i>Resize Image</i> 84
6.9	Hasil Uji Efek Kontras Warna 85
6.10	Hasil Uji Ketahanan Pesan pada <i>Metadata</i> 86

ABSTRAK

ANALISIS DAN PENGEMBANGAN METODE PADA TEKNIK STEGANOGRAFI UNTUK MENGATASI PERMASALAHAN MANIPULASI *ROBUSTNESS*

Oleh

DEDI DARWIS

Pemanfaatan steganografi saat ini telah banyak diterapkan pada pertukaran data melalui internet, pesan singkat, media sosial serta penyembunyian data di dalam *personal computer (PC)*. *Robustness* merupakan hal yang penting pada keamanan steganografi. Pada umumnya, citra yang disisipi pesan tidak memiliki ketahanan terhadap serangan, sehingga pesan akan rusak ketika dilakukan ekstraksi setelah manipulasi *robustness* diterapkan. Beberapa jenis dari serangan *robustness* adalah manipulasi *cropping*, *rotate*, *resize*, dan pemberian efek warna pada gambar. Hal ini akan menjadi masalah terhadap keamanan Steganografi gambar karena *stego-image* yang dilakukan manipulasi akan mengalami kerusakan pada pesan rahasia ketika dilakukan proses ekstraksi karena piksel pada *stego-image* mengalami perubahan nilai.

Pada penelitian ini dikembangkan pendekatan baru untuk mengatasi permasalahan *robustness* dengan mengembangkan metode *LSB*, pemanfaatan domain spasial, *exif metadata image* dan kriptografi *fernet*. Penelitian ini menghasilkan tiga pendekatan baru dalam hal mengatasi permasalahan *robustness* namun tetap memperhatikan kualitas citra hasil steganografi. Metode yang dikembangkan diberi nama : *Center Sequential Technique (CST)*, *Center Embedded Pixel Positioning (CEPP)* dan *Steganography on Image Metadata (SIM)*.

Berdasarkan hasil uji yang dilakukan, metode *CST*, *CEPP* dan *SIM* dapat mengatasi manipulasi *cropping* lebih dari 50% secara simetri dan asimetri. Namun, metode *CST* dan *CEPP* tidak dapat menahan operasi untuk *rotate*, *resize* dan pemberian efek warna pada gambar. Sedangkan untuk operasi *rotate*, *resize* dan pemberian efek warna pada gambar hanya dapat ditangani oleh metode *SIM*. Berdasarkan pengujian yang dilakukan, metode *CST* dapat menghasilkan rata-rata nilai *PSNR* sebesar 51,14776 db, dan pada metode *CEPP* menghasilkan rata-rata nilai *PSNR* 51,96582 db, sedangkan untuk metode *SIM*, nilai *PSNR* mencapai 100 db. Hal ini membuktikan bahwa metode yang dikembangkan terutama pada metode *SIM* dapat menghasilkan kualitas citra *stego image* yang baik berdasarkan perhitungan nilai *PSNR*.

Kata Kunci : *Center Embedded Pixel Positioning*, *Center Sequential Technique*, *Fidelity*, *LSB*, *Steganography on Image Metadata*, *Robustness*

ABSTRACT**ANALYSIS AND DEVELOPMENT OF METHODS IN
STEGANOGRAPHIC TECHNIQUES TO OVERCOME ROBUSTNESS
MANIPULATION PROBLEMS****By****DEDI DARWIS**

The use of steganography has now been widely applied to data exchange via the internet, short messages, social media and data hiding in personal computers (PCs). Robustness is important in steganographic security. In general, image which is embedded with the message have not resistance to attack, so the message will be damaged when it was extracted after robustness manipulation. Several types of robustness attacks are cropping, rotating, resizing, and applying color effects to the images. This will be a problem for the security of image Steganography because the Stego image that is manipulated will experience damage to the secret message when the extraction process is carried out because the pixels on the Stego image change in value.

In this study, a new approach was developed to overcome the robustness problem by developing the LSB method, utilizing spatial domains, exif metadata images and fernet cryptography. This study proposed three new approaches in terms of overcoming the problem of robustness, but still retain the quality of the steganographic image. The methods developed were named: Center Sequential Technique (CST), Center Embedded Pixel Positioning (CEPP) and Steganography on Image Metadata (SIM).

Based on the results of tests carried out by the CST, CEPP and SIM those methods can overcome the cropping manipulation for more than 50% symmetrically and asymmetrically. However, the CST and CEPP methods cannot withstand manipulations to rotate, resize and apply color effects to images. Meanwhile, the manipulation of rotate, resize and color effects on the image can only be handled by the SMI method. Based on the tests carried out, the CST method can produce an average PSNR value of 51,14776 db and the CEPP method produces an average PSNR value of 51,96582 db, and for the SIM method, the PSNR value reaches 100 db. This proves that the method developed especially on the SIM method can produce a good stego image quality based on the calculation of the PSNR value.

Keywords: *Center Embedded Pixel Positioning, Center Sequential Technique, Fidelity, LSB, Steganography on Image Metadata, Robustness*