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. Suripto 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 menjalan 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. Suripto 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 selesainanya 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 arahannya.
12. Ibu Dr. Khoirin Nisa, S.Si., M.Si. selaku Sekretaris Program Studi Doktor MIPA atas bantuan dan arahannya.
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 Kompetetif Nasional dari Kemendikbudristek selama lima tahun berturut-turut (2017 – 2021)

- A New Digital Image Steganography Based on Center Embedded Pixel Positioning (2021).
- Perbandingan Metode Descrete 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

DAFTAR GAMBAR

Gambar Halaman

DAFTAR TABEL

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*

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Komunikasi digital adalah suatu bagian infrastruktur yang sangat mendasar akhir-akhir ini dan banyak aplikasi yang berbasis internet saat ini. Internet umumnya tidak menggunakan *link* yang aman, sehingga informasi yang berjalan rentan terhadap serangan dari pihak lain. Pentingnya mengurangi kemungkinan informasi terdeteksi selama masa transmisi menjadi masalah. Sebagai hasilnya, keamanan informasi yang melewati saluran terbuka sudah menjadi masalah yang mendasar (1) .

Data multimedia sudah berkembang dengan cepat dan luas melalui internet dalam bentuk yang bervariasi seperti gambar, audio, video dan *text*. Dalam komunikasi digital yang menggunakan internet, segala sesuatu dapat dilihat dan diakses oleh setiap pengguna. Sehingga, keamanan informasi adalah suatu hal yang penting dan diperlukan. Ada tiga tujuan dari keamanan informasi yakni *confidentiality*, *integrity*, dan *availability* (CIA). *Confidentiality* (kerahasiaan) berarti bahwa informasi harus aman dan tidak dapat diakses oleh pengguna yang tidak memiliki hak. *Integrity* berarti keakuratan dari informasi, dan *Availability* (ketersediaan) berarti bahwa informasi itu dapat diakses tepat waktu oleh pengguna yang berhak. Keamanan jaringan sederhana tidaklah cukup untuk komunikasi informasi yang *reliable* seperti *text*, audio, video dan gambar digital (2).

Terdapat beberapa teknik yang dapat digunakan untuk mengamankan informasi diantaranya dengan menggunakan enkripsi, *watermarking, digital watermarking, reversible watermarking,* kriptografi, steganografi dan lain-lain. Pada penelitian ini akan dibahas mengenai teknik steganografi. Teknik steganografi dipilih karena pengembangan dari teknik kriptografi yang dapat mengamankan data dengan cara menyisipkan pesan rahasia ke dalam media lainnya, sehingga keberadaan pesan rahasia tersebut tidak menimbulkan kecurigaan oleh pihak lain yang bukan sebagai penerima pesan (3).

Pada steganografi gambar, pesan rahasia disembunyikan di dalam *cover image* untuk menyamarkan pesan dari penyerang (orang yang tidak memiliki hak terhadap informasi) dan pesan yang sudah disisipkan pada *cover image* disebut sebagai *stego-image*. Pada dasarnya, tujuan steganografi bukan hanya untuk menghindari pihak yang tidak memiliki hak terhadap informasi dari men-*decode* pesan yang tersembunyi, tetapi mencegah agar pesan yang disembunyikan tidak menimbulkan kecurigaan.

Cara mengetahui kualitas gambar dari hasil steganografi adalah menguji kehandalan dari algoritma atau teknik yang digunakan pada saat proses penyisipan dan ekstraksi. Ada empat metode untuk melakukan pengujian yaitu : *imperceptibility*, *fidelity*, *recovery*, dan *robustness* (4).

Proses manipulasi *robustness* dapat menimbulkan masalah pada steganografi gambar. Pada umumnya citra yang disisipi pesan tidak memiliki ketahanan terhadap serangan ini atau pesan akan rusak ketika dilakukan ekstraksi setelah dilakukan manipulasi *robustness* (5), (6).

Manipulasi *robustness* yang pertama adalah dengan melakukan *cropping* pada gambar. Hal ini akan menjadi masalah terhadap steganografi gambar karena *stego-image* yang dilakukan pemangkasan akan mengalami kerusakan pada pesan rahasia ketika dilakukan proses ekstraksi karena piksel pada *stego-image* mengalami perubahan nilai. Terdapat penelitian yang mengusulkan suatu kerangka konseptual untuk melindungi informasi yang hilang dari *stego-image* yang sudah di *crop* (7). Serangan yang dilakukan pada *stego-image* dapat membuat pesan yang tersembunyi pada *cover image* menjadi rusak. Salah satu serangan pada *stego-image* adalah serangan *cropping*. Manipulasi *cropping* pada *image processing* dilakukan dengan membuang sebagian atau memotong pada bagian gambar tertentu. Umumnya pesan yang tersembunyi pada *stego-image* berada pada bit yang paling akhir dan berlokasi pada pojok kiri atas gambar. Sehingga, jika *stego image* dipotong maka pesan yang tersembunyi pada gambar tersebut akan sulit untuk diekstrak bahkan sampai hilang atau rusak.

Manipulasi *robustness* yang kedua adalah dengan melakukan *resize image* pada *stego image*. *Resize image* dilakukan dengan cara memodifikasi ukuran resolusi pada gambar sehingga *stego image* akan mengalami pemampatan-pengecilan / pembesaran pada ukuran aslinya. Jika pada *stego image* dilakukan manipulasi *resize*, maka pesan yang ada pada *stego image* tersebut memungkinkan tidak bisa dilakukan ekstraksi karena gambar yang telah dimampatkan/diperbesar akan mengalami perubahan nilai piksel. Penelitian yang dilakukan oleh Kodovsky & Fridrich (8) yang membahas permasalahan *resize image* dan menyatakan bahwa salah satu penyebab *stego image* tidak dapat dilakukan proses ekstraksi karena ketika panjang pesan rahasia yang disisipkan pada *stego image* mengalami perubahan nilai piksel secara proporsional.

Manipulasi *robustness* yang ketiga adalah dengan melakukan rotasi gambar *(rotate image)*. *Stego image* pada umumnya tidak memiliki ketahanan pada serangan rotasi gambar karena jika gambar mengalami pergeseran sedikit pada posisi sebelumnya maka nilai piksel akan berubah. Perubahan piksel akan lebih signifikan jika gambar dirotasi sampai dengan 90^0 atau lebih yang menyebabkan pesan rahasia yang tersembunyi pada *stego image* tidak dapat dilakukan proses ekstraksi. Pada penelitian yang dilakukan oleh Bhatu & Shah (9) menggunakan kombinasi tiga metode yaitu *discrete cosine transform* (DCT), *lifted wavelet transform* (LWT) dan *singular value decomposition* (SVD) untuk menangani masalah *capacity*, *robustness*, *security* dan *imperceptibility* pada steganografi. Hasil uji coba yang dilakukan menghasilkan *imperceptibility* yang sangat baik, *robustness* dan *capacity* penanaman pesan yang baik. Pendekatan ini menghasilkan kinerja yang baik terhadap berbagai serangan proses citra seperti *salt & pepper noise, gaussian noise, gaussian low pass filter, sharpen, gaussian blur*, namun masih memiliki kekurangan yaitu pada serangan terhadap rotasi gambar.

Manipulasi *robustness* yang terakhir yang dikaji pada penelitian ini adalah menguji ketahanan *stego image* dengan melakukan serangan *gaussian blur* yaitu dengan cara memberikan sebuah efek *blur* yang dihasilkan oleh sebuah fungsi *gaussian*. Dengan menggunakan serangan ini maka *stego image* akan memiliki bagian

gambar yang tidak jelas *(blur)*, serangan ini juga akan mengakibatkan pesan rahasia pada *stego image* tidak dapat dilakukan proses ekstraksi. Penelitian yang dilakukan oleh Singh & Siddiqui (10) menangani masalah manipulasi *robustness* dengan menggunakan metode *daubechies complex wavelet transform* (DCxWT), *singular value decomposition* (SVD) dan *chaotic sequence*. Penelitian ini menghasilkan eksperimen yang menunjukkan bahwa kombinasi metode *DCxWT, SVD* dan *chaotic sequence* dapat memberikan *security* dan *robustness* terhadap beberapa serangan *geometric* dan *image processing* biasa seperti *JPEG compression, gaussian low-pass filtering, median filtering, cropping, rotation, resizing* dan *histogram equalization attacks.*

Teknik dalam steganografi secara umum dikategorikan menjadi dua yaitu teknik daerah spasial dan teknik daerah *transform*. Pada dasarnya teknik daerah spasial tidak terlalu kompleks dan sederhana dalam proses steganografi. Sedangkan teknik daerah *transform* membutuhkan komputasi atau perhitungan yang lebih kompleks. Proses penyisipan pesan pada teknik daerah spasial lebih mudah dikembangkan dibandingkan dengan menggunakan teknik daerah *transform*. Sehingga penggunaan teknik daerah spasial dapat meningkatkan kualitas steganografi dari aspek *robustness* terhadap serangan manipulasi *image processing* yang bermacam-macam seperti *filtering, gaussian blur, cropping, noise, rescaling* dan manipulasi lainnya (10).

Penerapan teknik-teknik tersebut tentunya tidak lepas dari algoritma yang digunakan, baik itu menggunakan algoritma yang sudah ada, kombinasi dua algoritma atau lebih maupun memodifikasi algoritma. Diantara algoritma yang paling sering digunakan (spasial atau *transform*) adalah *least significant bit* (*LSB*), *discrete cosine transforms* (DCT), *discrete wavelet transforms* (DWT) dan lain-lain. Beberapa penelitian sering menggunakan beberapa algoritma tersebut, dengan memodifikasi atau mengkombinasikan dengan algoritma lain. M. Kumar & Yadav (11) mengusulkan pengembangan algoritma pada domain *transform* dan eksperimen dilakukan menggunakan serangan *image processing* yang berbeda-beda. Hasil simulasi menunjukkan bahwa ada peningkatan yang besar pada nilai

PSNR stego-image. Muyco & Hernandez (12) melakukan penelitian dengan memodifikasi fungsi *hash* pada algoritma *LSB* dan memanfaatkan *metadata* dalam hal penyimpanan pesan. Penelitian yang dilakukan menghasilkan sebuah model penyimpanan dengan menyisipkan data melalui *exif metadata image* pada *cover* dan tetap menghasilkan kualitas *stego image* yang baik.

Penelitian yang dilakukan berkenaan dengan pengembangan metode pada steganografi adalah untuk menghasilkan *stego image* yang memiliki ketahanan terhadap serangan-serangan manipulasi *robustness* tanpa mengurangi kualitas citra pada aspek *fidelity*.

1.2 Rumusan Masalah

Bagaimana membuat pendekatan baru pada teknik steganografi yang dapat meningkatkan *robustness stego image* terhadap manipulasi *image processing* seperti *cropping, resize, rotate* dan *colouring* yang tahan hingga lebih dari 50% dan tetap mempertahankan aspek kualitas citra?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengembangkan metode pada steganografi dalam hal mengatasi permasalahan manipulasi *robustness* dengan tetap mempertahankan kualitas citra pada aspek *imperceptibility, fidelity* dan *recovery*.

1.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat menjadi alternatif dan referensi dalam hal mengamankan data digital melalui teknik steganografi yang aman dari manipulasi *robustness*.

1.5 Batasan Penelitian

1. Algoritma atau metode steganografi yang dijadikan sebagai dasar eksperimen pada penelitian ini adalah *Least Significant Bit (LSB)* dan *Image Metadata.*
2. Metode *LSB* yang digunakan pada penelitian ini adalah untuk mengembangkan algoritma pada perubahan piksel yang menggunakan

domain spasial.

3. Piksel yang digunakan adalah pada daerah spasial.
4. Pesan rahasia menggunakan media gambar (*grayscale* dan *RGB*) dan *file txt.*
5. Media penampung pesan atau *cover image* adalah gambar dengan format ekstensi **.JPG* atau **.PNG.*
6. Serangan *image processing* yang dibahas adalah serangan yang berfokus terhadap *cropping, resize, rotate dan colouring/gaussian blur.*
7. Bahasa pemrograman yang digunakan untuk melakukan eksperimen adalah *Python 3.7.*
8. Metode yang digunakan untuk pengujian adalah *robustness, imperceptibility, fidelity* dan *recovery.*

1.6 Kebaruan Penelitian *(Novelty)*

Penelitian ini menghasilkan kebaruan berupa pendekatan baru pada teknik penyisipan pesan dan teknik ekstraksi pesan pada steganografi. Pendekatan tersebut berfokus pada ketahanan *stego image* terhadap manipulasi *robustness*. Terdapat tiga pendekatan baru pada penelitian yang dilakukan yaitu:

1. Metode *Center Sequential Technique*

   Metode ini menyisipkan gambar dengan format *grayscale* ke tengah *cover image* dengan cara sekuensial untuk mencegah manipulasi *cropping* sampai dengan 50%.
2. Metode *Center Embedded Pixel Positioning*

   Metode ini menyisipkan gambar dengan format *RGB* ke wilayah domain spasial di posisi tengah *cover image* untuk mencegah manipulasi *cropping* sampai dengan 70%.
3. *Steganography on Image Metadata*

   Metode ini menyisipkan pesan menggunakan *exif metadata* pada *cover image*. Metode ini juga dikombinasikan dengan kriptografi *fernet cipher algorithm* yang berfungsi untuk membuat *stego-key* dan enkripsi pesan. Metode ini dapat menahan semua manipulasi *robustness* (*cropping, resize, rotate* dan yang lainnya) sampai dengan tingkat ketahanan 90%.

BAB II
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka *(State of the Art)*

1. Penelitian yang dilakukan oleh Juarez-Sandoval et al (13) dengan judul *Cropping and Noise Resilient Steganography Algorithm using Secret Image Sharing*. Steganografi yang diterapkan pada penelitian ini menggunakan *secret image sharing* (SIS). Kinerja dari algoritma steganografi yang diterapkan dievaluasi menggunakan beberapa *cover image* dan beberapa gambar rahasia dengan ukuran yang berbeda.

   Kapasitas maksimal penyimpanan pesan tergantung dari skema SIS yang digunakan. Skema SIS (3,4)-th memiliki kapasitas penyimpanan 25% dari *cover image*, sedangkan SIS (3,5)-th 16.67% dari *cover image.* Kapasitas *fault tolerance* dari steganografi yang diterapkan dievaluasi menggunakan serangan *cropping.* Hasil eksperimen penelitian ini menunjukkan bahwa kualitas gambar yang diekstrak dari *stego-image* tersebut memiliki kualitas yang tinggi bahkan bila *stego-image* mengalami *cropping* lebih dari 20%.

2. Penelitian yang dilakukan oleh Swain & Lenka (14) dengan judul *A novel steganography technique by mapping words with LSB array*. Dalam penelitian ini diterapkan teknik steganografi baru menggunakan *LSB array*. Empat *LSB array* seperti *LSB0, LSB1, LSB2* dan *LSB3* didefinisikan terlebih dahulu. Hasil eksperimen pada metode ini menguatkan *robustness* pada steganografi dan kapasitas penampungan pesan juga baik. Tidak ada kecurigaan secara visual yang dapat diamati dari *stego image*. Serangan steganalitik seperti analisis *Chi-square* tidak berhasil mendeteksi lokasi pesan pada *stego image*.

3. Penelitian yang dilakukan oleh Sedighi et al (15) dengan judul *Content-Adaptive Steganography by Minimizing Statistical Detectability*.

Berdasarkan rancangan steganografi model *covel MVG* yaitu model statistik *cover image*, dalam *omniscient warden* yang menggunakan *Likelihood Ratio Test* (*LRT)* menjadi lebih optimal karena akan menghasilkan frekuensi tinggi dalam model tersebut. Pada penelitian ini dihasilkan ruang parameter secara dimensional untuk menangkap karakter gambar yang tidak berubah.

4. Penelitian yang dilakukan oleh Rejani et al (16) dengan judul *Pixel Pattern Based Steganography on Images*. Karakteristik dari algoritma yang diterapkan adalah tidak perlu mengubah piksel pada gambar seperti pada algoritma yang lain kecuali bila benar-benar diperlukan. Bagi komputer, gambar adalah sekumpulan data atau informasi yang merepresentasikan intensitas cahaya di beberapa titik yang menyusun sebuah data *image raster*.

   Seluruh gambar digital umumnya disimpan dalam *file* (24-bit) *RGB* atau (8-bit) *grayscale*. Sebuah gambar 24-bit menyediakan banyak ruang untuk menyimpan informasi. Seluruh kombinasi warna diturunkan dari tiga warna primer yaitu merah, hijau, dan biru *(RGB)*. Pada setiap warna primer ini direpresentasikan oleh satu *byte*, karena semua nilai *RGB* direpresentasikan oleh angka, maka dapat digunakan untuk merepresentasikan teks menggunakan algoritma *modbit*.

   Algoritma *modbit* sangat mirip dengan algoritma *Luhm mod n*. Algoritma ini secara umum digunakan untuk menghasilkan (*generate*) rumus *checksum*. Algoritma ini digunakan untuk menemukan piksel yang dapat merepresentasikan karakter. Tiap karakter dari teks yang dimasukkan akan dipetakan pada serangkaian angka dan pemetaan ini akan dikelola dari dalam pada program steganografi. Sebagai contoh huruf ‘a’ dapat direpresentasikan oleh 10 digit, huruf ‘b’ dapat direpresentasikan oleh 12 digit, dan seterusnya. Selama proses enkripsi program ini akan memindai (*scan*) gambar dan akan menambahkan nilai *RGB*, kemudian membaginya dan menemukan nilai *mod* (sisa hasil bagi). Jika *mod* cocok dengan karakter tersebut, maka lokasi pada gambar dapat digunakan untuk

merepresentasikan karakter tersebut. Untuk menyimpan lokasi piksel yang merepresentasikan sebuah karakter, pengguna dapat menyimpannya dalam *file* teks yang terpisah atau membuatnya sebagai bagian dari *metadata* gambar tersebut.

Penelitian ini menghasilkan suatu metode steganografi yang lebih baik untuk penanaman pesan rahasia berbentuk bit pada bagian *metadata* gambar yang berbasis pada nilai *RGB* dan posisi piksel-nya. Gambar hanya akan diubah pada karakter di mana algoritma tidak dapat menemukan piksel yang tidak dapat merepresentasikan karakter tersebut. Karena *metadata* telah dimodifikasi, *stego image* terlihat sama persis dengan gambar originalnya atau setidaknya akan sulit untuk mendeteksi perubahan pada gambar bila dilihat dengan mata telanjang.

5. Penelitian yang dilakukan oleh Bhatu & Shah (9) dengan judul *Customized Approach to Increase Capacity and Robustness in Image Steganography*. Pendekatan yang dilakukan mencoba untuk meningkatkan *capacity* dan *robustness* dari gambar steganografi. Dalam penelitian ini, digunakan tiga metode yakni *Discrete Cosine Transform (DCT), Lifted Wavelet Transform (LWT)* dan *Singular Value Decomposition (SVD).* Karena stabilitas dari nilai-nilai tunggal dari *SVD* dan keunggulan *LWT* dalam meningkatkan kehalusan dan mengurangi efek *noise*, maka pendekatan yang diusulkan menghasilkan *imperceptibility* yang sangat baik, *robustness* dan *capacity* penanaman yang baik. Pendekatan ini menghasilkan kinerja yang baik terhadap berbagai serangan proses citra seperti *Salt & Pepper Noise, Gaussian Noise, Gaussian Low Pass Filter, Sharpen,* dan *Gaussian Blur*.

6. Penelitian yang dilakukan oleh Al-Afandy et al (4) dengan judul *High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography.* Pada penelitian ini, tiap bagian dari pesan teks disisipkan ke dalam gambar terpotong dengan urutan rahasia menggunakan pendekatan *LSB.* Penyisipan dilakukan menggunakan *cover image* dari tiga

channel warna. Pada simulasi yang dilakukan, gambar yang digunakan adalah gambar *JPEG* bewarna dengan ukuran 512 × 512, resolusi 96 × 96 dpi dan kedalaman bit 24.

Beberapa tes yang diuji pada *stego image* diantaranya; tes visual untuk menentukan perubahan kualitas pada gambar *stego image*, nilai *PSNR* dari *stego image* dan kompleksitas ekstraksi pesan rahasia. Penelitian ini menghasilkan teknik penyembunyian data yang sangat aman menggunakan *cropping image* dan *steganography LSB*. Hal ini berdasarkan pembagian pesan rahasia yang dibagi ke dalam empat bagian dan mengekstrak keempat potongan dari *cover image* dengan koordinat rahasia khusus. Potongan disusun ulang dengan *cover image* menjadikan sebuah *stego-image*. Metode ini terbukti lebih aman dalam penyembunyian data dan tentunya lebih kompleks dalam ekstraksi data.

7. Penelitian yang dilakukan oleh Atawneh et al (17) dengan judul *Secure and Imperceptible Digital Image Steganographic Algorithm Based on Diamond Encoding in DWT domain*. Penelitian ini, mengenalkan sebuah algoritma baru yang disebut *DE-DWT* yang menggunakan skema *Diamond Encoding (DE)* untuk meningkatkan efisiensi penyisipan pesan yang dilakukan menggunakan algoritma *DWT*. *DE-DWT* menyisipkan pesan rahasia ke dalam sepasang koefisien dari *cover image* dengan menyesuaikan nilai-nilai sepasang koefisien ini. Algoritma ini dapat mengurangi distorsi yang terdapat pada *stego image*. Algoritma yang diusulkan mengkonversi bit rahasia ke dalam urutan digit *base-5*. Setelah itu, *cover image* diubah ke dalam domain *DWT* dan dipecah ke dalam serangkaian koefisien yang berpasangan. Skema *DE* digunakan setelahnya untuk mengubah setidaknya satu koefisien dari tiap koefisien yang sepasang untuk menanam digit *base-5* dari bit rahasia.

   Langkah selanjutnya yaitu membalikkan algoritma *DWT* untuk mendapatkan *stego image*. Metode yang digunakan mengurangi distorsi

pada saat penyisipan data. Algoritma ini mampu meningkatkan strategi *overflow/underflow* yang digunakan sebagai bagian dari *DE*. Metode ini mampu meningkatkan performa penyisipan pesan, dan lebih aman dari serangan *steganalysis*. Eksperimen menunjukkan bahwa algoritma ini memiliki efesiensi penyisipan yang lebih efisien dalam hal *imperceptibility* dan *embedding payload*. Hasil eksperimen juga mampu menghasilkan ketahanan data terhadap serangan seperti *compression, salt and pepper, gaussian noise* dan *cropping*.

8. Penelitian yang dilakukan oleh Juarez-Sandoval et al (18) dengan judul *Compact Image Steganalysis for LSB-Matching Steganography*. Dalam penelitian ini, metode *compact image* digunakan pada steganografi *LSB Matching*, dimana vektor fitur yang terdiri dari hanya 12 elemen diekstraksi dari gambar. Metode ini menganalisis artefak statistik yang terjadi pada gambar ketika data rahasia disematkan di dalamnya oleh steganografi *LSB Matching*.

   Metode ini memilih 12 fitur yang paling relevan berdasarkan *probability density function (PDF)* dari perbedaan piksel yang berdekatan dan *co-occurrence matrix* gambar, yang dapat membedakan *stego-image* dari gambar asli. *Support Vector Machine (SVM)* digunakan sebagai pengklasifikasi menggunakan vektor pelatihan dengan 12 elemen. Hasil eksperimen menunjukkan bahwa skema yang diusulkan memberikan kinerja diskriminasi yang lebih baik dari pada metode lain yang membutuhkan lebih banyak elemen fitur untuk diskriminasinya.

9. Penelitian yang dilakukan oleh Zhang et al (19) dengan judul *Robust Coverless Image Steganography Based on DCT and LDA Topic Classification*. Pada penelitian ini, untuk meningkatkan ketangguhan dan kemampuan menahan serangan steganalisis, dikembangkan algoritma steganografi yang baru menggunakan *discrete cosine transform (DCT)* dan *latent dirichlet allocation (LDA).* Langkah pertama, model *LDA* digunakan

untuk mengklasifikasikan *database* citra. Kedua, gambar *cover* dipilih dan membuat 8 × 8 blok *DCT*. Kemudian urutan fitur *robust* yang dihasilkan melalui hubungan antara koefisien arus searah di blok yang berdekatan.

Terakhir, membuat indeks terbalik yang berisi urutan fitur, *Discrete Cosine (DC)*, koordinat lokasi, dan jalur gambar yang akan dibuat. Pada metode ini, informasi rahasia diubah menjadi urutan biner dan dipartisi menjadi segmen-segmen, dan citra yang urutan fiturnya sama dengan segmen informasi rahasia dipilih sebagai citra sampul menurut indeks. Setelah itu, semua gambar sampul dikirim ke penerima. Dalam keseluruhan proses, tidak ada modifikasi yang dilakukan pada gambar asli. Hasil eksperimen dan analisis menunjukkan bahwa algoritma yang diusulkan dapat menahan deteksi algoritma steganalisis yang ada, dan memiliki ketahanan yang lebih baik terhadap pemrosesan citra pada umunya dan kemampuan yang lebih baik untuk keamanan steganografi. Metode ini juga memiliki ketahanan terhadap serangan geometris sampai batas tertentu.

Berdasarkan penelitian sebelumnya yang telah diuraikan pada tinjauan pustaka, maka perbedaan penelitian sebelumnya dengan penelitian yang dilakukan untuk menemukan kebaruan penelitian adalah sebagai berikut :

1. Penelitian ini berfokus pada penyelesaian masalah manipulasi *robustness* pada steganografi.
2. Pada penelitian ini metode yang digunakan adalah mengembangkan *Least Significant Bit* pada domain spasial.
3. Penelitian ini melakukan eksperimen dengan membuat pendekatan baru pada teknik steganografi gambar.
4. Fokus pengujian untuk *robustness* dengan cara melakukan *attack* pada *stego image* menggunakan *cropping*, *rotate*, *resize*, dan *colouring* lalu dilakukan proses ekstraksi.
5. Penelitian yang diusulkan tetap memperhatikan aspek *imperceptibility* dan *fidelity* untuk memastikan bahwa kualitas citra hasil dari metode yang diusulkan tetap tinggi.

2.2 Konsep Steganografi

Steganografi berasal dari bahasa Yunani yang berarti “tulisan tersembunyi”. Secara definisi steganografi adalah sebuah teknik untuk menyembunyikan keberadaan suatu data melalui sebuah media tertentu (20). Adapun komponen dalam steganografi antara lain:

1. *Cover*

   Dalam *stego-image*, *cover* yaitu berupa gambar asli yang belum disisipkan pesan yang akan menjadi media untuk pesan yang akan disembunyikan.
2. Pesan

   Suatu pesan yang dapat disembunyikan dalam *cover image* dapat berupa *plain text, cipher text,* gambar, atau apapun yang dapat disisipkan dalam satuan *bit*.
3. *Stego-Key*

   Stego-key adalah sebuah tipe *password* yang juga dapat disembunyikan, kemudian men-*decode* pesan.

Teknik atau metode steganografi dapat dibagi menjadi dua kategori, yaitu *image domain* atau sering disebut *spatial domain* dan *transform domain* atau *frequency domain* (20).

1. *Image domain* atau *spatial domain*

   Teknik penyisipan pesan pada intensitas piksel secara langsung. Teknik ini meliputi metode *bit-wise* yang menerapkan penyisipan bit dan manipulasi *noise.* Format gambar yang paling sesuai menggunakan metode ini adalah *lossless* dan teknik ini umumnya bergantung pada format gambar (20).
2. *Transform domain* atau *frequency domain*

   Metode dimana *cover image* ditransform dan kemudian pesan disisipkan pada gambar tersebut. Teknik *frequency domain* dapat menyembunyikan jumlah data yang banyak dengan tingkat keamanan yang tinggi, tidak terlihat dan pesan rahasia tidak hilang (20).

2.3 Konsep Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpan (21). Dalam dunia komputer, citra adalah sebuah *file* sederhana yang menampilkan warna yang berbeda dan intensitas cahaya pada daerah yang berbeda dari sebuah gambar (14).

2.4 Jenis Citra

Ada tiga jenis citra yang umum digunakan dalam pemrosesan citra. Ketiga jenis citra tersebut yaitu citra berwarna, citra berskala keabuan, dan citra biner (22).

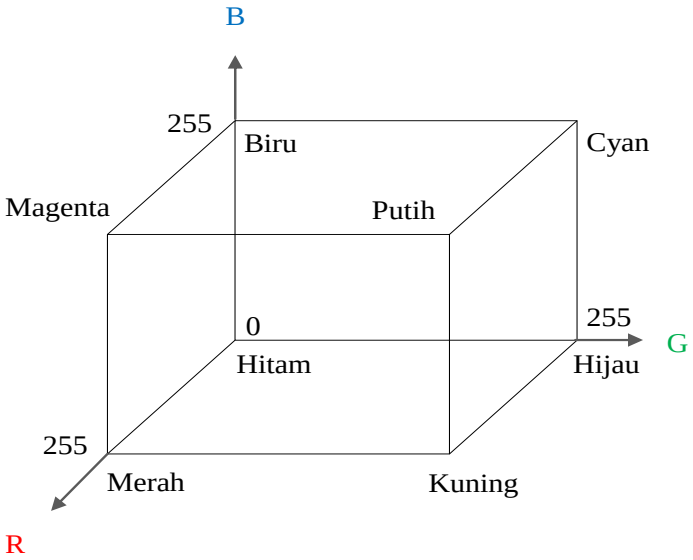
2.4.1 Citra Berwarna

Citra berwarna atau biasa dinamakan citra RGB merupakan jenis citra yang menyajikan warna dalam bentuk komponen R *(Red)* atau merah, G *(Green)* atau hijau, dan B *(Blue)* atau biru. Setiap komponen warna menggunakan 8 bit (nilainya berkisar antara 0 sampai dengan 255). Dengan demikian, kemungkinan warna yang dapat disajikan mencapai 255 x 255 x 255 atau 16.281.375 warna. Pada Tabel 2.1 diberikan contoh nilai dari warna R, G , dan B.

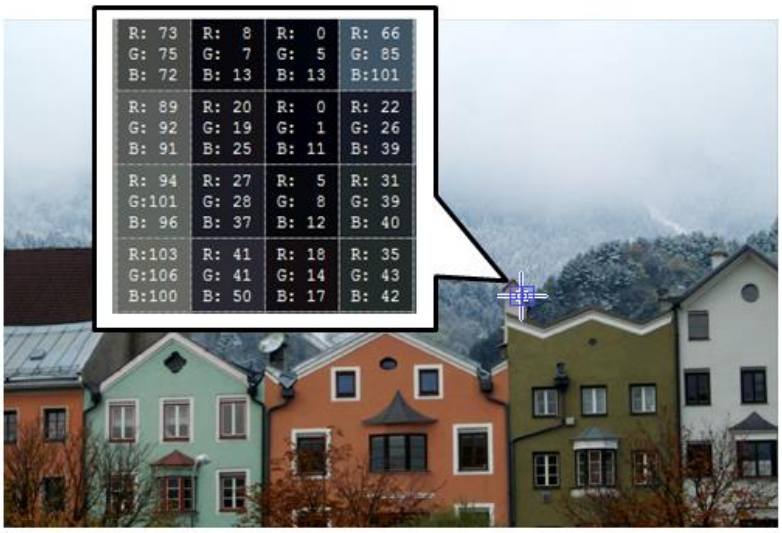
Tabel 2.1 Warna dan Nilai Penyusunan Warna

Warna	**R**	**G**	**B**
Merah	255	0	0
Hijau	0	255	0
Biru	0	0	255
Hitam	0	0	0
Putih	255	255	255
Kuning	0	255	255

Gambar 2.1 dan 2.2 menunjukkan pemetaan warna dalam ruang tiga demensi, adapun gambar selanjutnya menunjukkan keadaan suatu citra dan representasi warnanya.

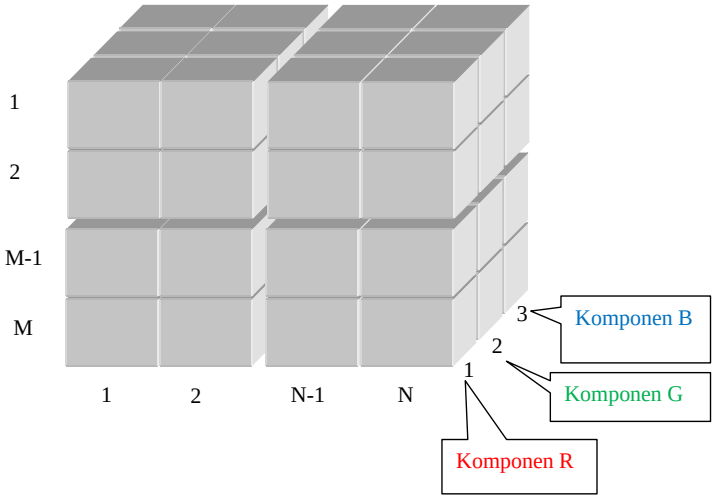


Gambar 2.1 Warna RGB dalam Ruang Berdimensi Tiga (22)



Gambar 2.2 Citra Berwarna dan Representasi Warnanya (22)

Hasilnya menunjukkan bahwa kota berupa larik berdimensi tiga, dengan dimensi ketiga berisi tiga buah nilai. Hal inilah yang membedakan dengan citra berskala keabuan. Secara umum, larik pembacaan citra berwarna dapat digambarkan seperti pada Gambar 2.3.

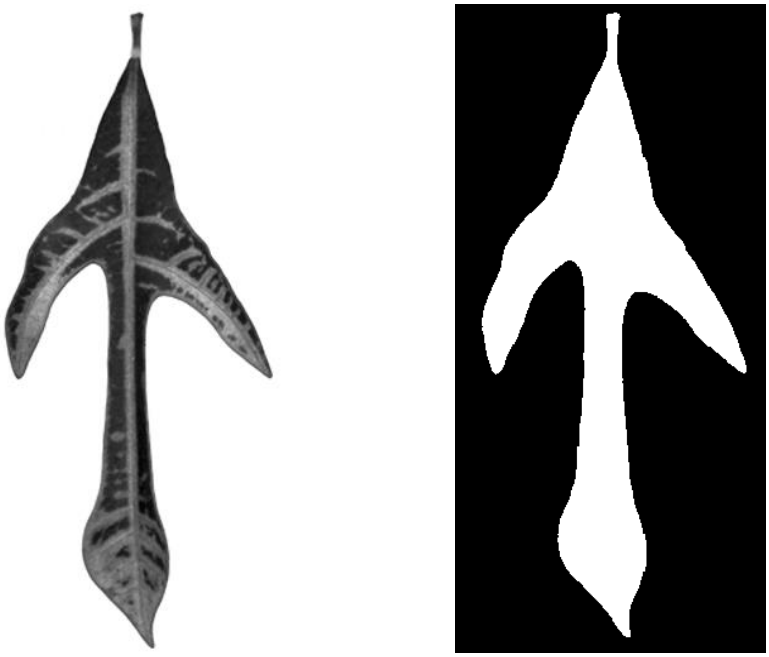


Gambar 2.3 Hasil Pembacaan Citra Berwarna (22)

Dimensi ketiga menyatakan komponen R, G, B. Indeks pertama menyatakan komponen R, indeks kedua menyatakan komponen G, dan indeks ketiga menyatakan komponen B.

2.4.2 Citra Biner

Citra biner adalah citra dengan setiap piksel hanya dinyatakan dengan sebuah nilai dari dua buah kemungkinan (yaitu nilai 0 dan 1). Nilai 0 menyatakan warna hitam dan nilai 1 menyatakan warna putih. Citra jenis ini banyak dipakai dalam pemrosesan citra, misalnya untuk kepentingan memperoleh tepi bentuk suatu objek. Sebagai contoh, perhatikan Gambar 2.4 bagian kiri menyatakan citra beraras keabuan, sedangkan bagian kanan adalah hasil konversi ke citra biner.



(a) Citra daun berskala keabuan (b) Citra biner

Gambar 2.4 Citra Biner (22)

2.4.3 Citra Berskala Keabuan

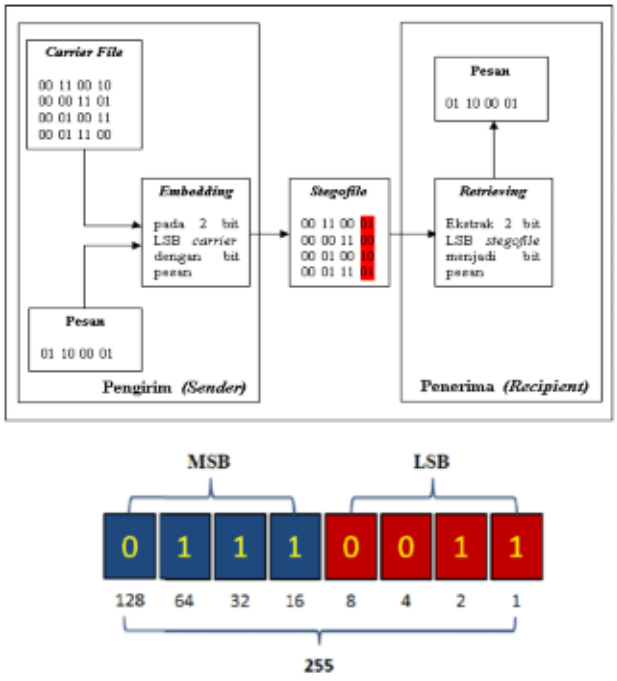
Sesuai dengan nama yang melekat, citra jenis ini menangani gradasi warna hitam dan putih, yang tentu saja menghasilkan efek warna abu-abu. Pada jenis gambar ini, warna dinyatakan dengan intensitas. Dalam hal ini, intensitas berkisar antara 0 sampai dengan 255, nilai 0 menyatakan hitam dan nilai 255 menyatakan putih.

2.5 Piksel

Secara kasat mata seluruh sistem grafis dasarnya adalah *raster-base* (pola berbentuk kotak yang sejajar). Gambar yang terlihat pada perangkat adalah sebuah *array raster* dari sebuah elemen gambar, atau disebut piksel, yang dihasilkan oleh sistem grafis (23).

2.6 *Least Significant Bit (LSB)*

Metode *Least Significant Bit (LSB)* merupakan metode-metode yang tidak terlalu kompleks, namun penyimpanan pesan pada *cover* objek juga cukup besar. Dasar metode ini adalah bilangan berbasis *biner* yaitu angka 0 dan 1, karena pada data digital merupakan susunan angka 0 dan 1 maka proses penerapannya menjadi mudah. Lebih lanjut metode ini berhubungan erat dengan ukuran 1-bit dan ukuran 1 *byte* di mana 1 *byte* data terdiri dari 8-bit data dan bit pada posisi paling kanan disebut dengan *LSB*. Steganografi dengan metode *LSB* diganti dengan bit yang disembunyikan. Karena bit yang diganti hanya bit yang paling akhir, maka *stego image* yang dihasilkan hampir sama persis dengan *cover image*-nya (Zhang et al (6). Sedangkan menurut Swain & Lenka (14), *Least Significant Bit (LSB)* adalah bit-bit yang jika diubah tidak akan berpengaruh secara nyata terhadap kombinasi warna yang dihasilkan oleh komponen warna pada gambar. Sehingga dapat disimpulkan bahwa metode *Least Significant Bit* (*LSB*) merupakan metode yang mengubah bilangan biner pada bit terakhir yang menghasilkan *stego image* yang hampir persis dengan *cover image*-nya. Representasi biner pada metode *LSB* dapat dilihat pada Gambar 2.5.



Gambar 2.5 Representasi Biner (22)

Metode *LSB* secara dasar memang belum dapat menangani masalah *robustness* pada steganografi, namun beberapa penelitian telah melakukan modifikasi pada algoritma *LSB* dan hasilnya menunjukkan bahwa algoritma ini dapat menahan beberapa serangan manipulasi *robustness* seperti *cropping*. Penelitian yang pernah dilakukan Al-Afandy et al (4) dengan judul *High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography*, telah berhasil membuat modifikasi pada metode *LSB* dalam hal menangani masalah pada *cropping* dengan cara pada tiap bagian dari pesan teks disisipi ke dalam gambar terpotong dengan urutan rahasia menggunakan pendekatan *LSB*. Penyisipan dilakukan menggunakan *cover image* dari tiga *channel* warna. Pada simulasi yang dilakukan, gambar yang digunakan adalah gambar *JPEG* bewarna dengan ukuran 512 × 512, resolusi 96 × 96 dpi dan kedalaman bit 24. Beberapa tes yang diuji pada *stego image* diantaranya; tes visual untuk menentukan perubahan kualitas pada *stego image*, nilai *PSNR* dari *stego image* dan kompleksitas ekstraksi pesan rahasia. Penelitian ini mengusulkan cara penyembunyian rahasia yang sangat aman menggunakan *cropping image* dan *steganography LSB*. Hal ini berdasarkan pembagian pesan rahasia yang dibagi kedalam empat bagian dan mengekstrak keempat potongan dari *cover image* dengan koordinat rahasia khusus. Potongan disusun ulang dengan *cover image* menjadikan sebuah *stego-image*. Metode ini terbukti lebih aman dalam penyembunyian data dan tentunya lebih kompleks dalam ekstraksi data.

Penelitian lain yang terkait dalam memodifikasi metode *LSB* adalah yang dilakukan oleh Sur et al (24). Pendekatan baru ini yang diberi nama *Randomized cropping* dilakukan dengan cara mengkombinasikan metode *LSB* dan *pseudo random number generator (PRNG)*. *Randomized cropping* yang diimplementasikan dalam skema yang diusulkan, adalah seperti baris n dan kolom m dipotong dimana m dan n adalah dua integer bernilai positif. Sebagai contoh I dapat berupa sebuah matriks gambar $M \times N$ dengan baris M dan kolom N. Jika satu baris dipotong dari matriks, hasil matriks gambar berukuran $(M-1) \times N$. Setiap satu piksel dipotong dari lokasi yang berbeda dari tiap kolom, tanpa kehilangan sifat umumnya, operasi ini hampir sama dengan *cropping* satu baris dan menghasilkan matriks ($M-$

$1) \times N$. Lokasi dari tiap pixel yang dipotong untuk tiap kolom ditentukan dengan *PRNG* yang dapat menghasilkan urutan PRN dalam jangkauan $1 \ldots \ldots N$. Demikian pula, pada kolom dapat dipotong dari matriks $(M-1) \times N$ menggunakan urutan PRN dengan jangkauan $1 \ldots \ldots M-1$, menghasilkan matriks baru berukuran $(M-1) \times (N-1)$. Hasil dari urutan *pseudo random* ini akan dibagikan pesan rahasia kepada pengirim dan penerima. Hasil PRNG diketahui oleh penerima akhir, dikarenakan pixel dapat dipotong sebelum ekstraksi data dari gambar. Untuk sebuah gambar $M \times N$, distribusi spasial dari pixel gambar dapat disusun ulang dalam $M^N \times N^{M-1}$. Hasil penelitian yang dilakukan, *randomized cropping* digunakan dengan dimensi *cropping* $m = 2$ dan $n = 2$. Skema yang diajukan menggunakan daerah *Integer Wavelet* (IW) untuk penyisipan data. Daerah IW yang mana terlihat oleh *steganalyzers* berbeda dari daerah IW dimana penyisipan sebenarnya dilakukan karena pengacakan daerah penyisipan pesan. Secara intuitif, operasi yang diusulkan mengubah koefisien *integer wavelet*. Hal ini dapat diverifikasi secara eksperimental dengan mengalisis perbedaan diantara empat sub-kelompok yang didapatkan melalui penguraian IWT dari bagian gambar asli berukuran sama, kami mempertimbangkan bagian teratas dan paling kiri yang berukuran $[(M-2) \times (N-2)]$. Hasil eksperimen menunjukkan bahwa algoritma *randomized cropping* menghasilkan kinerja yang sangat baik serta dapat mengatasi serangan *steganalytic*.

Swain & Lenka (14) juga melakukan eksperimen modifikasi algoritma *LSB* dengan pendekatan baru yang diberi nama *A Novel Steganography Technique by Mapping Words with LSB Array*. Penelitian ini memodifikasi *LSB* menggunakan array dengan cara satu dari *LSB* array tersebut dipilih dan dibentuk berdasarkan panjang dari pesan rahasia. Ada dua cara yang digunakan yaitu algoritma penyisipan pesan yang digunakan pengirim dan algoritma ekstraksi pesan yang digunakan oleh penerima. Penelitian ini mencocokkan sebuah kata dengan *array LSB* berdasarkan algoritma yang dibuat. Metode ini menghasilkan dua tingkat keamanan yakni pada level *cryptography* dan pada level *steganography*. Pertama empat *array* yang sudah dipilih, kemudian kata-kata tersebut dipetakan, indeks dan panjang dienkripsi,

kemudian dikompresi dan disisipkan pada lokasi yang sudah ditentukan. Seluruh tahapan ini digabungkan sehingga membuat teknik ini lebih aman. Kapasitas penanaman pesan pun lebih baik. Tidak terlihat artefak visual yang terlihat pada *stego image*. Steganalisis seperti RS dan *Chi-square* tidak berhasil mendeteksi metode *steganography* ini.

Penelitian yang dilakukan oleh Wamiliana et al (25) membahas tentang *The Hybrid Method of Column Transposition With Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) using file jpg/jpeg and png*. Penelitian ini menggabungkan dua teknik pengamanan data menggunakan kriptografi dan steganografi dengan tujuan membuat keamanan berlapis sehingga semakin sedikit peluang data dicuri oleh pihak yang tidak berwenang. Penelitian ini menggunakan pesan rahasia berupa file berformat txt, sedangkan *cover image* berupa gambar berformat jpg dan png. Hasil dari penelitian ini menunjukkan bahwa *AMELSBR* berhasil menyembunyikan *file* dan memulihkan *file* yang telah disisipkan sebelumnya tanpa menyebabkan distorsi *(noise)* gambar *stego* yang berlebihan. Metode *Column Transposition* dapat mempengaruhi hasil manipulasi gambar seperti kecerahan dan kontras berubah dalam nilai piksel. Metode yang diterapkan tidak dapat melakukan ekstraksi data jika *stego image* dimasukkan ke dalam media sosial yang dapat mengkompresi citra dari *stego image*.

Penelitian selanjutnya terkait tentang *robustness* adalah penelitian yang dilakukan oleh Juarez-Sandoval et al (13) dengan judul *Cropping and Noise Resilient Steganography Algorithm using Secret Image Sharing*. Metode yang digunakan adalah *Secret Image Sharing (SIS)* yang memanfaatkan pengembangan dari metode *LSB*. Dari eksperimen yang dilakukan pada penelitian ini, didapatkan bahwa kualitas gambar yang diekstrak dari *stego-image* menunjukkan bahwa gambar yang diekstrak memiliki kualitas tinggi bahkan bila *stego image* mengalami *cropping* lebih dari 20%.

2.7 *Metadata* Gambar

Metadata merupakan kumpulan informasi dalam suatu *file* yang menjelaskan, mendeskripsikan terkait tentang data yang terkandung pada suatu *file* atau berkas digital (26). Lebih lanjut lagi, *metadata* dapat digunakan untuk keperluan manajemen data dalam suatu *database*. Pada jenis data berupa gambar, *metadata* mengandung informasi waktu pengambilan gambar, pengaturan kamera, dimensi piksel, ukuran gambar, dan informasi lainnya (27). Pada citra digital, terdapat suatu format standar untuk berkas/*file* gambar yang dihasilkan melalui kamera digital atau kamera *smartphone* yaitu *exchangeable image format* (*Exif*). *Exif* inilah yang menjadi *metadata* bagi *file* citra digital yang dapat merekam informasi penting mengenai sebuah *file*. Pemanfaatan *metadata* gambar pada era digital banyak dimanfaatkan untuk proses forensik dalam hal melihat rekam jejak data gambar atau terjadinya manipulasi atau perubahan pada gambar maka dapat diketahui melalui *metadata* (28). Selain itu, *metadata* gambar dapat juga dimanfaatkan untuk penyisipan pesan menggunakan steganografi (29). Beberapa penelitian yang memanfaatkan *exif image* untuk steganografi yaitu penelitian yang dilakukan oleh Araujo & Kazemian (30) yang membahas tentang steganografi menggunakan pendekatan *DSoBMP-I (Distributed Steganography over BMP faze I)* dalam hal peningkatan kapasitas menggunakan *cover* dengan format *BMP, JPG, PNG* dan *GID*. Sebelum pesan disisipkan ke *cover*, terlebih dahulu pesan dienkripsi menggunakan *RC4* dan *RSA*. Hasil eksperimen yang dilakukan membuktikan bahwa *cover* dengan format *BMP* dapat menghasilkan kapasitas penyimpanan yang lebih besar pada *file metadata*.

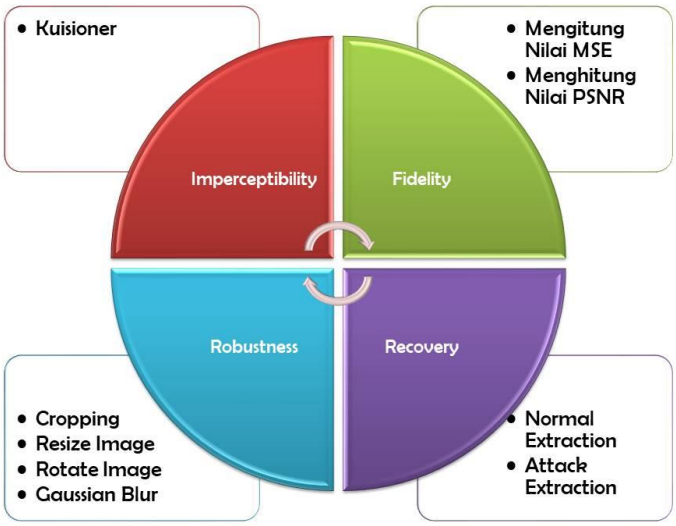
2.8 Kriptografi *Fernet*

Fernet cipher algorithm atau kriptografi *fernet* merupakan kriptografi dari salah satu paket pengembangan metode *Advance Encryption Standard (AES)* (31). *Fernet cipher* biasanya digunakan untuk membuat kunci *password* dan enkripsi yang tidak terlalu kompleks (32). Kriptografi *Fernet* ini sangat ideal untuk mengenkripsi data yang masuk pada *memory* atau *file* karena tidak mengekspos *byte* yang tidak diautentikasi. Kelemahan dari metode ini adalah tidak cocok untuk teks dengan

ukuran yang besar (*Big File*).

2.9 Pengujian Algoritma Steganografi

Teknik pengujian digunakan untuk membuat alur atau skenario pengujian terhadap implementasi metode yang diterapkan pada pemrograman yang digunakan. Teknik pengujian digambarkan dengan gambar kerangka yang menjelaskan bagaimana proses pengujian dari awal sampai dengan mendapatkan hasil penelitian yang diharapkan. Pengujian pada steganografi yang digunakan pada penelitian ini disajikan pada Gambar 2.6.



Gambar 2.6. Kerangka Pengujian Steganografi

Alur skenario pengujian:

1. *Imperceptibility*

Setelah data disisipkan pada suatu media, media yang menjadi *cover* tersebut seharusnya secara kasat mata terlihat sama dengan media yang sebelumnya belum disisipkan data (33). Dalam pengujian ini, akan melibatkan beberapa responden yang diminta untuk mengisi kuesioner. Responden akan diminta membedakan *stego image* dengan gambar asli *(cover image)*. Hasil kuesioner dihitung secara statistik dan ditentukan persentase tingkat *imperceptibility*.

2. Fidelity

Fidelity mengacu pada kemampuan untuk menguji gambar secara akurat, tanpa adanya distorsi visual atau hilangnya informasi (34). Pada proses ini akan dilakukan pengujian *fidelity* dengan mengukur nilai *Mean Square Error (MSE)* dan *Peak-Signal to Noise-Ratio (PSNR). PSNR* merupakan parameter yang digunakan mengukur kualitas citra yang dihasilkan (35). Metode *PSNR* adalah ukuran perbandingan antara nilai piksel *cover image* dengan nilai piksel pada citra *stego* yang dihasilkan (6). Sebelum menentukan *PSNR* terlebih dahulu ditentukan nilai rata-rata kuadrat *absolute error* antara *cover image* dengan citra *stego* yaitu nilai *MSE* (*Mean Square Error*) (6). Rumus yang digunakan untuk menghitung nilai *MSE* diberikan pada Persamaan 2.1.

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{X.Y}$$

Keterangan:

MSE_{AVG} = Nilai rata-rata *MSE cover image.*

MSE_R = Nilai *MSE* warna merah. …… (2.1)

MSE_G = Nilai *MSE* warna hijau.

MSE_B = Nilai *MSE* warna Biru.

$X.Y$ = Dimensi gambar.

Rumus atau formula yang digunakan untuk menghitung nilai *PSNR* terdapat pada Persamaan 2.2.

$$PSNR = 10_{log10}\left(\frac{255^2}{MSE}\right) \quad \text{…… (2.2)}$$

Keterangan:

$PNSR$ = Nilai *PSNR* citra digital.

MSE = Nilai *Mean Square Error* dari citra.

Citra *stego* dapat dikatakan berkualitas baik jika nilai *PSNR* dari citra *stego* tersebut bernilai tinggi (36). Tingkatan kualitas nilai *PSNR* berbanding terbalik dengan nilai

MSE, semakin tinggi nilai *PSNR* semakin rendah nilai *MSE*. Semakin tinggi kualitas yang dihasilkan dari citra *stego* maka semakin rendah nilai dari *MSE* (11).

3. *Robustness*

Robustness adalah ketahanan yang mengarah kepada data citra penampung (seperti dirubahnya kontras, penajaman, rotasi, perbesaran gambar, pemotongan dan sebagainya). Jika pada citra dilakukan operasi pengolahan citra, maka pada umumnya data yang tersembunyi akan mengalami kerusakan (13).

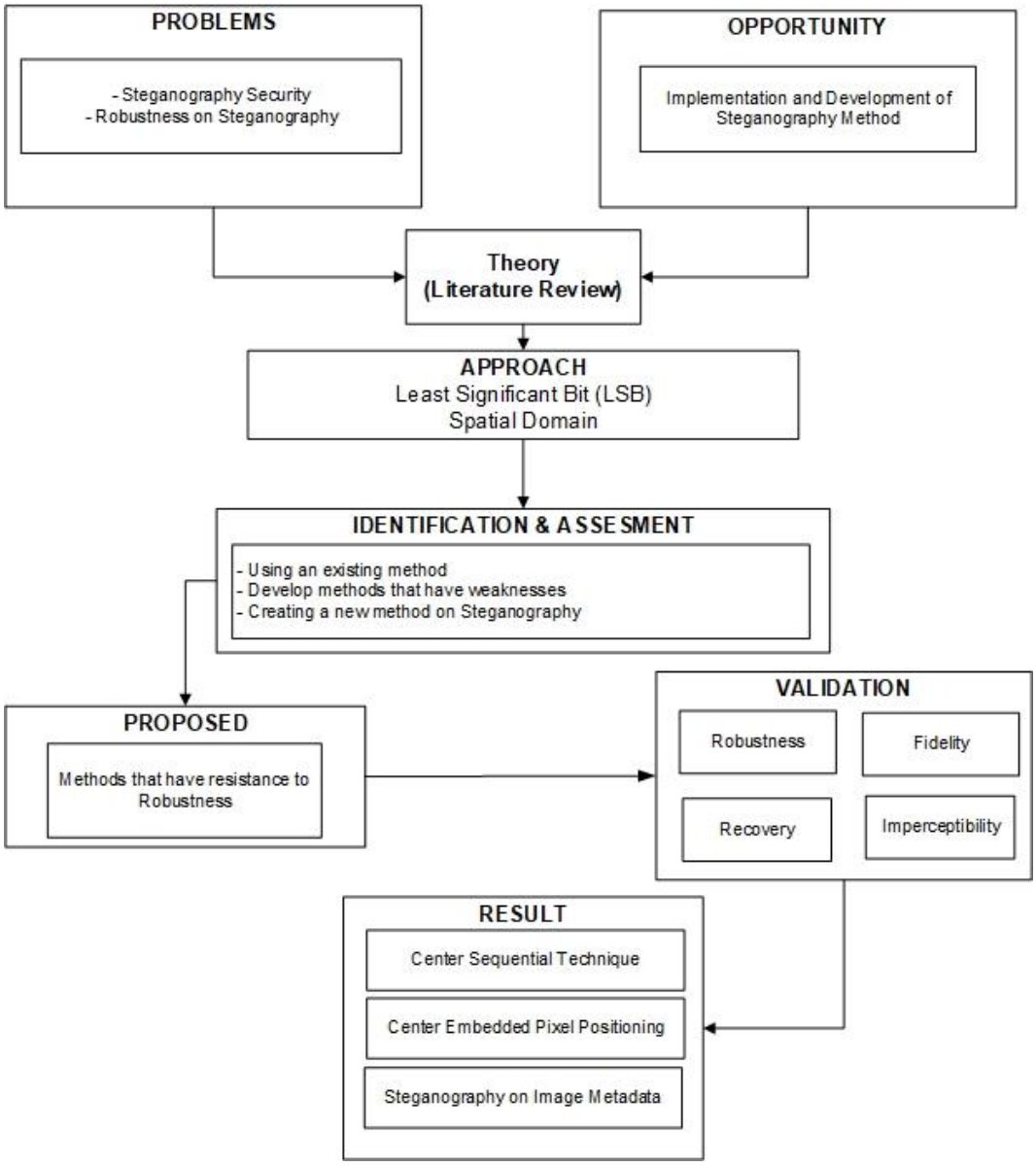
4. Recovery

Kemampuan steganografi dalam memulihkan data setelah proses ekstraksi data. Karena tujuan steganografi adalah menyembunyikan informasi, maka pesan rahasia di dalam *stegano image* harus dapat diambil kembali untuk digunakan lebih lanjut (9).

BAB III
METODE PENELITIAN

3.1 Kerangka Penelitian

Kerangka penelitian pada dasarnya adalah kerangka hubungan antara konsep-konsep yang akan diamati atau diukur melalui penelitian yang dilakukan. Berikut kerangka penelitian yang digunakan dapat dilihat pada Gambar 3.1.



Gambar 3.1 Kerangka Penelitian

Penjelasan Gambar 3.1 untuk kerangka penelitian:

1. *Problems* (Masalah)

   Masalah inti yang terdapat pada penelitian ini adalah keamanan steganografi dan serangan pada *robustness* yang meliputi *cropping, image rotation, image resize* dan *gaussian blur*. Penelitian ini difokuskan pada penyelesaian permasalahan tersebut.

2. *Opportunity* (Kesempatan)

   Kesempatan yang dapat dilakukan pada penelitian ini adalah dengan mempelajari metode yang sudah ada pada steganografi dan mengamati kelemahan-kelemahan dari metode tersebut. Selanjutnya, melakukan pengembangan untuk menyelesaikan permasalahan *robustness* pada steganografi dengan mengumpulkan semua literatur yang berhubungan dengan metode dan algoritma yang digunakan.

3. *Approach* (Pendekatan)

   Pendekatan yang dilakukan adalah berdasarkan hasil analisis metode utama dan pendukung yaitu metode *Least Significant Bit,* dengan memanfaatkan domain spasial pada proses penyisipan pesan.

4. *Identification & Assesment* (Identifikasi & Tujuan)

   Identifikasi yang dilakukan adalah menggunakan dan mengembangkan metode yang sudah ada. Tujuannya adalah untuk menciptakan metode baru atau pendekatan baru pada steganografi dalam hal mengamankan data dari manipulasi *robustness*.

5. *Proposed* (Usulan)

   Usulan yang diajukan adalah meningkatkan *robustness* terhadap serangan *cropping, image rotation, resize image,* dan *gaussian blur* dengan menggunakan metode yang dikembangkan.

6. *Validation* (Pengujian)

   Pengujian yang dilakukan adalah pengujian manual diantaranya *robustness, imperceptibility, fidelity* dan *recovery*.

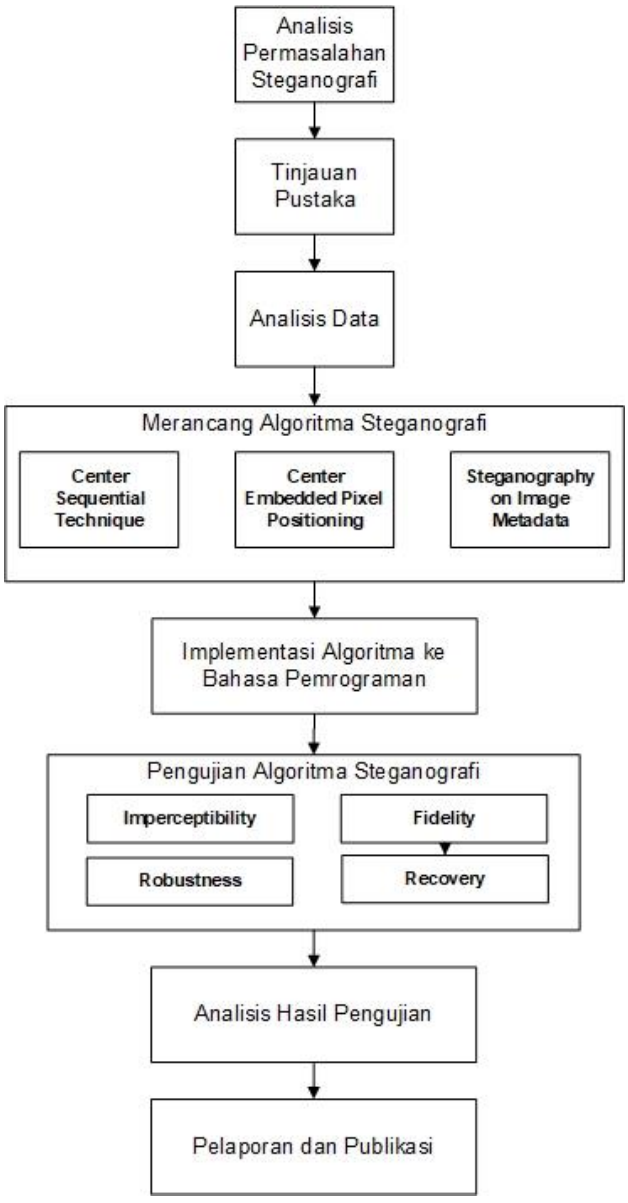
7. *Result* (Hasil)

   Hasil dari penelitian ini adalah implementasi metode yang dikembangkan

untuk meningkatkan ketahanan *stego image* terhadap serangan *robustness.* Penulis mengusulkan tiga pendekatan baru yaitu: *Center Sequential Technique, Center Embedded Pixel Positioning, Steganography on Image Metadata.*

3.2 Tahapan Penelitian

Penelitian ini terdiri dari beberapa tahapan dimulai dari analisis data sampai dengan publikasi. Gambar 3.2 adalah tahapan penelitian yang dilakukan selama proses penyelesaian disertasi.



Gambar 3.2 Tahapan Penelitian

Penjelasan Gambar 3.2 untuk tahapan penelitian:

1. Analisis Permasalahan Steganografi

   Tahap awal dari penelitian ini adalah melakukan analisis terhadap permasalahan pada keamanan steganografi. *Robustness* merupakan salah satu permasalahan pada keamanan steganografi. Pada penelitian ini fokus permasalahan adalah untuk menyelesaikan permasalahan keamanan steganografi pada manipulasi *robustness* namun tetap memperhatikan aspek *imperceptibility* dan *fidelity*.

2. Tinjauan Pustaka

   Selanjutnya pada tahapan penelitian ini adalah melakukan studi pustaka yang berkaitan dengan konsep penerapan steganografi dalam hal keamanan *stego image* dan manipulasi *robustness*, lalu mempelajari bagaimana cara metode bekerja dan memahami kelemahan-kelemahan pada metode tersebut untuk dikembangkan dan disempurnakan kembali.

3. Analisis Data

   Langkah ini bertujuan untuk mengetahui bagaimana jenis-jenis pesan yang akan diamankan, dalam penelitian ini sampel data yang akan diambil adalah berupa pesan rahasia dalam bentuk file *txt*, gambar dengan jenis citra *grayscale* dan *RGB*, sedangkan untuk *cover image* diambil dari gambar dengan format *PNG* dan *JPG* dengan jenis gambar *grayscale* dan *RGB*.

4. Merancang Algoritma Steganografi

   Langkah selanjutnya adalah membuat rancangan yang berkaitan dengan penerapan Steganografi. Perancangan dibuat dalam bentuk *flowchart* dan *pseudocode* untuk menggambarkan bagaimana langkah-langkah pada algoritma yang digunakan, dan perhitungan matematis yang digunakan dalam rancangan steganografi. Rancangan algoritma yang diusulkan dibuat secara terpisah dengan urutan *Center Sequential Technique, Center Embedded Pixel Positioning, dan Steganograpy on Image Metadata.*

5. Implementasi Algoritma ke Bahasa Pemrograman

   Setelah algoritma baru yang diusulkan telah selesai dirancang, tahapan selanjutnya adalah menerjemahkan hasil rancangan algoritma tersebut ke

dalam bahasa pemrograman. Bahasa pemrograman yang digunakan adalah Python 3.7.

6. Pengujian Algoritma Steganografi

   Pada tahap ini peneliti melakukan simulasi dan pengujian yaitu dengan menggunakan citra dan teks yang akan diamankan. Berikut ini adalah kondisi yang akan disimulasikan dan diujikan oleh peneliti:

   a. Menyiapkan Data

      Menyiapkan data berupa informasi yang akan dikirim kepada penerima dalam bentuk file *txt* dan *image*.

   b. Menguji *Encoding* Steganografi

      Tahap ini adalah proses memasukkan pesan rahasia ke dalam *cover image*. Pengujian akan dilakukan setelah memasukan data. Selanjutnya memasukkan gambar berupa pesan rahasia ke dalam *cover image*. Setelah berhasil maka akan dilakukan pengujian dengan memperhatikan 4 aspek yaitu:

      1) Imperceptibility

         Aspek *imperceptibility* digunakan untuk mengetahui seberapa mudah *stego-image* dapat terdeteksi oleh inderawi manusia. Pengujian ini dilakukan secara manual dengan melibatkan responden, kemudian dihitung berapa persentase untuk citra yang mengalami perubahan, sedikit perubahan dan tidak ada perubahan.

      2) Fidelity

         Pengujian *fidelity* mengacu terhadap perubahan nilai piksel setelah disisipkan pesan. Pengujian *fidelity* dapat dilakukan dengan mengukur nilai *MSE (Mean Square Error)* dan *PSNR (Peak Signal to Noise Ratio)*, di mana keduanya memiliki satuan *db (desibels)*. Semakin rendah nilai *MSE* maka kualitas citra semakin baik.

      3) Pengujian *Recovery*

         Pengujian *recovery* merupakan proses *decoding* pada steganografi. Sebuah citra harus dapat dipisahkan dari *stego-image*-nya. Pengujian

dapat dilakukan dengan melihat keutuhan pesan yang diekstraksi dengan pesan yang asli.

4) Pengujian *Robustness*

Pengujian *robustness* merupakan inti dari pengujian yang dilakukan yaitu melakukan serangan dengan cara *cropping, image rotation, resize image* dan *gaussian blur* lalu melakukan ekstraksi *stego image* dan memastikan apakah pesan rahasia dapat diambil kembali dari *stego image*.

7. Analisis Hasil Pengujian

Pada tahapan ini akan dilakukan pengamatan dan evaluasi berdasarkan hasil pengujian yang sudah dilakukan dengan berbagai jenis serangan. Hasil pengujian ditampilkan dalam bentuk gambar dan atau grafik.

8. Pelaporan dan Publikasi

Tahapan ini bertujuan mendokumentasikan semua hasil dari penelitian dan pelaporan dalam bentuk disertasi serta mempublikasikan dalam bentuk jurnal dan prosiding.

3.3 Metode Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian ini yaitu sebagai berikut:

1. Tinjauan Pustaka

Dalam penelitian ini, metode kepustakaan yang dilakukan dengan cara membaca buku-buku yang berhubungan dengan steganografi, keamanan data, dan penyembunyian data, serta dengan mempelajari jurnal-jurnal dan prosiding hasil penelitian.

2. Dokumentasi (*Documentation*)

Pada proses pengumpulan data menggunakan metode dokumentasi kegiatan yang dilakukan adalah dengan cara membaca, mencatat, mengutip, dan mengumpulkan data-data secara teoritis dari buku-buku dan internet sebagai landasan penyusunan penelitian.

3. Observasi Pengumpulan Gambar

Dalam penelitian ini, dilakukan pengumpulan gambar-gambar yang akan dipakai untuk menguji algoritma yang akan dikembangkan. Gambar-gambar

yang digunakan adalah gambar primer (yang diambil sendiri oleh peneliti) dan gambar sekunder (gambar digital yang berasal dari internet atau media elektronik lain).

3.4 Kebutuhan *Software* dan *Hardware*

Program yang digunakan untuk melakukan eksperimen penelitian adalah Bahasa Pemrograman *Python 3.7* dengan spesifikasi *hardware* yang digunakan adalah komputer minimal *intel processor core i3* dengan penggunaan *memory RAM* minimal 4 GB.

3.5 Kerangka Pengujian

Kerangka pengujian digunakan untuk membuat alur atau skenario pengujian terhadap implementasi metode yang diterapkan pada pemrograman yang digunakan. Pada kerangka pengujian ini juga dijelaskan bagaimana proses pengujian dari awal sampai dengan mendapatkan hasil penelitian yang diharapkan. Berikut ini merupakan rencana alur pengujian yang akan dilakukan :

1. *Imperceptibility*

   Dalam pengujian ini, dilibatkan beberapa responden yang diminta untuk mengisi kuesioner. Responden akan diminta membedakan *stego image* dengan gambar asli *(cover image)*. Hasil kuesioner dihitung secara statistik dan ditentukan persentase tingkat *imperceptibility*. Format pertanyaan yang akan diberikan kepada responden dapat dilihat pada Tabel 3.1.

Tabel 3.1 Format Pertanyaan untuk Pengujian *Imperceptibility*

Cover Image	*Stego Image*	Hasil Pengamatan		
		Berbeda	Sedikit Berbeda	Tidak Ada Perbedaan
Cover Image 1	*Stego Image 1*	?	?	?
…….	…….	?	?	?
Cover Image n	*Stego Image n*	?	?	?

2. *Fidelity*

Skenario pengujian *fidelity* diambil dengan menghitung nilai *MSE* untuk kemudian dilakukan perhitungan nilai *PSNR*. Proses perhitungan nilai *MSE* dan *PSNR* menggunakan fungsi dan *library* yang ada pada *python*. Skenario pengujian *fidelity* dapat dilihat pada Tabel 3.2.

Tabel 3.2 Skenario Pengujian *Fidelity*

Cover Image	***MSE***	***PSNR***
Cover Image 1	?	?
…….	?	?
Cover Image n	?	?

3. *Robustness*

Steganografi seharusnya tahan terhadap serangan berbentuk *steganalysis* dan/atau manipulasi gambar (37). Pengujian *robustness* akan dilakukan dengan cara menyerang *stego image* dengan serangan-serangan *image processing* seperti *cropping, image resize, image rotation* dan lain-lain. Kemudian data diekstraksi untuk diketahui apakah tetap utuh atau rusak. Bila data yang diekstrak tetap utuh maka tingkat ketahanan data baik begitu pula sebaliknya. Skenario pengujian yang dilakukan untuk *robustness* dapat dilihat pada Tabel 3.3 hingga Tabel 3.6.

Tabel 3.3 Skenario Pengujian *Robustness (Cropping)*

Stego Image	**Posisi Pemangkasan Gambar**	**Persentase Pemangkasan Gambar**	**Hasil Ekstraksi**
Stego Image	Kiri	?	?
Stego Image	Kanan	?	?
Stego Image	Atas	?	?
Stego Image	Bawah	?	?
Stego Image	Semua Posisi	?	?

Tabel 3.4 Skenario Pengujian *Robustness (Image Resize)*

Stego Image	**Persentase *Resize***	**Hasil Ekstraksi**
Stego Image 1	?	?
….	?	?
Stego Image n	?	?

Tabel 3.5 Skenario Pengujian *Robustness (Image Rotation)*

Stego Image	**Jenis Rotasi**	**Hasil Ekstraksi**
Stego Image	Rotasi ke kanan 90 derajat	?
Stego Image	Rotasi ke kiri 90 derajat	?
Stego Image	*Flip Vertical*	?
Stego Image	*Flip Horizontal*	?

BAB IV
CENTER SEQUENTIAL TECHNIQUE

4.1 Metode *Center Sequential Technique*

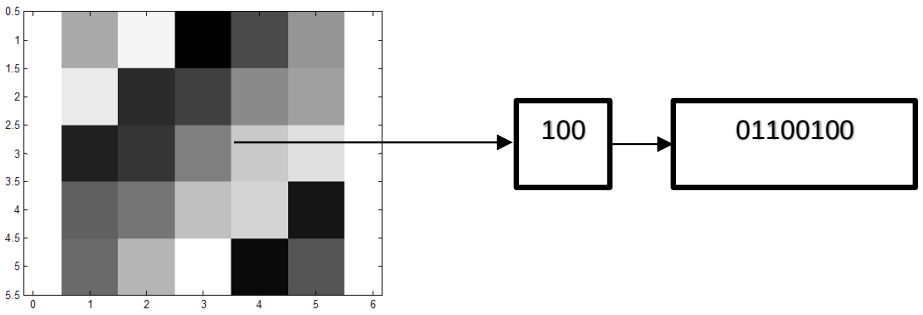
Ide awal dari penelitian ini adalah bagaimana memanfaatkan domain spasial pada *cover image* secara sekuensial pada saat penyisipan pesan. Pada dasarnya terdapat dua pendekatan pada domain spasial pada proses penyisipan pesan yaitu secara acak (*random*) atau secara berurutan (*sequentia*l). Metode baru yang diusulkan bertujuan untuk menangani salah satu masalah dari steganografi gambar yaitu *robustness* khususnya pada manipulasi *cropping*. Metode yang dikembangkan berfokus pada gambar dengan format *grayscale* untuk *cover image* maupun gambar pesan karena jenis gambar *grayscale* lebih mudah dibandingkan jenis gambar *RGB* dalam hal pengelolaan citra. Pada gambar *grayscale* pembacaan piksel hanya dilakukan pada satu kanal warna yang nilai intensitas pikselnya didasarkan pada derajat keabuan. Pada citra *grayscale* 8-*bit*, derajat warna hitam sampai dengan putih dibagi ke dalam 256 derajat keabuan di mana warna putih sempurna direpresentasikan dengan nilai 255 dan hitam sempurna dengan nilai 0.

Penyisipan pesan dilakukan dengan cara sekuensial yaitu gambar pesan dalam bentuk bit ditanamkan pada posisi tengah gambar *cover* dengan menghitung panjang dan lebar dari gambar *cover* yang digunakan sehingga metode ini diberi nama *Center Sequential Technique (CST)*. Posisi *center* atau posisi tengah gambar yang dimaksud pada metode ini adalah berdasarkan ukuran piksel citra yaitu lebar dan tinggi citra. Posisi *center* bukan berdasarkan makna gambar pada suatu citra.

Hasil dari penelitian yang dikembangkan menggunakan metode *CST* ini telah dipublikasikan pada ***Journal of Physics: Conference Series***, pada tahun 2019. Judul artikel pada prosiding tersebut adalah "***A New Approach of Steganography Using Center Sequential Technique***".

Secara umum cara kerja dari algoritma *Center Sequential Technique* adalah sebagai berikut:

1. Membaca ukuran gambar *cover* dan gambar rahasia.
2. Melakukan pengecekan apakah ukuran gambar pesan lebih besar dari ukuran gambar *cover.*
3. Memetakan piksel dari kedua gambar untuk dipisah antara area penyisipan pesan di tengah *cover image* (kontainer gambar) dan di luar area kontainer dengan ketentuan nilai area di luar kontainer pada akhir bit diubah menjadi 0, dan area di dalam kontainer menjadi 1.
4. Membuat sebuah gambar sementara untuk digunakan sebagai gambar *output* dengan mengubah nilai-nilai tiap piksel pada gambar *cover* dan pesan ke dalam bentuk biner seperti yang ada pada Gambar 4.1.



Gambar 4.1 Ekuivalen Nilai Piksel dengan Biner

5. Menentukan koordinat penanaman gambar pesan ke tengah gambar *cover*, sehingga gambar pesan selalu berada pada posisi tengah gambar *cover* dengan syarat ukuran gambar pesan lebih kecil dari ukuran gambar *cover*. Dengan menentukan $x_{start}, x_{end}, y_{start},$ dan y_{end} melalui lebar dan tinggi gambar *cover* (w, h) dan gambar pesan (x, y). Untuk menentukan posisi gambar pesan yang diletakkan pada gambar *cover* pada proses penyisipan menggunakan persamaan 4.1 dan 4.2.

$$x_{start} = \left(\frac{1}{2} \times w\right) - \left(\frac{1}{2} \times x\right) \ , \ x_{end} = \left(\frac{1}{2} \times w\right) + \left(\frac{1}{2} \times x\right) \qquad \ldots\ldots (4.1)$$

$$y_{start} = \left(\frac{1}{2} \times h\right) - \left(\frac{1}{2} \times y\right) \ , \ y_{end} = \left(\frac{1}{2} \times h\right) + \left(\frac{1}{2} \times y\right) \qquad \ldots\ldots (4.2)$$

Keterangan :

$w =$ lebar gambar *cover*

$h =$ tinggi gambar *cover*

$x =$ lebar gambar pesan

$y =$ tinggi gambar pesan

$x_{start} =$ titik awal pesan disisipkan dari lebar gambar *cover*

$x_{end} =$ titik akhir pesan disisipkan dari lebar gambar *cover*

$y_{start} =$ titik awal pesan disisipkan dari tinggi gambar *cover*

$y_{end} =$ titik akhir pesan disisipkan dari tinggi gambar *cover*

4.2 Implementasi Metode *CST*

4.2.1 Algoritma Penyisipan Pesan

Pada Persamaan 4.1 dan 4.2 merupakan proses penentuan nilai awal dan nilai akhir batas area tempat penyisipan gambar pesan. Berikut ini merupakan potongan dari *pseudocode* dari alur proses penyisipan pesan menggunakan metode *CST*.

Pseudocode Penyisipan Pesan Metode CST:

```
function merge (cover, secret)
  if secret > cover (pixel column) or secret > cover (pixel
  row) then
  begin
    warning ← ('Image 1 size is lower than image 2 size!')
  end
  else
  begin
    pixel_map1 ← cover load
    pixel_map2 ← secret load
    new_image ← image.new (cover, secret)
    pixel_new ← new_image
    if secret[1] mod 2 = 0
    begin
      secret_height ← secret[1] +1
    end
    else
    begin
      secret_height ← secret[1]
    end
    n ← 0
    m ← 0
    x_start ← (cover[0] / 2) – (secret[0]/2)
    x_end ← (cover[0] / 2) – (secret[0]/2)
    y_start ← (cover[1] / 2) – (secret[1]/2)
```

```
     y_end ← (cover[1] / 2) – (secret[1]/2)
end function
```

Proses pertama dilakukan untuk pembacaan *cover image* dan gambar pesan. Jika ukuran dimensi gambar pesan 50% > *cover image*, maka proses penyisipan pesan tidak dapat dilakukan. Setelah pengecekan *cover image* dan gambar pesan selesai dilakukan, selanjutnya adalah proses menentukan koordinat tengah untuk wadah penampung gambar pesan. Penyisipan ini menggunakan metode *LSB* dengan cara mengubah semua bit menjadi '0' yang berada pada luar area kontainer, dan semua bit menjadi '1' pada wilayah area kontainer pesan yang berada di tengah.

4.2.2 Algoritma Ekstraksi Pesan

Proses ekstraksi pesan dilakukan dengan cara membaca area kontainer pesan yang memiliki bit *LSB* dengan nilai '1'. Tujuan dibuat penanda melalui perubahan nilai bit '0' dan '1' adalah pada saat proses *cropping stego-image*, pesan masih dapat diekstraksi dengan syarat bit yang dipotong adalah di wilayah area bit '0'. Berikut ini merupakan potongan *pseudocede* pada proses ekstraksi pesan.

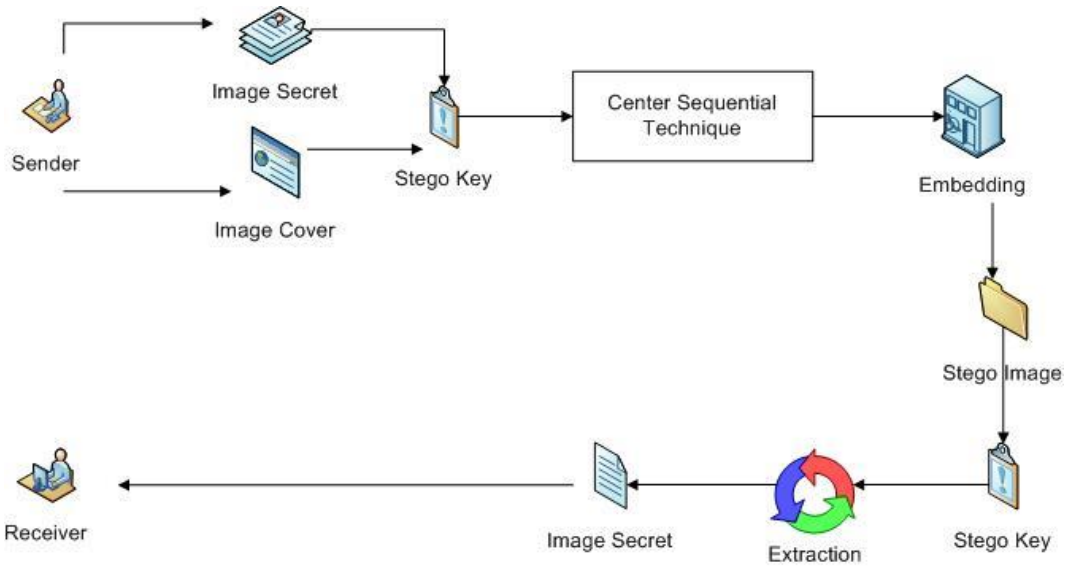
Pseudocode Ekstraksi Pesan Metode CST:

```
function unmerge (img)
   pixel_map ← img
   new_image ← image.new(img)
   original_size ← img.size
   for i to range img.size[0]
   begin
     for j to range img.size[1]
     begin
       l,a ← covert integer to binary (pixel_map[i,j])
       extr ← (l[4:]+ "0000", a[4:] + "0000")
       pixel_new ← i,j, convert binart to integer[i,j]
     end
   end
end function
```

4.3 Pembahasan

4.3.1 Model Algoritma *CST*

Setiap algoritma steganografi yang digunakan pasti memiliki model sendiri untuk melakukan proses penyisipan dan ekstraksi data pada *cover image* yang digunakan. Hal ini nantinya akan menentukan kualitas dari citra yang digunakan sebagai *stego-image*. Penelitian ini mengusulkan model dan teknik baru pada steganografi dengan cara meletakkan piksel gambar rahasia ke posisi tengah gambar *cover* sehingga jika dilakukan pemangkasan pada *stego-image* maka gambar rahasia akan tetap utuh ketika proses *recovery*.



Gambar 4.2. Model Algoritma *Center Sequential Technique*

Gambar 4.2 merupakan model yang dibuat pada teknik Steganografi *Center Sequential Technique*. Berikut penjelasan dari model yang dikembangkan:

1. Pengirim pesan rahasia menyiapkan *cover image* dan *secret image* dengan syarat *secret image* memiliki ukuran yang lebih kecil dari *cover image*;
2. Menentukan *stego-key* yang dijadikan sebagai acuan pada saat proses ekstraksi. Untuk *stego-key* yang digunakan adalah berdasarkan ukuran dimensi dari *secret image*;

3. Setelah menentukan *stego key* proses selanjutnya adalah menerapkan algoritma *Center Sequential Technique* untuk menggabungkan *cover image* dan *secret image*;
4. Proses *extraction* dilakukan dengan cara membaca *stego-key*, jika sesuai maka akan menghasilkan *secret image* sesuai dengan yang dikirimkan oleh pengirim.

4.4 Hasil Pengujian

4.4.1 Proses Penyisipan Pesan

Proses penyisipan pesan pada metode yang diterapkan menggunakan gambar jenis *grayscale* dengan format *PNG* sebagai *cover image*. *PNG* merupakan singkatan dari *Portable Network Graphics*. Format *PNG* dipilih sebagai *cover image* karena memiliki kemampuan *lossless compression* yang mendukung citra asli dapat disusun kembali seperti semula setelah disisipkan pesan. Format *PNG* juga mendukung aktivitas perpindahan citra yang dilakukan melalui *website* atau jaringan. Contoh citra yang akan digunakan pada penelitian ini yaitu citra *lenna.png* dan *pepper.png*. Citra tersebut dipilih karena telah umum digunakan oleh peneliti-peneliti sebelumnya pada saat uji coba metode pengolahan citra digital terutama pada steganografi gambar. Berikut ini pada Gambar 4.3 merupakan citra yang digunakan untuk *cover image* pada uji coba penyisipan pesan.

lenna.png

pepper.png

Gambar 4.3 *Cover Image*

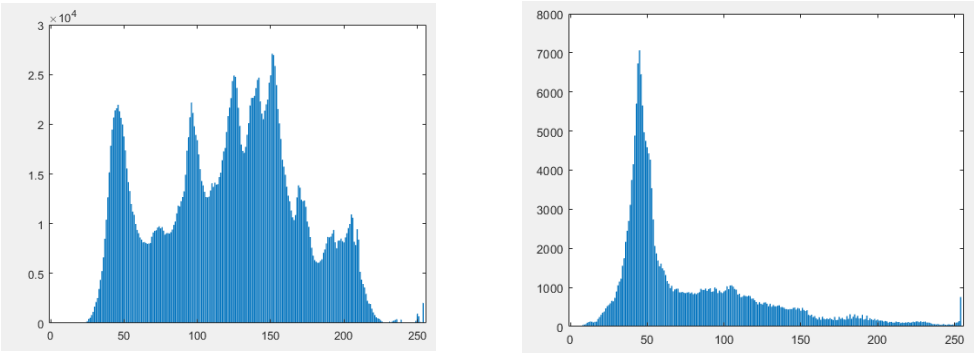
Pesan yang disisipkan ke dalam *cover image* berupa citra dengan format yang sama yaitu *PNG*. Gambar rahasia (*secret image*) menggunakan dua variasi ukuran gambar yang berbeda. Hal ini dilakukan untuk membandingkan komposisi ukuran

stego image dan *cover image*. Berikut ini pada Tabel 4.1 merupakan komposisi perbandingan antara *cover image* dan *stego image* pada proses penyisipan pesan.

Tabel 4.1. Komposisi Perbandingan *Cover Image* dan *Stego Image*

Cover Image	Ukuran *Cover Image (KB)*	Ukuran *Secret Image (KB)*	Ukuran *Stego Image (KB)*
lenna1.png	572	1	590
lenna2.png	572	8,51	594
pepper1.png	156	1	70,4
pepper2.png	156	8,51	70,4

Pada *cover image lenna1.png* dan *lenna2.png*, *stego image* mengalami peningkatan ukuran baik menggunakan ukuran *secret image* yang kecil maupun *ukuran secret image* yang lebih besar. Sedangkan pada *cover image pepper1.png* dan *pepper2.png*, ukuran *stego image* mengalami penurunan. Meningkat dan menurunnya ukuran *stego image* berdasarkan sebaran nilai intensitas pada *cover image*. Jika sebaran nilai intensitas yang merata pada derajat keabuan, maka ukuran *stego image* akan semakin meningkat. Jika sebaran nilai intensitas tidak merata maka ukuran *stego image* akan menjadi lebih kecil. Berikut pada Gambar 4.4 adalah *histogram* yang dihasilkan pada gambar *lenna.png* dan *pepper.png*.



lenna.png *pepper.png*

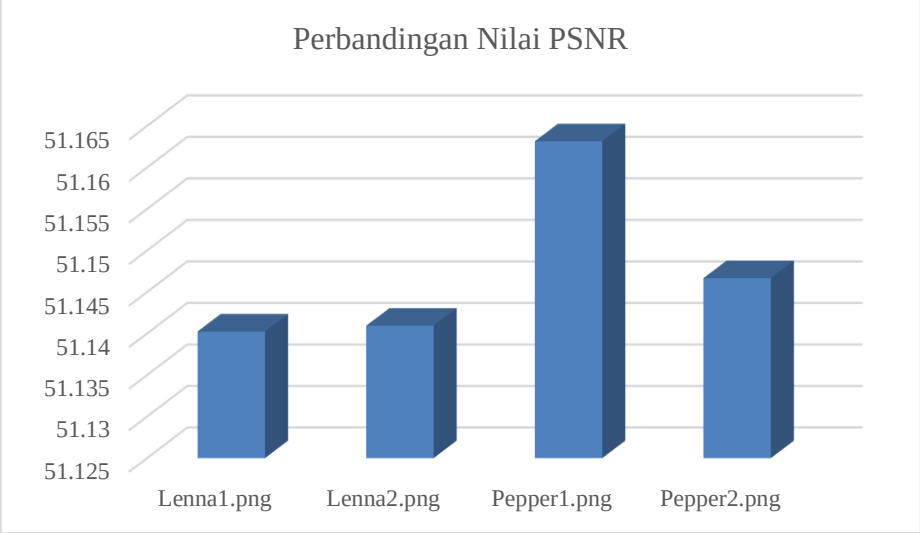
Gambar 4.4 Perbandingan Nilai Intensitas *Stego Image*

4.4.2 Pengujian *Fidelity*

Pengujian *fidelity* digunakan untuk mengukur kualitas citra dengan membandingkan citra asli (*cover image*) dengan citra yang telah disisipi pesan (*stego-image*). Pengujian dilakukan dengan cara menghitung nilai *Peak-Signal to Noise-Ratio (PSNR).*

Tabel 4.2. Hasil Uji Nilai *PSNR*

Stego Image	*PSNR (db)*
lenna1.png	51,14025152
lenna2.png	51,14094615
pepper1.png	51,16316048
pepper1.png	51,14667365



Gambar 4.5. Perbandingan Nilai *PSNR* pada *Stego Image*

Hasil uji pada Tabel 4.2, dan Gambar 4.5 menunjukkan nilai perbandingan *PSNR* pada *cover image*. Nilai *PSNR* tertinggi adalah pada *cover image pepper1.png*, nilai *PSNR* terendah adalah pada *cover image lenna1.png*, sedangkan nilai rata-rata *PSNR* yang didapat pada *cover image* tersebut adalah 51,14776. Metode *CST* yang dikembangkan pada penelitian ini menghasilkan nilai *PSNR* lebih dari 40db. Hal ini menunjukkan bahwa *stego-image* menggunakan metode *CST* menghasilkan

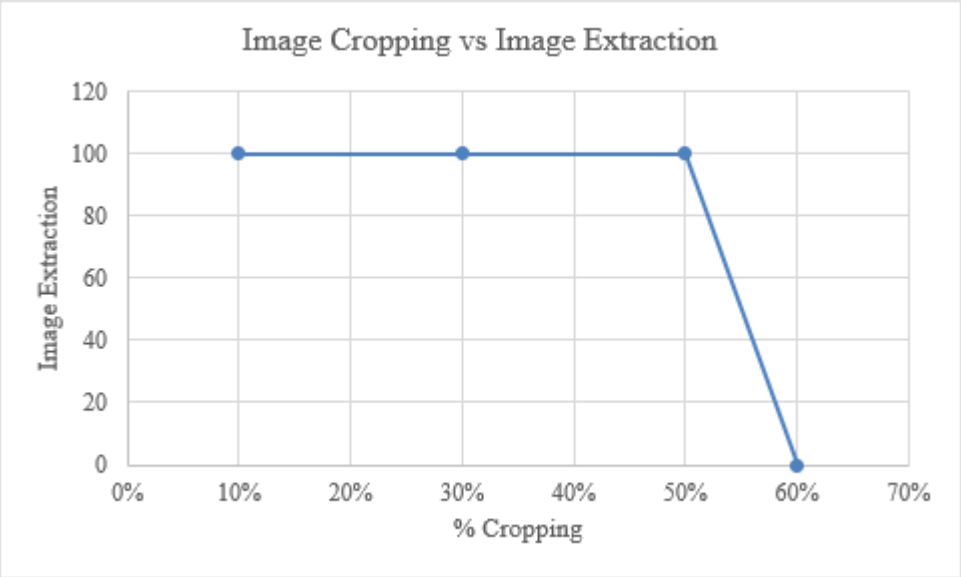
kualitas citra yang baik, sehingga gambar yang sudah disisipkan pesan tidak mengalami perubahan secara signifikan.

4.4.3 Pengujian *Robustness*

Uji coba pada bagian ini adalah inti dari penelitian yang dilakukan, uji coba *robustness* dilakukan dengan cara menyerang *stego-image* melalui *cropping* gambar dari berbagai posisi lalu dilakukan ekstraksi pada *stego-image* untuk melihat apakah gambar rahasia masih dapat diekstraksi atau tidak.

Tabel 4.3. Hasil Uji *Cropping*

Stego-image	*Crop Position*	*% Crop*	*Extraction*
lenna1.png	*Left*	10	*Success*
lenna1.png	*Right*	10	*Success*
lenna1.png	*Bottom*	10	*Success*
lenna1.png	*Top*	10	*Success*
lenna1.png	*All Position*	10	*Success*
lenna1.png	*Left*	30	*Success*
lenna1.png	*Right*	30	*Success*
lenna1.png	*Bottom*	30	*Success*
lenna1.png	*Top*	30	*Success*
lenna1.png	*All Position*	30	*Success*
lenna1.png	*Left*	50	*Success*
lenna1.png	*Right*	50	*Success*
lenna1.png	*Bottom*	50	*Success*
lenna1.png	*Top*	50	*Success*
lenna1.png	*All Position*	50	*Success*
lenna1.png	*Left*	>=60	*Fail*
lenna1.png	*Right*	>=60	*Fali*
lenna1.png	*Bottom*	>=60	*Fail*
lenna1.png	*Top*	>=60	*Fail*
lenna1.png	*All Position*	>=60	*Fail*



Gambar 4.6. Hasil Uji *Cropping*

Hasil uji pada Tabel 4.3 dan Gambar 4.6 menunjukkan bahwa gambar pada *stego-image* dapat dilakukan pemangkasan dari kiri, kanan, atas, bawah dan semua posisi pemangkasan. Metode baru yang diusulkan dapat membuktikan bahwa *stego-image* menggunakan metode *Center Sequential Technique* dapat dilakukan proses ekstraksi meskipun sudah dilakukan serangan *cropping* sampai dengan 50%, namun proses ekstraksi tidak dapat dilakukan jika serangan *cropping* sampai dengan lebih dari 60% hal ini disebabkan karena gambar pesan yang ditanam pada *cover image* ada di posisi tengah sehingga gambar pesan akan ikut terpotong dan tidak dapat diekstraksi.

4.5 Evaluasi Hasil Pengujian

Berdasarkan hasil pembahasan dan pengujian yang dilakukan, maka dapat disimpulkan bahwa metode steganografi *Center Sequential Technique* dapat diterapkan pada steganografi gambar, hal ini dibuktikan dari berhasilnya proses penyisipan dan ekstraksi gambar pesan pada *stego image*. Kemudian, kualitas citra yang dihasilkan dari metode *Center Sequential Technique* memiliki nilai *PSNR* yang baik, yaitu lebih dari 50 db.

Metode yang dikembangkan juga memiliki ketahanan terhadap serangan *cropping* dari posisi kiri, kanan, tengah, atas dan semua posisi dan memiliki ketahanan *ratio cropping* lebih dari 50%. Kelemahan dari metode ini adalah hanya dapat menampung *cover image* jenis *grayscale.*

BAB VII
KESIMPULAN DAN SARAN

7.1 Kesimpulan

Metode yang dikembangkan pada penelitian ini difokuskan pada ketahanan *stego image* terhadap manipulasi *robustness.* Pendekatan yang dilakukan adalah dengan memanfaatkan metode *LSB,* domain spasial, *exif image metadata* dan kriptografi *fernet*. Dari hasil penelitian didapat tiga metode yang yaitu: *Center Sequential Technique (CST), Center Embedded Pixel Positioning (CEPP)* dan *Steganography on Image Metadata (SIM).*

Metode *CST, CEPP* dan *SIM* dapat mengatasi manipulasi *cropping* lebih dari 50% secara simetri dan asimetri. Namun, metode *CST* dan *CEPP* tidak dapat menahan manipulasi untuk *rotate, resize* dan pemberian efek warna pada gambar. Kelemahan dari *CST* dan *CEPP*, diperbaiki dengan metode *SIM*. Berdasarkan hasil uji yang dilakukan, pada metode SIM dapat menahan serangan *resize, rotate* dan pemberian efek warna pada gambar.

Kualitas citra yang dihasilkan oleh metode yang telah dikembangkan tidak mempengaruhi secara signifikan terhadap *stego image* yang dihasilkan. Berdasarkan hasil uji 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, dan sedangkan untuk metode SIM, nilai *PSNR* mencapai 100 db.

7.2 Saran

1) Pada metode *CST* dan *CEPP* perlu dilakukan pengembangan dalam hal membedakan antara bit *LSB* pada area di luar kontainer pesan (bit ‘0’) dan area di dalam kontainer pesan (bit ‘1’) karena steganalisis dapat menemukan area penyisipan pesan rahasia.
2) Pada penelitian selanjutnya dapat dilakukan penyisipan pesan tidak hanya pada *“center”* berdasarkan *“ukuran”* gambarnya saja, tetapi juga dapat dilakukan berdasarkan “*center*” pada *“objek”* gambarnya.

3) Untuk pengembangan selanjutnya pada metode *CST* dan *CEPP* perlu diuji coba pesan yang disisipkan berupa *string*/teks agar dapat dilakukan eksperimen lebih lanjut tentang bagaimana pembacaan wilayah citra penampung pesan.
4) Pada metode *SIM* perlu dilakukan pengembangan lebih lanjut untuk mengatasi kelemahan yaitu jika *stego-image* dimanipulasi menggunakan *Paint 3D*, *Windows Photo Editor,* dan *Adobe Photoshop* maka pesan tidak dapat diekstraksi.
5) Perlu dilakukan kompresi pesan teks terlebih dahulu sebelum pesan disisipkan ke *cover image* pada metode *SIM* agar kapasitas penyimpanan pesan dapat lebih banyak lagi.
6) Perlu dilakukan eksperimen lebih lanjut tentang atibut lain dari *metadata* yang dapat disisipkan pesan dan lebih tahan terhadap segala manipulasi citra menggunakan *software* apapun.

DAFTAR PUSTAKA

1. Mishra, B., Beg, R., Singh, VP. 2013. Information Security Through Digital Image Steganography Using Multilevel and Compression Technique. *MIT International Journal of Computer Science & Information Technology*. 3(1):26–9.
2. Razzaq, M.A., Shaikh, R.A. 2017. Digital Image Security : Fusion of Encryption , Steganography and Watermarking. *International Journal of Advanced Computer Science and Applications*, 8(5):224–8.
3. Desoky, A. 2012. *Noiseless Steganography*. CRC Press. 298 p.
4. Al-Afandy, K.A., Faragallah, O.S., Elmhalawy, A., El-Rabaie, E.S.M, El-Banby, G.M. 2016. High security data hiding using image cropping and *LSB* least significant bit steganography. *Colloquium in Information Science and Technology*. 400–404.
5. Paraskevov, H., Zhelezov, S., Uzunova-Dimitrova, B., 2017. Robustness of the secret message in stego file against flip and rotation attack. *Annals of the Academy of Romanian Scientists: Series on Mathematics and its Applications*. 9(1):5–16.
6. Zhang, Y., Qin, C., Zhang, W., Liu, F., Luo, X. 2018. On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*. 146:99–111.
7. Potdar, V.M, Han, S., Chang, E. 2005. Fingerprinted secret sharing steganography for robustness against image cropping attacks. *3rd IEEE International Conference on Industrial Informatics*, 717–24.
8. Kodovsky, J., Fridrich, J., 2013. Steganalysis in resized images. *IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings* - Proc. 2857-2861.
9. Bhatu, M.B., Shah, H.Y. 2016. Customized Approach To Increase Capacity And Robustness In Image Steganography. *In: International Conference on Inventive Computation Technologies (ICICT)*.
10. Singh, S., Siddiqui, T.J. 2013. Robust image steganography using complex

wavelet transform. *IMPACT - International Conference on Inventive Computation Technologies (ICICT)*. 56–60.

11. Kumar, M., Yadav, M. 2014. Image Steganography Using Frequency Domain. *International Journal of Scientific & Technology Research*. 3(9): 226-230.
12. Muyco, S.D., Hernandez, A.A. 2019. A modified hash based least significant bits algorithm for steganography. *ACM International Conference Proceeding Series*. 215–220.
13. Juarez, S.O., Fierro. R.A., Espejel. T.A., Nakano. M.M., Perez. M.H. 2015. Cropping and noise resilient steganography algorithm using secret image sharing. *Sixth International Conference on Graphic and Image Processing (ICGIP 2014)*. 94431S.
14. Swain. G., Lenka, S.K. 2015. A novel steganography technique by mapping words with *LSB* array. *International Journal of Signal and Imaging Systems Engineering.* 8(1–2):115–122.
15. Sedighi. V., Cogranne. R., Fridrich. J. 2015. Content-adaptive steganography by minimizing statistical detectability. *IEEE Transactions on Information Forensics and Security*. 11(2):221–234.
16. Rejani. R., Murugan, D., Krishnan, V.D. 2015. Pixel Pattern Based Steganography on Images. *Journal on Image and Video Processing*. 5(3):991–997.
17. Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., Gupta. B. 2017. Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia tools and applications*. 76(18):18451–18472.
18. Juarez, S.O., Cedillo, H.M., Sanchez, P.G., Toscano, M.K., Perez, M.H., Nakano, M.M. 2017. Compact image steganalysis for *LSB*-matching steganography. *International Workshop on Biometrics and Forensics, IWBF , IWBF*.
19. Zhang, X., Peng, F., Long, M. 2018. Robust Coverless Image Steganography Based on DCT and LDA Topic Classification. *IEEE Transactions on*

Multimedia. 20(12):3223–3238.

20. Prajapati, H.A., Chitaliya, N.G. 2015. Secured and Robust Dual Image Steganography: A Survey. *International Journal of Innovative Research in Computer and Communication Engineering*. 01(03): 30–37.
21. Andono, P., Sutojo, T., Muljono. 2017. *Pengolahan Citra Digital*. Yogyakarta: Andi.
22. Kadir, A., Susanto, A. 2013. *Teori dan Aplikasi Pengolahan Citra.* Yogyakarta: ANDI.
23. Mittal, M., Verma, A., Kaur, I., Kaur, B., Sharma, M., Goyal, L.M. 2019. An efficient edge detection approach to provide better edge connectivity for image analysis. *IEEE Access*. 33240–33255.
24. Sur, A., Ramanathan, V., Mukherjee, J. 2012. Secure Steganography Using Randomized Cropping. *Transactions on data hiding and multimedia security VII*. 82–95.
25. Wamiliana., Usman, M., Hijriani, A., Warsito., Setiawan, R. 2017. The Hybrid Methods of Column Transposition with Adaptive Minimum Error Least Significant Bit Replacement (AME*LSB*R) Using file jpg / jpeg and png. *International Journal of Computer Science and Network Security*. 17(7):174–179.
26. Sloan, T., Hernandez, C.J. 2018. Dismantling OpenPuff PDF steganography. *Digital Investigation.* 25:90–96.
27. Newman, J., Lin, L., Chen, W., Reinders, S., Wang, Y., Wu, M. 2019. StegoAppDB: A steganography apps forensics image database. *IS and T International Symposium on Electronic Imaging Science and Technology*. (5):1–12.
28. Jarusek, R., Volna, E., Kotyrba, M. 2019. Photomontage detection using steganography technique based on a neural network. *Neural Networks.* 116:150–165.
29. Castiglione, A., De Santis, A., Soriente, C. 2007. Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. *Journal of Systems and Software*. 80(5):750–764.

30. Araujo, II., Kazemian, H. 2020. Improving Steganographic capacity using distributed steganography over BMP. *Multimedia Tools and Applications.*
31. Bray, S.W. 2020. *Introduction to Cryptography and Python.* John Wiley & Sons, Inc. Published. 1–30.
32. Rahaeimehr, R. 2019. Novel Cryptographic Authentication Mechanisms for Supply Chains and OpenStack Novel Cryptographic Authentication Mechanisms for Supply Chains and OpenStack. *Opencommons UCCON*.
33. Kumar, S.K., Reddy, P.D.K., Ramesh, G., Maddumala, V.R. 2019. Image transformation technique using steganography methods using LWT technique. *Trait du Signal.* 36(3):233–237.
34. Silverstein, D.A., Farrell, J.E. 1996. Relationship between image fidelity and image quality. *IEEE International Conference on Image Processing*. 1:881–884.
35. Tang, W., Li, B., Tan, S., Barni, M., Huang, J. 2019. CNN-Based Adversarial Embedding for Image Steganography. *IEEE Transactions on Information Forensics and Security*. 14(8):2074–2087.
36. Zhou, Z., Mu, Y., Wu, Q.M.J. 2019. Coverless image steganography using partial-duplicate image retrieval. *Soft Computing.* 23(13):4927–38.
37. Mishra, M., Mishra, P., Adhikary, M.C. 2014. Digital Image Data Hiding Techniques: A Comparative Study. *Ansvesa.* 7(2):105–15.
38. Wu, P., Yang, Y., Li, X. 2018. StegNet: Mega Image steganography capacity with deep convolutional network. *Futur Internet*. 10(6):1–15.
39. Hussain, M., Wahab, A.W.A., Idris, Y.I., Bin, H.A.T.S., Jung, K.H. 2018. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*. 65:46–66.
40. Darwis, D., Junaidi, A., Wamiliana. 2019. A New Approach of Steganography Using Center Sequential Technique. *Journal of Physics: Conference Series*. 1338(1).
41. Wazirali, R., Chaczko, Z., Gibbon, J. 2017. Steganographic image sharing app. *International Conference on Systems Engineering, ICSEng*. 494–499.