THESIS PROGRESS REPORT

(Reported on April, 18 2025)

RGB Image Steganography Using Multiple Embedding

Submitted by

Dimas Anwar Aziz (203022410012)

(dimasanwaraziz@student.telkomuniversity.ac.id)

Approved by

Supervisor (I):

(Prof. Ari Moesriami Barmawi, Ph.D.)

Supervisor (II):

(-)

Contents

Progress Summary: (max 500 words)

Penelitian mengenai steganografi Multiple Embedding untuk gambar RGB telah mencapai kemajuan. Tahapan studi literatur, identifikasi masalah, formulasi kontribusi, dan penyusunan proposal telah diselesaikan. Saat ini, fokus penelitian berada pada tahap desain dan implementasi metode yang diusulkan. Berdasarkan studi awal dan tinjauan literatur, teridentifikasi bahwa metode sebelumnya yang menggunakan pendekatan berbasis kode seperti Reed-Muller memiliki keterbatasan, terutama dalam hal kapasitas pada gambar grayscale [5]. Oleh karena itu, penelitian ini mengusulkan penggunaan Polar Codes yang dikombinasikan dengan teknik multiple embedding untuk gambar RGB. Tujuannya adalah meningkatkan kapasitas penyembunyian data secara signifikan (target minimal 50% lebih tinggi dari metode Kingsley et al. [5]) sambil mempertahankan kualitas visual gambar stego (PSNR $>$ 40 dB).

Proses desain metode, termasuk alur kerja encoding, pembangkitan jejak kunci, penyisipan kunci dan data rahasia menggunakan Polar Codes, serta skema pembagian kunci (secret sharing) telah dirancang. Tahap implementasi awal sedang berjalan, mencakup pengembangan fungsi-fungsi inti dalam Python menggunakan library seperti OpenCV dan NumPy. Tantangan utama saat ini adalah mengoptimalkan algoritma Polar Codes untuk penyisipan pada ketiga channel warna RGB secara efisien dan memastikan integrasi yang mulus dengan mekanisme multiple embedding. Tahap selanjutnya adalah pengujian awal imperceptibility dan kapasitas, diikuti dengan pengujian robustness terhadap

berbagai serangan. Kesulitan yang dihadapi terutama berkaitan dengan kompleksitas matematis Polar Codes dan penyesuaiannya untuk domain steganografi gambar berwarna. Komentar dari pembimbing terkait metode penelitian akan terus diintegrasikan dalam pengembangan. Diharapkan tahap implementasi dan pengujian awal dapat diselesaikan sesuai jadwal.

1 Background

Dalam era digital yang semakin berkembang, keamanan data digital menjadi prioritas utama. Informasi pribadi, data bisnis, dan data kritikal lainnya harus dilindungi dari ancaman kebocoran atau akses yang tidak sah. Dalam menghadapi tantangan ini, kriptografi dan steganografi muncul sebagai solusi penting untuk meningkatkan keamanan data digital.

Steganografi merupakan teknik menyembunyikan pesan di dalam suatu media penyisipan pesan atau cover image, sehingga keberadaan pesan rahasia yang disisipkan tidak dapat dilihat secara langsung [1]. Steganografi memungkinkan pertukaran pesan rahasia melalui penyembunyian informasi pada berbagai media digital seperti gambar, video, dan audio, tanpa menimbulkan kecurigaan [2]. Steganografi dapat dipandang sebagai kelanjutan kriptografi dan dalam praknya pesan rahasia dienkripsi terlebih dahulu, kemudian cipherteks disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaannya. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya [3].

Di antara berbagai media digital yang dapat digunakan untuk steganografi,

gambar menjadi pilihan yang populer karena beberapa alasan. Pertama, gambar digital tersedia secara luas dan pertukaran gambar di internet adalah hal yang umum, sehingga tidak menimbulkan kecurigaan. Kedua, gambar memiliki kapasitas untuk menyembunyikan informasi. Ketiga, manipulasi pixel pada gambar dapat dilakukan dengan berbagai teknik. Namun, tantangan utama dalam steganografi gambar adalah menemukan keseimbangan antara kapasitas penyembunyian data, kualitas gambar, dan ketahanan terhadap deteksi [4].

Penelitian sebelumnya telah menunjukkan kemajuan signifikan dalam meningkatkan kapasitas penyembunyian data pada gambar grayscale. Kingsley et al. [5] berhasil meningkatkan kapasitas penyembunyian data hingga 450% menggunakan metode code base. Meski begitu, penggunaan gambar grayscale membatasi aplikasi praktis karena hanya memiliki satu channel pencahayaan. Di sisi lain, Fikri et al. [4] mendemonstrasikan bahwa penerapan steganografi pada gambar berwarna memiliki ketahanan yang baik, meskipun gambar dengan dominasi warna hitam menunjukkan kompatibilitas yang kurang optimal. Berdasarkan temuan-temuan tersebut, penelitian ini bertujuan untuk memperluas metode embedding ke gambar berwarna yang memiliki tiga channel warna (Merah, Hijau, dan Biru). Fokus utama adalah untuk meningkatkan kapasitas penyembunyian data sambil mempertahankan kualitas visual dan ketahanan terhadap deteksi. Penelitian ini juga akan mengevaluasi kompatibilitas metode yang diusulkan dengan berbagai jenis gambar berwarna, termasuk yang memiliki area gelap yang luas. Dengan mengoptimalkan penggunaan ketiga channel warna, diharapkan dapat dicapai peningkatan signifikan dalam kapasitas penyembunyian

data dibandingkan dengan metode yang hanya menggunakan gambar grayscale, sambil tetap mempertahankan kealamiahan gambar yang dihasilkan.

Aspek pengetahuan dalam penelitian ini berfokus pada teknik steganografi untuk gambar berwarna, metode steganografi berbasis kode, dan analisis kualitas gambar digital. Hal ini mencakup pemahaman mendalam tentang manipulasi channel warna RGB, teknik penyisipan data yang efektif, serta metode evaluasi kualitas gambar stego yang dihasilkan. Penekanan khusus diberikan pada optimasi penggunaan ketiga channel warna untuk memaksimalkan kapasitas penyimpanan data sambil mempertahankan kualitas visual.

Dari sisi pengguna, penelitian ini ditujukan untuk beberapa kelompok utama. Pertama, profesional keamanan informasi yang membutuhkan solusi penyembunyian data yang andal dan aman. Kedua, peneliti di bidang steganografi dan keamanan data yang dapat memanfaatkan metode ini untuk pengembangan lebih lanjut. Ketiga, pengembang aplikasi keamanan data yang memerlukan komponen steganografi yang efisien dan mudah diintegrasikan.

Aspek kegunaan penelitian mencakup berbagai aplikasi praktis dalam sistem data hiding, perlindungan hak cipta, dan watermarking digital. Metode yang dikembangkan dirancang dengan mempertimbangkan kemudahan implementasi, efisiensi komputasi, dan fleksibilitas penggunaan. Fokus utama adalah mencapai keseimbangan optimal antara kapasitas penyembunyian data, kualitas gambar hasil, dan ketahanan terhadap berbagai teknik deteksi steganografi.

Infrastruktur yang digunakan dalam penelitian ini berbasis Mac mini M2 dengan spesifikasi teknis yang mendukung pemrosesan gambar yang efisien. Sis-

tem dilengkapi dengan prosesor Apple M2 chip yang memiliki 8-core CPU dan 10-core GPU, didukung oleh 8GB memori dan penyimpanan SSD 256GB. Penggunaan sistem operasi macOS memberikan platform yang stabil untuk pengembangan dan pengujian metode steganografi yang diusulkan.

2 Literature Review

Kingsley et al (2020) pada papernya membahas tentang rendahnya kapasitas penyisipan dan nilai PSNR (Peak Signal-to-Noise Ratio) pada skema steganografi berbasis kode yang ada, yang hanya mencapai 150% kapasitas dan 48 dB kualitas visual gambar stegano. Untuk mengatasi masalah ini, metode yang diusulkan adalah teknik penyisipan ganda (multiple embedding), yang bertujuan untuk menyisipkan bit rahasia lebih dari sekali pada LSB (Least Significant Bit) dari piksel yang dipilih berdasarkan kunci rahasia. Parameter yang digunakan untuk mengukur keberhasilan metode ini meliputi kapasitas penyisipan dan nilai PSNR dari gambar stego yang dihasilkan. Kelebihan dari metode ini adalah kemampuan untuk mencapai kapasitas penyisipan yang lebih tinggi hingga 450% dan nilai PSNR yang meningkat menjadi 51 dB, serta meningkatkan ketahanan terhadap serangan seperti scratching dan kompresi JPEG. Namun, penelitian ini masih diterapkan pada gambar hitam putih [5].

Pada penelitian yang dilakukan oleh Dwi Andika et al (2020), mereka membahas keterbatasan kapasitas penyimpanan dalam teknik steganografi menggunakan algoritma GifShuffle pada citra GIF. Tantangan utama yang dihadapi adalah kesulitan dalam menyisipkan pesan teks dengan ukuran besar. Untuk

mengatasi masalah ini, mereka memodifikasi nilai bit dalam penyimpanan pesan, yang bertujuan meningkatkan kapasitas tanpa mengorbankan kualitas visual gambar. Uji coba menggunakan parameter seperti ukuran data yang dapat disisipkan serta kualitas gambar menunjukkan bahwa metode ini berhasil meningkatkan kapasitas penyimpanan hingga lebih dari 256 KB tanpa mengurangi kualitas gambar secara signifikan. Namun, metode ini memerlukan modifikasi tambahan pada algoritma GifShuffle yang dapat meningkatkan kompleksitas implementasi dan pemrosesan [6].

Susanto et al (2020) dalam penelitiannya menggabungkan metode steganografi Least Significant Bit (LSB) dengan algoritma enkripsi RSA untuk meningkatkan keamanan dalam penyisipan pesan terenkripsi pada gambar. Parameter yang digunakan untuk mengukur kualitas gambar setelah penyisipan adalah Peak Signal-to-Noise Ratio (PSNR), dengan hasil yang menunjukkan PSNR tertinggi sebesar 78 dB untuk pesan berukuran 1024 bit. Kelebihan metode ini adalah perubahan kualitas gambar yang hampir tidak terlihat, namun kekurangannya adalah kompleksitas yang meningkat seiring dengan ukuran pesan dan besarnya kunci RSA yang digunakan, yang memengaruhi performa [7].

Basri et al (2021) meneliti penggunaan metode steganografi dengan teknik Least Significant Bit (LSB) untuk menyembunyikan gambar di dalam gambar lainnya, khususnya dalam konteks interaksi sosial melalui media digital. Penelitian ini mengukur rasio ukuran gambar tersembunyi terhadap gambar cover serta kemampuan gambar cover mempertahankan kualitas visualnya. Hasilnya menunjukkan bahwa metode ini efektif menyembunyikan informasi tanpa

perubahan signifikan pada gambar cover. Namun, metode ini memiliki keterbatasan dalam menangani gambar dengan transparansi, karena hanya memperhitungkan komponen warna merah, hijau, dan biru (RGB), tanpa memperhitungkan komponen alpha [8].

Penelitian Wiranata et al (2021) berfokus pada penyisipan pesan rahasia dalam gambar dan audio menggunakan metode Least Significant Bit (LSB) yang dikombinasikan dengan enkripsi Caesar Chipper dan Rivest Code 4 untuk menjaga kerahasiaan data. Penelitian ini menguji kemampuan aplikasi untuk menyembunyikan dan mengambil pesan secara utuh, serta perubahan ukuran file gambar dan audio setelah proses penyisipan. Kelebihan metode ini adalah kemampuannya menjaga kerahasiaan tanpa perubahan signifikan pada kualitas gambar atau suara. Namun, ada perubahan ukuran file yang diakibatkan oleh proses enkripsi dan penyisipan pesan [9].

Penelitian yang dilakukan oleh Abdillah et al (2023) membahas tentang perlindungan data dan akses dengan menggunakan steganografi melalui teknik Least Significant Bit (LSB), di mana teks disisipkan dalam gambar melalui perubahan nilai pixel terkecil. Parameter yang diukur mencakup akurasi penyisipan teks dan kualitas gambar yang tetap terjaga setelah proses encoding dan decoding. Kelebihan utama metode ini adalah kemampuannya menyembunyikan informasi tanpa mengubah kualitas visual gambar secara signifikan. Namun, metode ini memiliki keterbatasan dalam kapasitas penyisipan teks dan rentan terhadap serangan manipulasi gambar yang dapat merusak data tersembunyi [10].

Tabel 1 menunjukkan perbandingan hasil penelitian terdahulu.

Table 1: Comparison of Previous Research

Author	**Method**	**Advantages**	**Disadvantages**
Kingsley et al. (2020)	Multiple embedding technique with secret key-based pixel selection	Increased capacity up to 450%, PSNR improved to 51dB	Limited to grayscale images only
Andika et al. (2020)	Modified GifShuffle algorithm for GIF images	Increased storage capacity over 256KB	Complex implementation, limited to GIF format
Susanto et al. (2020)	Combined LSB with RSA encryption	High PSNR (78dB) for 1024-bit messages	Increased complexity with larger messages and RSA keys
Basri et al. (2021)	LSB technique for image-in-image hiding	Effective information hiding with minimal visual changes	Limited handling of transparency (alpha channel)
Wiranata et al. (2021)	LSB combined with Caesar Cipher and RC4	Good security with dual encryption	File size increases after embedding
Abdillah et al. (2023)	LSB technique for text embedding	Maintains visual quality effectively	Limited text capacity, vulnerable to image manipulation

Berdasarkan tabel 1, dapat disimpulkan bahwa berbagai metode steganografi telah menunjukkan kelebihan dan kekurangan masing-masing. Metode multiple embedding oleh Kingsley et al. (2020) berhasil meningkatkan kapasitas penyembunyian data secara signifikan hingga 450% dengan kualitas visual yang baik (PSNR 51 dB), namun terbatas pada gambar grayscale. Metode GifShuffle yang dimodifikasi oleh Andika et al. (2020) meningkatkan kapasitas penyimpanan pada gambar GIF, tetapi kompleksitas implementasinya tinggi. Kombinasi LSB dan enkripsi RSA oleh Susanto et al. (2020) menghasilkan PSNR

tinggi (78 dB) namun dengan peningkatan kompleksitas. Metode LSB oleh Basri et al. (2021) efektif untuk menyembunyikan gambar dalam gambar lain dengan perubahan visual minimal, tetapi kurang optimal untuk gambar dengan transparansi. Kombinasi LSB dengan Caesar Cipher dan RC4 oleh Wiranata et al. (2021) memberikan keamanan yang baik namun meningkatkan ukuran file. Terakhir, metode LSB oleh Abdillah et al. (2023) efektif dalam menjaga kualitas visual namun memiliki keterbatasan kapasitas teks dan rentan terhadap manipulasi gambar.

Artikel ini memperkenalkan skema steganografi kuantum yang menyembunyikan citra abu-abu di dalam citra berwarna. Keamanan ditingkatkan dengan menggunakan pengacakan Arnold dan menyematkan citra rahasia dalam tiga cara berbeda: DWT di saluran R, DCT di saluran G, dan LSB di saluran B. Pendekatan ini meningkatkan ketidaktampakan, keamanan, dan ketahanan steganografi. PSNR rata-rata adalah 54,33 dB, menunjukkan kualitas visual yang tinggi, dan skema ini dapat menangani citra rahasia hingga setengah ukuran citra sampul. Namun, artikel tersebut mengakui kurangnya dukungan perangkat keras untuk komputer kuantum dan bergantung pada simulasi komputer klasik untuk pengujian. [**?**]

3 Problem Statement

Penelitian sebelumnya dalam steganografi berbasis kode telah menunjukkan kemajuan signifikan. Kingsley et al. [5] berhasil meningkatkan kapasitas penyembunyian data dari sekitar 150% menjadi 450%, yang merupakan peningkatan

substansial untuk case yang membutuhkan kapasitas tinggi. Meskipun demikian, penelitian pada gambar grayscale [3] masih membatasi pengaplikasiannya karena kurangnya fleksibilitas dalam penggunaan channel warna.

4 Objective and Hypotheses

Tujuan utama penelitian ini adalah:

1. Mengembangkan teknik steganografi berbasis kode dengan multiple embedding yang dioptimalkan untuk gambar RGB, dengan target peningkatan kapasitas penyembunyian data minimal 50% dibandingkan metode sebelumnya (Kingsley et al. [5]). Hipotesisnya adalah penggunaan Polar Codes pada gambar RGB akan memungkinkan peningkatan kapasitas yang lebih besar daripada aplikasi pada gambar grayscale.

2. Mempertahankan kualitas visual gambar stego dengan nilai Peak Signal-to-Noise Ratio (PSNR) di atas 40 dB. Hipotesisnya adalah peningkatan kapasitas melalui multiple embedding dan Polar Codes tidak akan secara signifikan menurunkan kualitas visual gambar [12].

Metode yang diusulkan, yaitu multiple embedding dengan Polar Codes, dipilih karena potensi Polar Codes dalam mencapai kapasitas Shannon dengan kompleksitas yang relatif rendah dan kemampuannya dalam koreksi kesalahan, yang diharapkan dapat menyeimbangkan antara kapasitas dan kualitas visual pada gambar RGB.

5 Research Method

5.1 Method requirement specification

Kebutuhan utama metode yang dikembangkan adalah:

1. Mampu meningkatkan kapasitas penyembunyian data minimal 50% dibandingkan metode Kingsley et al. [5].
2. Menjaga kualitas visual gambar stego dengan PSNR di atas 40 dB.
3. Mengimplementasikan algoritma penyisipan multiple embedding yang efektif untuk gambar berwarna RGB.

Sistem harus dapat memproses gambar input (secret image) dan gambar penampung (cover image) dalam format RGB, melakukan proses encoding/embedding dan decoding/extraction, serta tahan terhadap serangan umum.

5.2 Design and Implementation of the proposed method

Desain metode yang diusulkan melibatkan beberapa tahapan kunci seperti yang diilustrasikan pada Gambar 1. Proses utamanya adalah menyisipkan bit-bit rahasia dari 'Secret Image' ke dalam 'Cover Color Image' menggunakan Polar Codes. Polar Codes digunakan untuk mengkodekan data rahasia sebelum penyisipan untuk meningkatkan reliabilitas dan mencapai kapasitas yang tinggi dengan kompleksitas $O(N \log N)$. Posisi piksel untuk penyisipan ditentukan secara acak namun deterministik berdasarkan seed. Selain itu, digunakan mekanisme

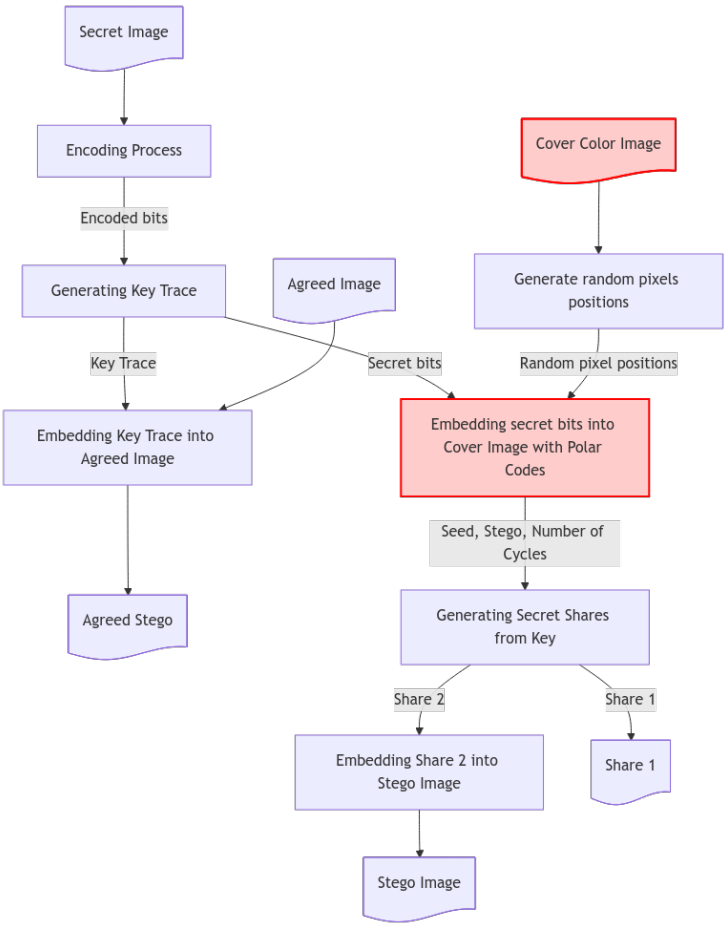

Figure 1: Design method

Key Trace yang disisipkan ke dalam 'Agreed Image' untuk menghasilkan 'Agreed Stego', serta skema pembagian kunci (Shamir's Secret Sharing) di mana 'Share 2' disisipkan ke 'Stego Image' dan 'Share 1' disimpan terpisah. Implementasi dilakukan menggunakan Python dengan library OpenCV dan NumPy, mendukung gambar RGB dan grayscale untuk perbandingan. Fokus implementasi adalah pada mekanisme multiple embedding, adaptasi Polar Codes untuk RGB, optimasi kapasitas (>50%), dan preservasi kualitas (PSNR > 40 dB).

5.3 Experimental results

Tahap eksperimen dirancang untuk mengevaluasi tiga aspek utama: Imperceptibility, Robustness, dan Capacity, seperti pada Gambar 2 proposal. Imperceptibility diukur menggunakan Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) untuk membandingkan kualitas visual gambar stego dengan gambar asli. Robustness diuji terhadap berbagai serangan seperti Noise (Gaussian [13], Salt & Pepper [14], Speckle [15]), Cropping, Scratching (Single & Multiple), dan Kompresi JPEG [16], dengan mengukur PSNR gambar rahasia yang berhasil dipulihkan. Capacity dievaluasi dengan mengukur rasio bit rahasia yang dapat disematkan terhadap ukuran gambar cover (bpp), menggunakan variasi ukuran secret image dan karakteristik gambar cover. Hasil eksperimen metode yang diusulkan (Polar Codes dengan multiple embedding) akan dibandingkan dengan metode sebelumnya (Reed-Muller code dengan multiple embedding). Saat ini, pengujian awal sedang dipersiapkan seiring dengan penyelesaian tahap implementasi.

5.4 Analysis of the experimental results

Analisis hasil eksperimen akan difokuskan pada perbandingan kuantitatif antara metode yang diusulkan (Polar Codes) dan metode acuan (Reed-Muller). Metrik utama yang akan dianalisis adalah:

- Imperceptibility: Nilai MSE dan PSNR akan dihitung dan dibandingkan. PSNR yang lebih tinggi (di atas 40 dB) dan MSE yang lebih rendah me-

nunjukkan kualitas visual yang lebih baik.

- Robustness: Nilai PSNR dari gambar rahasia yang dipulihkan setelah berbagai serangan akan dianalisis untuk mengukur ketahanan metode. Kemampuan koreksi kesalahan (ECC) dari kode yang digunakan (Polar Codes vs Reed-Muller) akan dievaluasi berdasarkan tingkat keberhasilan pemulihan data.

- Capacity: Kapasitas penyisipan (EC) dalam bit per pixel (bpp) akan dihitung menggunakan persamaan (6) dan dibandingkan antar metode. Analisis akan mencakup pengaruh variasi histogram gambar dan ukuran secret image terhadap kapasitas.

Analisis statistik seperti uji-t atau ANOVA mungkin digunakan untuk mengevaluasi signifikansi perbedaan kinerja antar metode.

6 Schedule Realization

Activity	Schedule		Realization		Output Target	Realiza
	Start	End	Start	End		
Literature study	Sem 1	Sem 1	Sem 1	Sem 1	Proposal Bab 1, 2	Selesai
Problem identification	Sem 1	Sem 1	Sem 1	Sem 1	Proposal Bab 3	Selesai
Contribution formulation	Sem 1	Sem 1	Sem 1	Sem 1	Proposal Bab 4	Selesai
Hypothesis formulation	Sem 1	Sem 1	Sem 1	Sem 1	Proposal Bab 4	Selesai
Proposal	Sem 1	Sem 1	Sem 1	Sem 1	Dokumen Proposal	Selesai
Design Encoding Process	Sem 2	Sem 2	Sem 2	Sem 2	Desain Algoritma	Selesai
Implement embedding schema	Sem 2	Sem 3	Sem 2	Sem 3	Kode Program (Embedding)	On Prog
Design decoding process	Sem 2	Sem 2	Sem 2	Sem 2	Desain Algoritma	On Prog
Design sharing schema	Sem 2	Sem 3	Sem 2	Sem 3	Kode Program (Sharing)	On Prog
Imperceptibility testing	Sem 3	Sem 3	Sem 3	-	Hasil Uji PSNR/MSE	Belum M
Robustness testing	Sem 3	Sem 4	Sem 3	-	Hasil Uji Serangan	Belum M
Capacity testing	Sem 3	Sem 4	Sem 3	-	Hasil Uji Kapasitas	Belum M
Thesis draft	Sem 4	Sem 4	Sem 4	-	Draft Tesis Lengkap	Belum M

Table 2: Realisasi Jadwal per 18 April 2025

References

[1] Ikwan Pujianto. "Uji Ketahanan Citra Digital Terhadap Manipulasi Robustness Pada Steganography". *Jurnal Informatika dan Rekayasa Perangkat Lunak* 2.1 (2021), pp. 16-27.

[2] Siaulhak Siaulhak, Safwan Kasma et al. "Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory". *BANDWIDTH: Journal of Informatics and Computer Engineering* 1.2 (2023), pp. 75-81.

[3] Anggya ND Soetarmono. "Studi Mengenai Aplikasi Steganografi Camouflage". *Teknika* 1.1 (2012), pp. 55-65.

[4] Muhammad Alfin Fikri and FX Ferdinandus. "Optimasi Teknik Steganografi Amelsbr Pada Empat Bit Terakhir Dengan Cover Image

Berwarna". *Antivirus: Jurnal Ilmiah Teknik Informatika* 16.1 (2022), pp. 25-38.

[5] Katandawa Alex Kingsley and Ari Moesriami Barmawi. "Improving Data Hiding Capacity in Code Based Steganography using Multiple Embedding." In: ().

[6] Dwi Andika and Dedi Darwis. "Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi". *Jurnal Ilmiah Infrastruktur Teknologi Informasi* 1.2 (2020), pp. 19-23.

[7] Ajib Susanto and Ibnu Utomo Wahyu Mulyono. "Kombinasi LSB-RSA untuk Peningkatan Imperceptibility pada Kripto-Stegano Gambar RGB". In: (2020).

[8] Muh Basri and Muhammad Fadhlil Gushari. "Penerapan Steganografi Gambar Berwarna pada Delapan Image Cover Menggunakan Metode LSB". *Jurnal Sintaks Logika* 1.3 (2021), pp. 153-158.

[9] Ade Davy Wiranata and Rima Tamara Aldisa. "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA". *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)* 5.3 (2021), pp. 277-281.

[10] Muhammad Oemar Abdillah, Ogie Ariansah Pane and Farhan Rusdy Asyhary Lubis. "Implementasi Keamanan Aset Informasi Steganografi Meng-

gunakan Metode Least Significant Bit (LSB)". *Jurnal Sains dan Teknologi (JSIT)* 3.1 (2023), pp. 40-46.

[11] Mamta Juneja and Parvinder S Sandhu. "An improved LSB based steganography technique for RGB color images". *International journal of computer and communication engineering* 2.4 (2013), p. 513.

[12] AB Nasution, S Efendi and S Suwilo. "Image steganography in securing sound file using arithmetic coding algorithm, triple data encryption standard (3DES) and modified least significant bit (MLSB)". *Journal of Physics: Conference Series*. Vol. 1007. 1. IOP Publishing. 2018, p. 012010.

[13] Ameen Mohammed Abd-Alsalam Selami and Ahmed Freidoon Fadhil. "A Study of the Effects of Gaussian Noise on Image". In: ().

[14] Shakair Kaisar and Jubayer AI Mahmud. "Salt and Pepper Noise Detection and removal by Tolerance based selective Arithmetic Mean Filtering Technique for image restoration". *International Journal of computer science and network security* 8.6 (2008), pp. 271-278.

[15] Mostafa Mansourpour, MA Rajabi and JAR Blais. "Effects and performance of speckle noise reduction filters on active radar and SAR images". In: Proc. Isprs. Vol. 36. 1. 2006, W41.

[16] Mr Venugopal Reddy CH et al. "Medical image watermarking schemes against salt and pepper noise attack". *International Journal of Bio-Science and Bio-Technology* 7.6 (2015), pp. 55-64.