**zzProteksi Citra dari *DeepFake* dengan CMUA-Watermark**

*Diajukan untuk Menyusun Skripsi  
di jurusan Teknik Informatika Fakultas Ilmu Komputer UNSRI*



Oleh :

Renaldi Budi Setiawan  
NIM : 09021281823066

**Jurusan Teknik Informatika**

**FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA  
2022**

**LEMBAR PENGESAHAN PROPOSAL SKRIPSI**

**Proteksi Citra dari DeepFake dengan CMUA-Watermark**

Oleh :

Renaldi Budi Setiawan

NIM : 09021281823066

Indralaya,Oktober 2022

Pembimbing I Pembimbing II,

Syamsuryadi, S.Si., M.Kom., Ph.D.   
NIP 197102041997021003

Muhammad Qurhanul Rizqie, S.KOM,. M.T., Ph.D.  
NIP 1671060312870008

Mengetahui,  
ketua Jurusan

Alvi Syahrini Utami, M.Kom.  
NIP. 19781222200642003

DAFTAR ISI

Halaman

HALAMAN JUDUL ……i

HALAMAN PENGESAHAN …...ii

DAFTAR ISI …..iii

DAFTAR TABEL …..iv

DAFTAR GAMBAR ….v

[**BAB I PENDAHULUAN** 6](#_Toc106435395)

[**1.1** **Pendahuluan** 6](#_Toc106435396)

[**1.2** **Latar Belakang Masalah** 6](#_Toc106435397)

[**1.3** **Rumusan Masalah** 7](#_Toc106435398)

[**1.4** **Tujuan Masalah** 8](#_Toc106435399)

[**1.5** **Manfaat Penelitian** 8](#_Toc106435400)

[**1.6** **Batasan Masalah** 8](#_Toc106435401)

[**1.7** **Sistematika Penulisan** 9](#_Toc106435402)

[**1.8** **Kesimpulan** 9](#_Toc106435403)

[**BAB II KAJIAN LITERATUR** 10](#_Toc106435404)

[**2.1** **Pendahuluan** 10](#_Toc106435405)

[**2.2** **Landasan Teori** 10](#_Toc106435406)

[**2.2.1** **Citra** 10](#_Toc106435407)

[**2.2.2** **DeepFakes** 11](#_Toc106435408)

[**2.2.3** **CMUAI-Watermark** 11](#_Toc106435409)

[**2.2.4** **Rational Unified Process** 12](#_Toc106435410)

[**2.3** **Penelitian Lain yang Relevan** 14](#_Toc106435411)

[**2.4** **Kesimpulan** 14](#_Toc106435412)

[**BAB III METODE PENELITIAN** 16](#_Toc106435413)

[**3.1** **Pendahuluan** 16](#_Toc106435414)

[**3.2** **Pengumpulan Data** 16](#_Toc106435415)

[**3.2.1** **Jenis dan Sumber Data** 16](#_Toc106435416)

[**3.2.2** **Metode pengumpulan Data** 17](#_Toc106435417)

[**3.3** **Tahapan Penelitian** 17](#_Toc106435418)

[3.3.1 Menentukan Kerangka Kerja Penelitian 18](#_Toc106435419)

[3.3.2 Menetukan Kriteria Pengujian 18](#_Toc106435420)

[3.3.3 Penarikan Hipotesa 19](#_Toc106435421)

[3.3.4 Menentukan Sumber Data 19](#_Toc106435422)

[3.3.5 Melakukan Pengujian Penelitian 19](#_Toc106435423)

[3.3.6 Mengevalusi Hasil penelitian dan Membuat kesimpulan 19](#_Toc106435424)

[**3.4** **Metode Pengembangan Perangkat Lunak** 20](#_Toc106435425)

[**3.4.1** **Face Incepsi** 20](#_Toc106435426)

[**3.4.2** **Fase Elaborasi** 20](#_Toc106435427)

[**3.4.3** **Fase Konstruksi** 21](#_Toc106435428)

[**3.4.4** **Fase Transisi** 21](#_Toc106435429)

[**3.5** **Manajemen Proyek Perangkat Lunak** 22](#_Toc106435430)

[**3.6** **Kesimpulan** 23](#_Toc106435431)

# **BAB I PENDAHULUAN**

## **Pendahuluan**

Pada bab ini akan dibahas berkenaan dengan garis besar pokok-pokok pikirandalam penelitian ini. Pokok pikiran yang akan dibahas antara lain latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian. Pokok-pokok pikiran yang diuraikan akan dijadikan acuan dalam kajian penelitian ini.

## **Latar Belakang Masalah**

Berita palsu telah menjadi isu yang mengancaman bagi wacana publik, masyarakat manusia, dan demokrasi (Borges et al., 2019; Qayyum et al., 2019). Berita palsu mengacu pada konten gaya berita fiktif yang dibuat untuk menipu publik (Aldwairi & Alwahedi, 2018; Jang &Kim, 2018). salah satu contohnya Berita palsu tersebut Adalah Deepfakes.

Deepfake sendiri baru dipopulerkan di tahun 2017, berawal dari pengguna Reddit mengunggah video porno hasil editan. Pengguna Reddit ini mengembangkan GAN menggunakan TensorFlow sebuah perangkat lunak mesin pencari gratis dari Google untuk menempelkan wajah selebriti ke tubuh perempuan dalam film porno. Teknologi Deepfake dapat menghasilkan, misalnya, video lucu, pornografi, atau politik seseorang yang mengatakan apa pun, tanpa persetujuan orang yang gambar dan suaranya terlibat (Hari, 2018; Fletcher, 2018). Foto KPM mahasiswa unsri sangat mudah diakses pada situs resmi laman Unsri versi lama (<https://old.unsri.ac.id/?act=daftar_mahasiswa>). Hal ini membuat sangat memungkinkan terjadi penyalagunaan foto tersebut oleh oknum yang dengan sengaja melakukan tindakkan tidak bertanggung jawab seperti pembuatan deepfake.

Untuk mencegah hal tersebut *adversarial* watermark dapat digunakan untuk memerangi model *deepfake*, *adversarial* watermark dapat menghasilkan gambar yang terdistorsi. Metode yang ada memerlukan proses pelatihan individu untuk setiap gambar wajah, untuk menghasilkan *adversarial attack* model terhadap model *deepfake* tertentu, yang sangat tidak efisien. Untuk mengatasi masalah ini, penelitian ini menggunakan metode universal *adversarial attack* model pada model *deepfake*, untuk menghasilkan Cross-Model Universal Adversarial Watermark (CMUA-Watermark) yang dapat melindungi ribuan gambar wajah dari beberapa model *deepfake* (Huang et al., 2021).

## **Rumusan Masalah**

Berdasarkan permasalahan pada latar belakang yang telah diuraikan maka rumusan masalah dari penelitian ini adalah

1. Bagaimana cara memproteksi citra gambar foto KPM mahasiswa Unsri dengan metode CMUA-Watermark?
2. Bagaimana tingkat akurasi metode CMUA-Watermark dalam memproteksi citra foto KPM mahasiswa Unsri dari *deepfakes*?

## **Tujuan Masalah**

Tujuan dari penelitian ini adalah:

1. Membangun perangkat lunak yang dapat memproteksi citra gambar foto KPM mahasiswa Unsri menggunakan metode CMUA-Watermark.
2. Mengetahui tingkat akurasi penggunaan metode CMUA-Watermark dalam memproteksi citra foto KPM mahasiswa Unsri dari *deepfakes*.

## **Manfaat Penelitian**

Manfaat yang diperoleh dari penelitian ini adalah:

1. Sistem yang dibuat dapat memproteksi citra gambar foto KPM mahasiswa Unsri menggunakan metode CMUA-Watermark.
2. Hasil penelitian dapat dijadikan sebagai rujukan untuk penelitian terkait di masa mendatang.

## **Batasan Masalah**

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Dataset yang digunakan merupakan dataset yang dipakai dalam penelitian milik dw (202x).
2. Data uji yang digunakan merupakan dataset foto mahasiswa jurusan Teknik Informatika Universitas Sriwijaya Angkatan 2018.
3. Ekstensi citra yang didukung oleh perangkat lunak adalah .jpg.

## **Sistematika Penulisan**

Sistematika penulisan tugas akhir mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut:

**BAB I. PENDAHULUAN**

Pada bab ini akan membahas landasan dari penelitian, seperti latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

**BAB II. KAJIAN LITERATUR**

Pada bab ini membahas literatur pada penelitian, seperti pengertian Citra, *Deepfake*, CMUAI-Watermark dan penelitian yang relevan.

**BAB III. METODOLOGI PENELITIAN**

Pada Bab ini menjelaskan pelaksanaan alur penelitian. yakni pengumpulan data dan perancangan pembangunan perangkat lunak. Serta tahapan dijelaskan secara detail berdasarkan kerangka yang dibuat.

## **Kesimpulan**

Pada Bab ini telah menjelaskan dasar dan patokan pada penelitian , seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

# 

# **BAB II KAJIAN LITERATUR**

## **Pendahuluan**

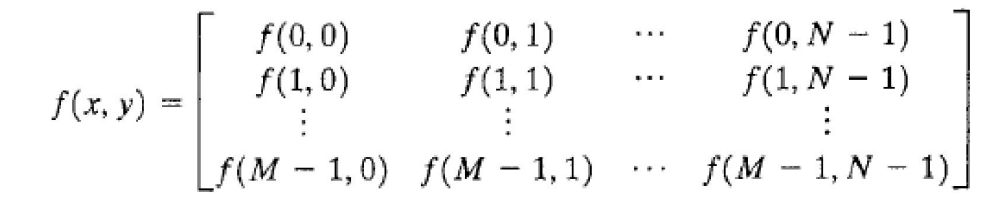
pada bab ini akan dijelaskan mengenai dasar-dasar teori digunakan pada penelitian ini. Serta penjelasan hasil dari penelitian-penelitian terkait mengenai citra, *Deepfakes*, CMUAI-Watermark dan RUP. Pada bab ini pula dibahas mengenai penelitian terkait lainnya yang relevan.

## **Landasan Teori**

### **Citra**

Citra didefinisikan sebagai fungsi dari dua *variable* misalnya *a*(*x,y*) dimana *a* sendiri sebagai amplitudo (misalnya kecerahan) citra pada koordinat (x,y). Citra digital *a*[*m,n*] merupakan citra dalam ruang diskrit 2D yang berasal dari citral Analog *a*(*x,y*) di ruang kontinu 2D melalui proses sampling yaitu yang biasa disebut sebagai digitalisasi (Young et al., 2006).

Menurut McAdrew citra digital adalah citra *f*(*x,y*) yang telah didiskritkan pada koordinat spasial dan kecerahan. Citra digital direpresentasikan oleh *array* dua dimensi dimana setiap *array* merepresentasikan satu kanal warna. Nilai warna kecerahan yang didigitalkan ini dinamakan nilai tingkat keabuan . Setiap elemen array tersebut dinamakan piksel atau pel yang diambil dari istilah ‘picture element’. Dimensi pada citra ditulis dengan format panjang x tinggi. Namun pada citra digital didefinisikan dengan ukuran tinggi *M* dan panjang *N.*



Koordinat citra dimulai dari pojok kiri atas, secara Sistematis di dimulai dari (0,0) dan berakhir di (M-1,N-1)(McAndrew, 2014).

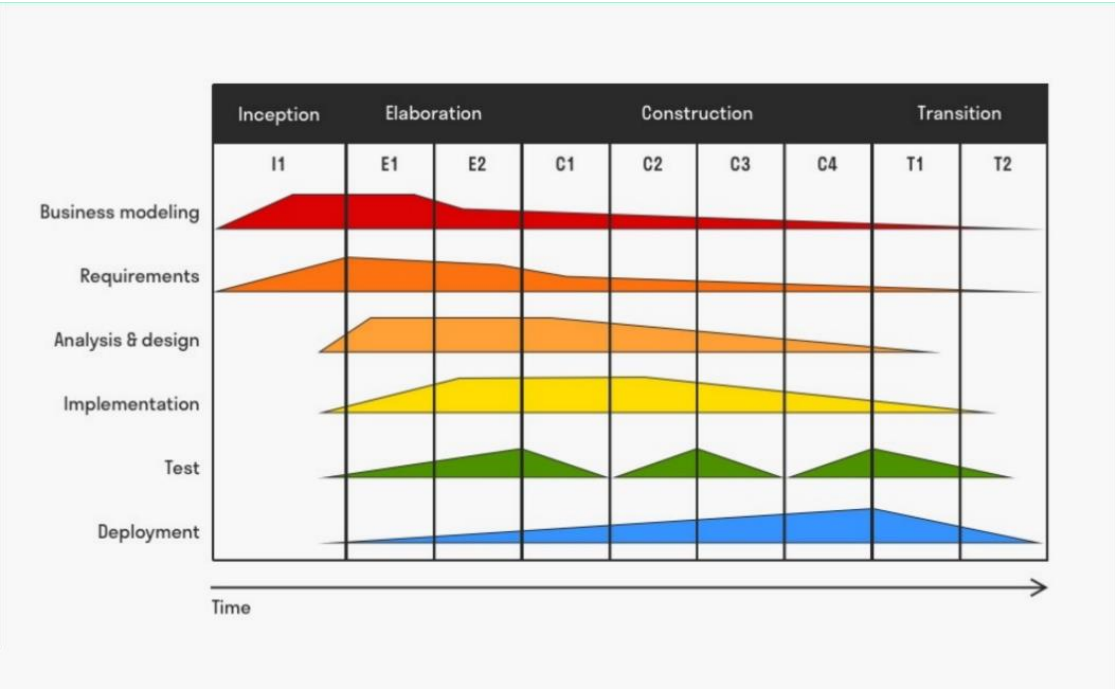
### **DeepFakes**

Deepfake merupakan teknik sintetis citra manusia yang berdasarkan pada kecerdasan buatan/AI. Ini digunakan untuk menggabungkan serta menempatkan gambar dan video yang ada ke sumber gambar atau video menggunakan teknik mesin belajar yang dikenal sebagai jaringan generatif adversarial (generative adversarial network) atau GAN(Hidayatul Khusna Sri Pangestuti, 2019).

### **CMUA-Watermark**

### **Rational Unified Process**

Rational Unified Process (RUP) adalah metode rekayasa pengembangan perangkat lunak yang digunakan untuk kedisiplinan dalam penetapan tugas dan tanggung jawab. Tujuan RUP adalah memastikan bahwa produk perangkat lunak yang dihasilkan akan berkualitas dan sesuai kebutuhan pengguna akhir (end-users) (Anwar, 2014). RUP yang baik akan tercipta lewat hasil kerja sama antara pengembang perangkat lunak, mitra dan pengguna. Salah satu perspektif dalam RUP merupakan *Dynamic Perspective* & *Lifecycle Phases* yang penggunaannya digambarkan dalam bidang dua dimensi. Bidang horizontal menyatakan lamanya waktu pengembangan dan aspek dinamis lainnya, sedangkan bidang vertikal menyatakan aspek statis dalam rekayasa pengembangan perangkat lunak. Perspektif RUP model ini dinyatakan seperti dalam gambar II-2.

  
Gambar \*\*-\*,Arsitektur Rasional Unified Process

Dalam bidang horizontal, terdapat fase atau tahap dalam proses rekayasa perangkat lunak yang memaparkan peran dari tiap unit. Fase dalam bidang ini terbagi ke dalam fase insepsi, elaborasi, konstruksi dan transisi.

1. Fase insepsi merupakan fase yang berfokus pada pendefinisian ruang lingkup atau batasan dalam proyek pengembangan dengan cara melakukan analisis desain berorientasi objek (Object Oriented Analysis Design). Tujuan dari fase ini adalah untuk mendapatkan seluruh pemahaman dari pihak yang berkaitan agar sistem yang diajukan sesuai dengan keinginan dan kebutuhan.
2. Fase elaborasi merupakan fase yang akan membuat arsitektur dasar sistem lewat hasil analisis sebelumnya. Fase ini juga akan menentukan perencanaan proyek serta spesifikasi dari fitur yang akan dimuat dalam sistem. Hasil dari fase ini merupakan dokumen arsitektur yang berguna untuk fase selanjutnya.
3. Fase Konstruksi merupakan fase menerjemahkan spesifikasi fitur dari dokumen rancangan sebelumnya ke dalam bentuk program/sistem sesuai dengan arsitekturnya. Fase ini berfokus pada peningkatan fungsi serta implementasi yang lebih mendalam terhadap spesifikasi sistem.
4. Fase Transisi merupakan fase pengujian sistem ke pengguna akhir dimana sistem yang dibuat harus memenuhi kebutuhan perangkat lunak dan kebutuhan penggunanya. Kendali dalam fase ini mulai dipindah kepada tim pemeliharaan perangkat lunak.

## **Penelitian Lain yang Relevan**

Penelitian yang telah dilakukan mengenai *adversarial machine learning at scale (A. Kurakin, I. Goodfellow, and S. Bengio, in ICLR, 2017.).* Dalam makalah ini mempelajari cara meningkatkan ketahanan terhadap contoh adversarial model besar (*Inception v3*) yang dilatih pada set data besar (*ImageNe*t). Menunjukkan bahwa pelatihan adversarial memberikan ketahanan terhadap contoh adversarial yang dihasilkan menggunakan metode satu langkah. Meskipun pelatihan adversarial tidak banyak membantu melawan metode iteratif yang diamati bahwa contoh adversarial yang dihasilkan oleh metode iteratif lebih kecil kemungkinannya untuk ditransfer di antara jaringan, yang memberikan ketahanan tidak langsung terhadap serangan adversarial kotak hitam. Selain itu kami mengamati bahwa peningkatan kapasitas model juga dapat membantu meningkatkan ketahanan terhadap contoh adversarial terutama ketika digunakan bersamaan dengan pelatihan adversarial. Akhirnya menemukan efek kebocoran label yang menghasilkan akurasi yang lebih tinggi pada contoh adversarial FGSM dibandingkan dengan contoh bersih ketika jaringan dilatih secara adversarial.

## **Kesimpulan**

Pada bab ini telah dibahas teori yang akan digunakan sebagai dasar penelitian ini. Pada bab ini juga telah dibahas mengenai penelitian terkait yang mendukung literatur penelitian ini. Mekanisme pelaksanaan penelitian selengkapnya akan dibahas dalam bab selanjutnya.

# **BAB III METODE PENELITIAN**

## **Pendahuluan**

Pada bab ini akan dijelaskan mengenai tahapan penelitian, metode penelitian serta manajemen proyek penelitian. Tahapan penelitian dijadikan sebagai acuan pada setiap fase pengembangan perangkat lunak agar dapat memberikan solusi untuk rumusan masalah dan tercapainya tujuan penelitian.

## **Pengumpulan Data**

Pada bagian ini akan dijelaskan mengenai data yang digunakan dalam

penelitian.

### **Jenis dan Sumber Data**

Jenis data yang digunakan sebagai objek penelitian adalah data Primer dan data Sekunder. Data primer berupa kumpulan data dari foto KPM mahasiswa unsri yang didapatkan dari proses *Scraping* pada situs resmi laman Unsri lama. Sedangkan data sekunder berupa data Kumpulan data dari *dataset* data CelebA (Liu et al., in Deep learning face attributes in the wild, 2015.)

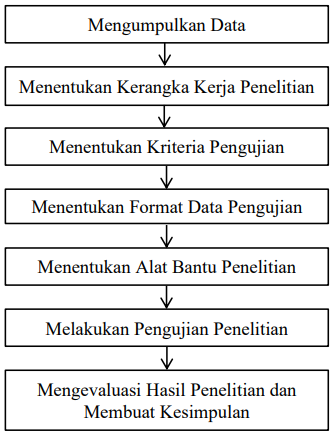
Gambar III-1. Contoh data yang dari *dataset* celebA

### **Metode pengumpulan Data**

Metode pengumpulan

## **Tahapan Penelitian**

tahapan penelitian yang dilakukan pada tugas akhir ini adalah:



Gambar III-2.alur Tahapan penelitian

Mengumpulkan data

data berupa video DeepFake dengan intensitas tinggi dari 59 wajah selebiriti dari berbagai umur yang terdapat dalam *dataset* Celeb-df. Untuk menunjukkan keefektifan *Landmark Breaker* dalam menghambat generasi *DeepFake*. Setiap video berisi satu subjek dengan berbagai pose kepala dan ekspresi wajah.

### Menentukan Kerangka Kerja Penelitian

Kerangka kerja yang dilakukan pada penelitian ini adalah sebagai berikut :

### Menetukan Kriteria Pengujian

Kriteria pengujian yang akan dilakukan pada penelitian:

Pengujian dilakukan dengan menggunakan metode Regresi Logistik Ordinal.

### Penarikan Hipotesa

Format data pengujian menggunakan pendekatan Confusion Matrix.

### Menentukan Sumber Data

Dalam melaksanakan penelitian Menentukan tingkat keparahan luka pada kecelakaan lalu lintas menggunakan metode Regresi Logistik Ordinal dibutuhkan alat dalam menunjang proses penelitian. Adapun alat yang digunakan sebagai berikut

1. Perangkat Keras

Proccessor : intel® core™ i7 8th *generation*

RAM : 16GB RAM

HDD : 1TB HDD strorage.

1. Perangkat Lunak

Sistem Operasi : Windows 10 64 bit

Teks Editor : Spyder

### Melakukan Pengujian Penelitian

Pengujian penelitian dimulai dengan tahap pra-pengulahan data masukkan, kemudian akan dilakukan beberapa tahap pengujian terhadap data tersebut.

### Mengevalusi Hasil penelitian dan Membuat kesimpulan

## **Metode Pengembangan Perangkat Lunak**

Metode pengembangan yang digunakan dalam penelitian ini adalah metode Rational Unified Process (RUP). Pengembangan sistem deteksi kemiripan kode sumber dibagi ke dalam empat tahap, yaitu fase insepsi, fase elaborasi, fase konstruksi dan fase transisi. Berikut merupakan tahapan pengembangan perangkat lunak yang akan dilakukan dalam tiap fasenya.

### **Face Incepsi**

Tahapan yang akan dilakukan dalam fase ini adalah sebagai berikut.

1. Pemodelan Sistem : Menentukan ruang lingkup dan batasan masalah.
2. Kebutuhan : Mendefinisikan spesifikasi perangkat lunak.
3. Analisis dan Perancangan : Melakukan analisis terhadap kebutuhan perangkat lunak termasuk di dalamnya kebutuhan fungsional dan non fungsional dari spesifikasi perangkat lunak.
4. Implementasi : Membuat seluruh rancangan sistem ke dalam bentuk diagram use-case.

### **Fase Elaborasi**

Tahapan yang akan dilakukan dalam fase ini adalah sebagai berikut.

1. Pemodelan Sistem: Membuat rancangan antarmuka (interface) sistem.
2. Kebutuhan: Menentukan spesifikasi dari sistem.
3. Analisis dan Perancangan: Membangun model activity diagram dan sequence diagram dari rancangan sistem.
4. Impelementasi: Membuat program berdasarkan diagram yang ditentukan sebelumnya.

### **Fase Konstruksi**

Tahapan yang akan dilakukan dalam fase ini adalah sebagai berikut.

1. Pemodelan Bisnis : Menentukan bahasa pemrograman yang akan membangun sistem.
2. Kebutuhan : Menentukan kebutuhan sistem sesuai dengan fungsi yang telah ditentukan.
3. Analisis dan Perancangan : Membangun tampilan antar-muka sistem.
4. Implementasi: Membangun sistem dengan membuat program menggunakan bahasa pemrograman yang telah ditentukan.

### **Fase Transisi**

Tahapan yang akan dilakukan dalam fase ini adalah sebagai berikut.

1. Pemodelan Sistem : Menentukan pengujian terhadap sistem.
2. Kebutuhan : Menentukan alat bantu pengujian terhadap sistem.
3. Analisis dan Perancangan : Merancang kasus penggunaan selama pengujian sistem.
4. Implementasi : Melaksanakan pengujian terhadap sistem menggunakan kasus penggunaan yang telah ditentukan.

## **Manajemen Proyek Perangkat Lunak**

Rencana manajemen proyek penelitian merupakan perencanaan aktivitas penelitian dari tahap awal hingga selesai. Perencanaan aktivitas pada penelitian ini akan menggunakan *Gantt Chart* seperti pada Tabel III-3.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Uraian Kegiatana | Tahun 2021 bulan ke- | | Tahun 2022 bulan ke- | | | |
| 11 | 12 | 1 | 2 | 3 | 4 |
| **1** | **Melakukan Pengumpulan Data** |  |  |  |  |  |  |
| a | Mengumpulkan data |  |  |  |  |  |  |
| b | Melakukan pra-pengolahan data |  |  |  |  |  |  |
| c | Melakukan modifikasi data sesuai skenario |  |  |  |  |  |  |
| d | Tersedia dokumen hasil tahapan penelitian |  |  |  |  |  |  |
| **2** | **Rekayasa Perangkat Lunak** |  |  |  |  |  |  |
| **2.1** | **Insepsi** |  |  |  |  |  |  |
| a | Menentukan pemodelan bisnis |  |  |  |  |  |  |
| b | Menentukan kebutuhan pengguna |  |  |  |  |  |  |
| c | Menentukan kebutuhan sistem |  |  |  |  |  |  |
| **2.2** | **Elaborasi** |  |  |  |  |  |  |
| a | Menentukan spesifikasi sistem |  |  |  |  |  |  |
| b | Membangun model *acitvity diagram* dan *sequence diagram* |  |  |  |  |  |  |
| c | Membangun rancangan tampilan antar-muka |  |  |  |  |  |  |
| **2.3** | **Konstruksi** |  |  |  |  |  |  |
| a | Membangun Model *Class Diagram* |  |  |  |  |  |  |
| b | Membangun Sistem (impelementasi kode) |  |  |  |  |  |  |
| c | Perbaikan Sistem |  |  |  |  |  |  |
| **2.4** | **Transisi** |  |  |  |  |  |  |
| a | Melakukan pengujian awal terhadap sistem |  |  |  |  |  |  |
| b | Tersedia dokumen hasil tahapan penelitian |  |  |  |  |  |  |
| **3** | **Melakukan Pengujian Penelitian Terhadap Sistem** |  |  |  |  |  |  |
| a | Membuat rancangan hasil pengujian dalam penelitian |  |  |  |  |  |  |
| b | Melakukan pengujian final terhadap sistem |  |  |  |  |  |  |
| c | Tersedia dokumen hasil penelitian |  |  |  |  |  |  |
| **4** | **Melakukan Analisis dan Kesimpulan dari Hasil Pengujian** |  |  |  |  |  |  |
| a | Melakukan analisis terhadap hasil pengujian penelitian |  |  |  |  |  |  |
| b | Membuat kesimpulan dan saran terhadap hasil pengujian penelitian |  |  |  |  |  |  |

Tabel Rencana Manajemen Proyek Penelitian

## **Kesimpulan**

Pada bab ini telah dibahas tentang proses pengumpulan data yang digunakan sebagai bahan uji perangkat lunak, tahapan penelitian, metode pengembangan perangkat lunak yang akan digunakan serta kriteria pengujian penelitian yang akan dilakukan terhadap sistem.