logo, metin, simge, sembol, ticari marka içeren bir resim

Açıklama otomatik olarak oluşturuldu

TED UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

**CMPE 491 – Analysis Report**

**SIMA**

**22.11.2024**

**İbrahim Ataberk Kabasakal – 17032700808**

**Furkan Tosun – 64312119164**

**Ahmet Tunç – 30274207140**

**Nusret Mert Yaşar - 52786056504**

Contents

[1. Introduction 3](#_Toc182842026)

[2. Current System 3](#_Toc182842027)

[3. Proposed System 4](#_Toc182842028)

[3.1 Overview 4](#_Toc182842029)

[3.2 Functional Requirements 4](#_Toc182842030)

[3.3 Nonfunctional Requirements 5](#_Toc182842031)

[3.4 Pseudo Requirements 5](#_Toc182842032)

[3.5 System Models 6](#_Toc182842033)

[3.5.1 Scenarios 6](#_Toc182842034)

[3.5.2 Use Case Model 7](#_Toc182842035)

[3.5.3 Object and Class Model 8](#_Toc182842036)

[3.5.4 Dynamic Models 9](#_Toc182842037)

[3.5.5 User Interface - Navigational Paths and Screen Mock-Ups 11](#_Toc182842038)

[4. Glossary 13](#_Toc182842040)

[5. References 13](#_Toc182842041)

# **1. Introduction**

The Secure Image Masking Algorithm (SIMA) project is an AI-driven software solution developed to automatically anonymize faces in both images and videos. Its core aim is to safeguard privacy by altering identifiable facial features—such as eyes, nose, and mouth—so they cannot be recognized. This tool is intended for use in fields like social media, surveillance footage, and news media, where protecting individual privacy is crucial. The project focuses on delivering a system that excels in performance, usability, and ethical adherence to provide a secure and seamless user experience.

The platform will be hosted on a user-friendly web interface at [fimasoft.com.tr](http://fimasoft.com.tr), allowing users to upload their media for instant anonymization. Utilizing advanced AI technologies like GANs or CNNs, this solution is particularly significant in today's context of heightened privacy concerns. It complies with global data protection laws like GDPR and addresses ethical issues surrounding data misuse.

**Key Challenges and Constraints:**

1. **Technical:** Ensuring high accuracy while maintaining real-time video anonymization.
2. **Economic:** The need for advanced hardware and large-scale storage capabilities to handle extensive data processing.
3. **Ethical:** Preventing the misuse of the system, such as anonymizing faces for illegal activities.
4. **Legal Compliance:** Aligning with international privacy laws to ensure the system can be used across borders.

kişi, şahıs, insan yüzü, boyun, giyim içeren bir resim

Açıklama otomatik olarak oluşturuldu insan yüzü, ekran görüntüsü, kişi, şahıs, metin içeren bir resim

Açıklama otomatik olarak oluşturuldu insan yüzü, kırpıntı çizim, çizgi film, çizim içeren bir resim

Açıklama otomatik olarak oluşturuldu

### **2. Current System**

At present, no publicly available system exists that specializes in automated face anonymization. The few existing solutions are either limited to experimental research or proprietary tools that are not accessible to general users. This lack of a readily available solution creates a significant gap in meeting privacy needs, particularly in areas like social media, surveillance, and journalism.

The SIMA project aims to bridge this gap by offering a robust, real-time face anonymization solution. This system will include:

* **AI-Based Anonymization:** Precise and effective alteration of facial features like eyes, nose, and mouth to ensure privacy.
* **Web Accessibility:** An intuitive platform enabling users to easily upload their media for processing.
* **Ethical and Legal Compliance:** A framework aligned with global privacy regulations, such as GDPR, to ensure ethical and secure usage.

metin, adam, insan, insan yüzü, giyim içeren bir resim

Açıklama otomatik olarak oluşturuldu ekran görüntüsü, Animasyon, Çizgi film, kırpıntı çizim içeren bir resim

Açıklama otomatik olarak oluşturuldu

# **3. Proposed system**

### 3.1 Overview

An AI-powered solution for automatic face anonymization in photos and videos is what the Secure Image Masking Algorithm (SIMA) project seeks to create. By changing some facial features (such as the eyes, nose, and mouth), the main goal is to safeguard individual privacy by making the person's identity unidentifiable. This approach, which guarantees privacy compliance and ethical data usage, is especially helpful in fields like social media, surveillance systems, and news media.

After it is put into use, SIMA will operate through a web-based platform that is connected to a powerful API, allowing for the real-time anonymization of images and videos. To guarantee safe and scalable deployment, the project places a strong emphasis on sustainability, social responsibility, legal compliance, and user-friendly design.

Assuring high accuracy, preserving real-time performance, and resolving ethical issues with prejudice and abuse in face detection technology are some of the primary hurdles.

### 3.2 Functional Requirements:

1. **Face Anonymization**: Recognizing and protecting particular facial features, like the mouth, nose, and eyes.
2. **Dataset Utilization**:Using publically accessible datasets such as FaceForensics and CelebA to train and test the model
3. **API Integration**:Using an API to include the face anonymization model into an intuitive online platform
4. **Real-Time Processing**:Enabling real-time anonymization of images and videos​
5. **User Experience**:Offering a user-friendly interface that makes it simple for users to anonymize their photos and videos.
6. **Batch Processing**:Allow users to anonymize multiple images or videos simultaneously.
7. **Error Handling**:Offer recovery methods and feedback for unsuccessful anonymization attempts or file types that are not supported.
8. **Platform Compatibility**:Compatibility with various browsers and OS systems to guarantee broad accessibility

### 3.3 Non-Functional Requirements:

1. **Performance**:Ensuring accurate and high-speed anonymization​.
2. **Compliance**:Complying with local privacy laws, like the GDPR.
3. **Sustainability**:Utilizing energy-efficient algorithms to reduce the influence on the environment.
4. **Ethical Responsibility**:Creating the technology in compliance with professional and ethical guidelines .
5. **Scalability and Deployability**:Building a web platform software architecture that is simple to grow and deploy.
6. **Security**:Protecting users' personal information and promoting psychological safety.
7. **High Availability**:To meet the demands of users worldwide, make sure the platform runs 7/24 with little downtime.
8. **Scalability**:To meet the demands of users worldwide, make sure the platform runs around-the-clock with little downtime.

### **3.4 Pseudo Requirements**

Pseudo requirements are constraints that, while not directly related to user functionality, still significantly impact the development of the SIMA project:

1. **Web-Based Accessibility:**  
   The solution must be implemented on an easily navigable online platform ([fimasoft.com.tr](http://fimasoft.com.tr)), enabling users to access it from various devices without needing to install additional software.
2. **Legal and Ethical Standards:**  
   The system must adhere to data privacy laws like GDPR and KVKK and include mechanisms to prevent misuse, such as restricting unauthorized access to user data and activity logs.
3. **Scalability:**  
   The backend system should be designed to handle an increasing number of users and a growing data load while maintaining stable performance.
4. **Real-Time Functionality:**  
   The anonymization process should deliver results within a few seconds to meet user expectations for fast and efficient service.
5. **AI Model Adaptability:**  
   The architecture must support regular updates and enhancements to the AI model, allowing it to adapt to new datasets and evolving anonymization challenges.

# 3.5 System Models

### 3.5.1 Scenarios

**Scenario 1: Individual User's Image Anonymization Process**  
1. The user logs into the platform.  
2. The user uses the upload tool to choose a picture.   
3. The system verifies the image's format and size. An error warning appears if the image is inappropriate.   
4. The AI model uses anonymization and detects faces.   
5. The system shows a comparison of the image before and after anonymization after the process is finished.  
6. The user can download the anonymized image if desired.  
  
**Scenario 2: Corporate User's Reporting Process**  
1. After logging in, the corporate user goes to the reporting area.   
2. Information on processing speed, anonymization success rates, and the number of processed photos is shown by the system.   
3. To create a comprehensive report, the user chooses a range of dates.   
4. A report for the chosen time frame is generated by the system and made available in downloadable PDF format.  
  
**Scenario 3: Feedback and Model Optimization**  
1. The anonymization results are inadequate, as the user observes.   
2. Using the platform's "Send Feedback" feature, the user provides feedback outlining the problem.   
3. This feedback is recorded by the system as an AI model report.   
4. After reviewing the comments, an administrator starts either manual or automatic model optimization.   
5. The model is updated and put into use.  
  
**Scenario 4: Real-Time Video Processing**  
1. The video anonymization feature is chosen by the user.   
2. The anonymization process starts when the user uploads a video file.   
3. Each video frame is processed by the AI model, which then anonymizes the faces.   
4. The user downloads the anonymized video after the procedure is finished.

### 3.5.2 Use Case Model

**Actors :**

Indıvıdual User , Aı Model , Corporate User , System Administrator , Web Platform

**Primary Use Cases :**

 **Multi-Region Anonymization**: Handles complex images with multiple individuals by identifying and processing each region separately.

 **Dynamic Learning**: Integrates user feedback into the model to continuously improve anonymization methods in real-time.

 **User Management**: Allows for account creation, login, and password management.

 **Image Upload**: Enables the uploading of images or videos to the platform.

 **Facial Detection and Anonymization**: The system processes uploaded files to detect and anonymize faces.

 **Result Viewing and Downloading**: Users can view or download the anonymized files.

 **Feedback and Optimization**: Users can submit feedback to enhance the model.

 **Statistical Reporting**: Corporate users receive detailed anonymization and performance reports.

 **Access Control**: Assigns roles or permissions to team members for collaborative use.

 **Real-Time Updates**: Displays live progress for ongoing tasks.

 **Error Notifications**: Alerts users if their uploads are invalid

Use Case Diagram

A computer screen shot of a computer screen

Description automatically generated

## 3.5.3 Object and Class Model

#### Classes

 **User** : represents people or organizations that access the system to see reports, upload photos, and start processes.

 **Individual User** : Designed for more straightforward use cases, it refers to individual users who wish to make their own photographs anonymous.

 **Corporate User** : Acts on behalf of companies requesting anonymization and bulk image processing reports.

 **AI Model** : Uses sophisticated algorithms to manage facial recognition and anonymization chores and continuously improves itself.

 **Image** : Stands for the uploaded images or videos that the system will process and make anonymous.

 **Processing Order** : Monitors and controls the state of the films and pictures that are presently being processed.

 **Feedback :** Gathers user-submitted comments to find mistakes or recommend changes to the model.

 **Statistics** :Saves the system's performance metrics, including the number of processed images, processing durations, and success rates.

 **Anonymizable (Interface)** : Specifies the necessary anonymization technique that the AI Model class implements.

 **Processable (Interface)** : Specifies common methods for initiating and monitoring processes, implemented by the Image and Processing Queue classes.

Class and Object Diagram

A black background with white text

Description automatically generated

## 3.5.4 Dynamic Models

The Dynamic Models for the SIMA project are represented through activity and state diagrams. These models demonstrate the overall workflow and different states of the system during operation.

#### Activity Diagram

The activity diagram highlights the process flow of the SIMA system. It consists of the following steps:

1. User Logs into the System.

2. User Uploads Image/Video.

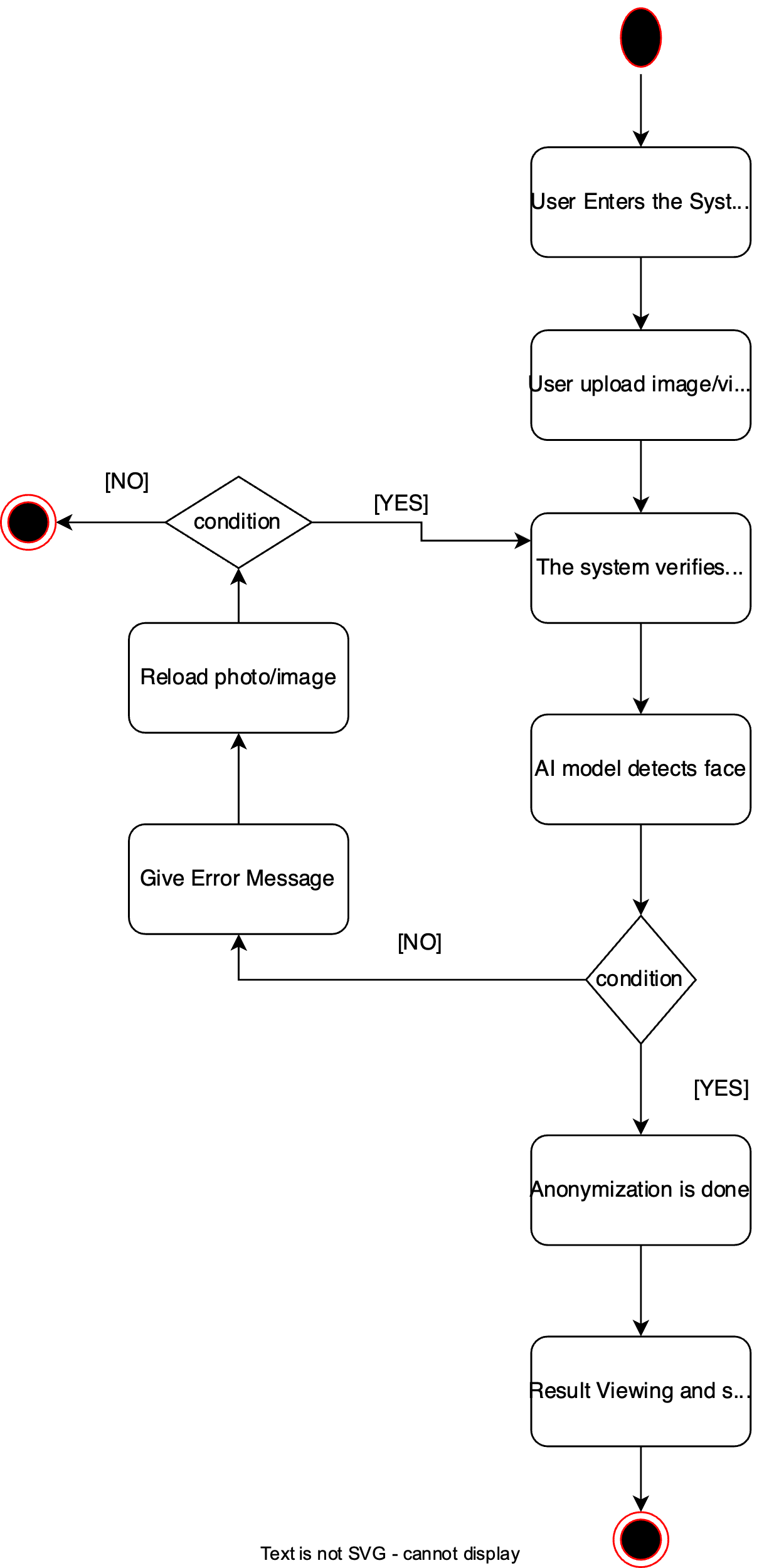
3. AI Model Processes File.

4. System Displays Anonymized Results (Before/After).

5. User Downloads Results or Submits Feedback.

6. Feedback is Recorded in the Database.

Activity Diagram



#### State Diagram

The state diagram represents various operational states of the SIMA system:

• Idle: The system waits for user actions.

• Uploading: The user uploads a file to the system.

• Processing: The AI model processes the uploaded file.

• Results Ready: The anonymized result is displayed to the user.

• Feedback Submitted: The user provides feedback on the processed file.

• System Optimized Based on Feedback: The system uses feedback to improve performance.

State Diagram

A screenshot of a computer

Description automatically generated

### 3.5.5 User Interface - Navigational Paths and Screen Mock-Ups

The user interface of SIMA was carefully designed to ensure an intuitive and user-friendly experience. The navigational paths and corresponding screen mock-ups for key pages are outlined below.

### Navigational Paths

1. Home Page: Introduction to SIMA and its features.

2. Upload Page: Provides an interface to upload files and track their status.

3. Result Page: Displays anonymized output with options to download results.

4. Help Page: Includes FAQs and contact information.

### Screen Mock-Ups

Two key mock-ups have been created to illustrate the user journey:

1. Result Page:

This page displays the original image on the left and the AI-processed anonymized image on the right. It includes a 'Download Results' button below the images for easy access. Below is the mock-up:

2. Upload Page:

This page allows users to upload files via a drag-and-drop interface or by clicking a file input button. A 'View Results' button is displayed below the upload section. Below is the mock-up:

A screenshot of a screen

Description automatically generatedA screenshot of a screenshot of a computer

Description automatically generated

# **4 Glossary**

The glossary provides definitions for key terms used throughout the project and its implementation.

**• Privacy-Preserving Action Recognition:** A framework to encode actions while protecting privacy.

• **Autoencoders:** Deep learning models used to compress and reconstruct data, often for anonymization.

• **GANs (Generative Adversarial Networks):** Machine learning models used for generating or modifying images.

• **Datasets:**

**- CelebA:** A dataset with over 200,000 images for face attribute learning.

- **VGGFace2:** A dataset with 3.3 million images for face recognition and anonymization.

**• AI-Supported Masking:** AI technology used to obscure sensitive facial features while preserving non-identifiable information.

**• Face Encryption:** The process of generating imperceptible perturbations to ensure facial recognition systems fail to identify the individual.

**• U-Net:** A neural network architecture widely used in segmentation tasks like face detection.

# **5 References**

ACM Code of Ethics and Professional Conduct. URL: https://www.acm.org/code-of-ethics

IEEE Code of Ethics URL: https://www.ieee.org/about/corporate/governance/p7-8.html

GDPR (General Data Protection Regulation) URL: https://gdpr-info.eu/

CelebA Dataset URL: http://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

FaceForensics Dataset URL: https://github.com/ondyari/FaceForensics

Fimasoft (Project Website) URL: http://www.fimasoft.com.tr/

VGGFace2 Dataset URL: https://www.robots.ox.ac.uk/~vgg/data/vgg\_face2/

Generative Adversarial Networks (GANs) URL: https://arxiv.org/abs/1406.2661

U-Net: Convolutional Networks for Biomedical Image Segmentation URL: https://arxiv.org/abs/1505.04597