Software Requirements Specification (SRS)

Dental Biometric System

Submitted by:
Hammad Latif
BS Computer Science
Department of Computer Science
Quaid-i-Azam University, Islamabad

Supervisor:
Dr. Ayyaz Hussain

Date of Submission:
February 6th, 2025

Table of Contents

Abstract

This project introduces a user-friendly dental biometric system designed specifically for administrators and forensic officers. This system streamlines identification and authentication processes within dental practices and forensic investigations. Utilizing intuitive interfaces, the system ensures ease of use for authorized personnel, enabling efficient management of dental records and enhancing security protocols. Through rigorous testing, the system demonstrates remarkable accuracy in identifying individuals based on dental biometric data. Key features include robust algorithms tailored for dental data analysis, empowering precise identification even in complex scenarios. Initially catering to administrative and forensic applications, the system holds potential for broader usage in forensic dentistry, dental records management, and access control within dental facilities. Future enhancements may include integrating additional biometric modalities and expanding functionalities to predict age based on available data, thereby augmenting its utility in forensic investigations and administrative tasks.

Dental Biometric System

1. Introduction

1.1 Purpose of DBS

The purpose of a Dental Biometric System (DBS) is to aid in the identification of human bodies in cases of massive catastrophes, airplane crashes, and natural disasters such as hurricanes and tsunamis where physical features like fingerprints and facial features are frequently destroyed, making identification difficult. Currently, dental records are used for identification, but the process is often time-consuming and inefficient. The implementation of a DBS will improve and automate this process, making it more efficient and reliable.

1.2 Scope of DBS

1.2.1 Main Functionalities

1. Maintaining radiographs and details of people
2. Feature extraction from radiographs
3. Identification of the person
4. Finding details about the person from radiograph
5. Security: The ability to secure biometric data and ensure the privacy and confidentiality of user information
6. Scalability: The ability to scale the system to accommodate a large number of users and support high-volume biometric transactions.

1.2.2 Objectives of DBS

1. To automate the process of matching premortem and antemortem datasets, making human identification quicker and more efficient, reducing the need for manual matching.
2. To reduce the workload of manual tasks and minimize human error.
3. To facilitate prompt identification and release of deceased bodies to their families for burial.
4. To improve the accuracy and reliability of dental record matching and identification.
5. To streamline the identification process and eliminate delays and inefficiencies in the current manual system.
6. To enhance the privacy and security of dental records and biometric data.

1.2.3. Project Deliverables

1. Technical Documentation: Detailed documentation of the analysis and design
2. Working Model: A functioning model of the dental biometric system, demonstrating its capabilities and performance.
3. User Manual: A comprehensive guide for dental staff on how to use the system, including its features, functions, and any limitations or restrictions.
4. Presentation: A formal presentation of the project, highlighting its key features, benefits, and contributions to the field of dental biometrics.
5. Source Code: The complete source code of the dental biometric system, including any necessary libraries and dependencies.
6. Desktop Application

1.3 Definitions

Table 1:Definitions

Terms	Descriptions
DBS	Dental Biometric System
User	Member of Forensic odontology department
SRS	Software Requirement Specifications: Description of software to be developed
ISO/IEC/IEEE	IEEE Recommended Practice for Software Requirements Specifications
DBMS	Database Management System
PDF	Portable Document Format
PNG	Portable Network graphics
Admin	Technical Employee of Forensic odontology department

1.4 References

1. ISO/IEC/IEEE 16326:2019

1.5 Overview

The remainder of SRS is organized as follow: Section 2 describes overall description of DBS including product perspective, product functions, user characteristic. Section 3 is most important part of SRS as it is describing specific functional requirements of SRS as well as non-functional requirements including performance requirements and software system attributes.

2. Overall Description

2.1. Product Perspective

The dental biometric system (DBS) is designed to be a standalone product, but it does require access to a database of dental records in order to perform its functions.

2.1.1. System Interfaces:

Not applicable.

2.1.2. User Interfaces:

The User Interface (UI) for a dental biometric system (DBS) would play a critical role in making the system easy to use and accessible to dental professionals. Here's a description of what a typical UI for a DBS might include:

1. Log In Screen: A screen that requires users to enter their credentials to access the system, ensuring that only authorized individuals can access the sensitive dental data stored in the system.
2. Main Menu: A main menu that provides access to the different functions of the system, such as data entry, searching, and reporting.
3. Data Entry Screen: A screen that allows dental professionals to enter new dental records into the system. This may include fields for capturing information such as name, age, gender, and dental radiographs.
4. Search Screen: A screen that allows users to search for dental records based on various criteria, such as patient name, date of birth, and dental characteristics.
5. Matching Results Screen: A screen that displays the results of a matching operation, indicating which premortem and antemortem datasets match and how closely they match.
6. Sign Out Screen: A screen that allows users to log out of the system when they are finished using it, ensuring that their session is securely terminated and the system remains protected from unauthorized access.

2.1.3. Hardware Interfaces:

Not Applicable.

2.1.4. Software Interfaces:

1. Database

Name: MySQL Server

Mnemonic: MySQL

Version number: Latest available version

Source: MySQL official website

The MySQL Server is used as the database management system for storing and retrieving dental records and patient information. It allows for efficient data storage and retrieval, making it possible to quickly and easily access patient information for the DBS.

2. Operating System

Name: Linux

Mnemonic: LIN

Version number: Latest available version

Source: Linux official website

The Linux operating system is used as the platform for the DBS. Linux provides a stable, secure, and efficient operating system environment, allowing the DBS to run smoothly and effectively. Additionally, Linux provides support for the MySQL database, allowing for seamless integration between the two components.

In terms of interfaces, the DBS interacts with the MySQL database to store and retrieve patient information. The data is stored in the database in a structured format, allowing for efficient and easy retrieval. The data can be accessed and updated through the DBS user interface, allowing dental staff to quickly and easily manage patient information.

2.1.5. Communication Interfaces:

Not Applicable.

2.1.6. Memory Constraints:

1. Minimum RAM: 2 GB
2. Hard disk space: Minimum 100 GB of free disk space
3. Operating System: Linux OS

2.1.7. Operations:

Not Applicable.

2.2. Product Functions:

Admin Side

1. Admin can add details about the individuals and radiographs.
2. Admin can update specific records.
3. Admin can search for a specific record using radiograph information.
4. Admin can search for a specific record using the individuals' date of birth.
5. Admin can delete specific or all records.
6. Admin can view the existing records.

Forensic officer Side

1. A forensic officer can identify an individual.

2. A forensic officer can determine the age, gender, and ethnicity of an individual.

2.3. User Characteristics

Admin:

Only administrator can access, add, modify, or delete information in the Dental Biometric System. It is necessary for the administrator to be a part of the forensic odontology department and have a system administrator ID verified by the forensic department. The administrator must have technical expertise to manage the DBS, and must be a professional. Beforehand, training should be provided to the administrator regarding the system.

Forensic officer

Only authorized forensic officers with valid credentials can access the Dental Biometric System to identify individuals and retrieve their details such as age, sex, and ethnicity. The forensic officers must be active in their field and possess the necessary skills and knowledge to effectively use the system. Regular training and technical support should be provided to ensure efficient use of the system.

2.4 Product Constraints

1. The system must comply with relevant privacy laws and regulations to ensure the confidentiality and security of user data.
2. Users must provide valid authentication credentials to access and use the system.
3. The system must accurately match antemortem and post-mortem dental records to ensure reliable identification.
4. The system must be scalable to handle large volumes of dental records and biometric data.
5. The system must be regularly maintained and updated to ensure optimal performance and functionality.

2.5 Assumptions and Dependencies

Assumptions:

- The users are trained in the proper use of the system.
- The system will be used in a secure environment.
- The data provided to the system is accurate and up-to-date.
- The hardware and software requirements are met.

Dependencies:

- The availability of a secure database to store patient information.
- The availability of trained personnel to operate and maintain the system.
- The availability of funding to purchase and maintain the hardware and software components of the system.

3. Specific Requirements

3.1 Functional Requirements

3.1.1 Use cases

1. Add details and radiograph

Actor: System Administrator

Pre-condition:

1. The system must be operational
2. The administrator must be logged in

Main Success Scenario:

1. The administrator uploads the radiograph of the person's teeth
2. The system confirms the successful upload of the radiograph
3. The administrator enters the person's full name
4. The administrator enters the person's date of birth
5. The administrator selects the person's ethnicity
6. The administrator uploads a photo of the person

Post-condition:

1. Radiograph, name, date of birth, ethnicity, and picture are stored successfully in the database.

2. Identify Person

Actor: Forensic Officer

Pre-condition:

1. The system must be operational.
2. The Forensic Officer must be logged in to the system.

Main Success Scenario:

1. The Forensic Officer uploads the radiograph of a person.
2. The system confirms that the radiograph has been uploaded successfully.
3. The system displays the details of the matching record, if any, including name, date of birth, ethnicity, and any other relevant information.

Post-condition:

1. The system redirects the Forensic Officer back to the identify person interface.

Alternative Flow:

3. No matching record is found for the uploaded radiograph.

3a. The system prompts the Forensic Officer to determine if he would like to save the radiograph details to the database for future reference.

3. Search person by date of birth

Actor: Forensic officer
Pre-condition:
1. System must be operational
2. Forensic officer must be logged in

Main Success Scenario:
1.Forensic officer enters the date of birth of the person
3. System displays the details found against the entered date of birth
   a. Age
   b. Sex
   c. Picture

Post condition:
1. System redirects the user back to the search interface

Alternative flow:
3. No details found against entered date of birth.

4. Update details and radiographs

Actor: System Administrator

Pre-condition:

1. The system must be working
2. System administrator must be logged in

Main Success Scenario:

1. The administrator searches for the record
2. The administrator uploads the new radiograph of the person's teeth
3. The system displays a response that the radiograph was uploaded successfully

4. The administrator updates the person's name, date of birth, sex, and ethnicity
5. The administrator updates the picture of the person.

Post-condition:

1. The system redirects the user to the update details and radiographs interface.

Alternative Flow:

1. No record found.

5. Delete a specific record

Actor: System Administrator

Pre-condition:

1. The system must be functioning
2. The System Administrator must be logged in

Main Success Scenario:

1. The System Administrator searches for the record to be deleted.
2. The System Administrator confirms the deletion of the record.
3. The system successfully deletes the record and saves the changes.

Post-condition:

1. The system redirects the System Administrator to the "Delete Record" interface.

Alternative Flow:

1. The record is not found.

6. Delete all records

Actor: System Administrator

Pre-condition:

1. The system must be operational
2. The System Administrator must be logged in

Main Success Scenario:

1. The System Administrator selects the option to delete all records.
2. The System confirms the deletion of all records.
3. The System saves the changes.

Post-condition:

1. The System redirects the System Administrator to the add records interface.

3.2 Other Functional Requirements

1. System has to check whether Student/Admin has entered his correct user-id and password.
Input:
Admin/ forensic officer enters his user-id and password.
Processing:
To check if id and password are valid it will send data to database for verification and receive response from database.
Output:
Accept or reject authorization from database.

2. Different answers from database about authorization.
Input:
Response from database
Invalid Password (If password is incorrect)
Invalid User-Id (If user id is incorrect)
Processing:
If System receives any of these responses from database, login will be failed and Admin/forensic officer will get an error message.
Output:
Login failed and an error message will be displayed.

3. If User-Id and Password are correct, authorization process is finished.
Input:
System gets accept from database from authorization process.
Processing:
Finishing authorization.
Output:
Opens Admin/forensic officer portal on Screen.

4. If login failed more than 3 times in a row, a message will be displayed that your account is temporarily blocked please contact your respective administration.
Input:
Entering wrong user-id and password for 4th time in succession.
Processing:
Initiate authorization process and message from database to block account.
Output:
Display error message that the forensic officer should contact forensic administration.

5. Age Calculation

Input: Date of Birth

Processing: The system calculates the age of the person based on the entered date of birth.

Output: Age of the Person

3.3 Performance Requirements

1. Fast and responsive user interface: The system must have a fast and responsive user interface, allowing users to quickly perform tasks such as searching, adding, updating, and deleting records.
2. Quick record retrieval: The system must be able to retrieve a record in less than 2 seconds, even with a large number of records stored in the database.
3. Minimum downtime: The system must be designed to have minimum downtime and should be available for use 99.9% of the time.
4. Scalable performance: The system should be designed to handle increased usage, and performance should not degrade significantly with increasing numbers of records stored in the database.
5. Data security: The system must ensure the security of the stored data, with measures such as encrypted data storage and regular backups.

3.4 Software System attributes

1. Reliability: System must have a 99.5% uptime during normal operating hours. The system must be able to recover from failures within 2 minutes.
2. Availability: System must be available for use 24 hours a day, 7 days a week, with the exception of planned maintenance windows, which must be scheduled outside of normal business hours.
3. Security: System must implement secure authentication protocols to prevent unauthorized access. Data transmitted over the network must be encrypted to protect against eavesdropping. System must keep a log of all user actions for auditing purposes.
4. Maintainability: System must be designed using modular architecture to allow for easy updates and maintenance. Code must be organized and documented to facilitate future updates by new developers.
5. Portability: System must be written in a programming language that is supported on multiple operating systems. Code must not contain platform-specific dependencies. The system must be tested on multiple operating systems to ensure compatibility.

4. Implementation and Testing

4.1. Implementation Overview

4.1.1 System Architecture:

The dental biometric system's architecture encompasses software components. At its core, the system consists of a biometric algorithm module, and a user interface module.

- **Biometric Algorithm Module:** This module implements the core algorithms for dental biometric identification/authentication. These algorithms analyze dental radiographs to extract unique features and patterns that can be used for identification purposes. Deep learning model VGG16 is used to extract features and for feature matching cosine similarity technique is used.
- **User Interface Module:** The user interface provides a platform for administrators and forensic officers to interact with the system. It allows users to input data, maintain it, do identification, and view the results of biometric analysis. The interface is intuitive, user-friendly, and accessible to accommodate users with some technical expertise.

4.1.2 Technologies Used:

The development of the dental biometric system involves a combination of technologies, frameworks, and tools to facilitate different aspects of the implementation process. Here's an example list of technologies I used:

- **Programming Languages:** Python
- **Frameworks/Libraries:** TensorFlow for Deep learning, and Kivy for desktop application.
- **Database:** MySQL
- **Development Tools:** Google Colab for prototyping algorithms

4.2. Data Collection

4.2.1 Data Acquisition

In our dental biometric system, I obtained dental biometric data from publicly available sources such as Kaggle, specifically utilizing panoramic dental radiographs. Panoramic radiographs provide a comprehensive view of the entire dentition, making them suitable for biometric analysis.

4.3. Algorithm Development

4.3.1 Biometric Algorithms

In dental biometric system, I utilized the VGG16 convolutional neural network (CNN) architecture for feature extraction from panoramic dental radiographs. VGG16 is a deep

learning model renowned for its effectiveness in image classification tasks. I adapted this architecture to extract discriminative features from dental images, which are crucial for biometric identification/authentication.

Following feature extraction, I employed cosine similarity as a metric for comparing biometric templates generated from dental images. Cosine similarity measures the cosine of the angle between two vectors, providing a measure of similarity irrespective of their magnitudes. In the context of biometric authentication, cosine similarity quantifies the resemblance between dental feature vectors extracted from input images and those stored in the system's database.

4.3.2 Implementation Details:

The implementation of these algorithms was carried out using Python programming language, leveraging popular libraries such as TensorFlow and Keras for deep learning functionalities. Here's a brief overview of the implementation process:

Feature Extraction with VGG16:

- I utilized pre-trained weights of the VGG16 model, which were trained on large-scale image datasets such as ImageNet. This enabled us to benefit from the learned representations of low-level and high-level features.
- Input panoramic dental radiographs were resized to the dimensions expected by the VGG16 model (e.g., 224x224 pixels) and pre-processed to meet the model's input requirements.
- The pre-processed images were fed into the VGG16 model, and feature vectors were extracted from one of the intermediate layers of the network.

Cosine Similarity Calculation:

- Biometric templates were generated from the feature vectors extracted using VGG16 for each input dental image.
- During the authentication process, the cosine similarity between the biometric template of the input image and the templates stored in the system's database was calculated.
- Cosine similarity scores were compared against a predefined threshold to determine whether the input image matches any of the stored templates, thereby facilitating biometric identification/authentication.

By integrating VGG16 for feature extraction and cosine similarity for template comparison, our dental biometric system achieves robust and accurate identification/authentication capabilities, ensuring reliable recognition of individuals based on their dental characteristics.

4.4. User Interface Design

4.4.1 UI Requirements:

The user interface for my dental biometric system caters to two primary user roles: administrators and forensic officers.

- **Administrator Requirements:**
  - Access to the entire system with privileges to perform various actions such as data management, system configuration, and biometric identification.
  - An admin panel for adding, updating, deleting, and searching data in the database.
  - Ability to register new forensic officers.
- **Forensic Officer Requirements:**
  - Access to the system for biometric identification purposes.
  - Ability to sign in to the system securely and perform identification tasks.

4.4.2 UI Design Process:

For the UI design process, I opted to streamline development and focused directly on implementation rather than conducting formal wireframing, prototyping, and iterative improvements.

4.4.3 UI Implementation:

The user interface was implemented using the Kivy framework. Kivy is an open-source Python library for rapid development of applications with a natural user interface. It supports various platforms including Windows, macOS, Linux, Android, and iOS, making it suitable for cross-platform deployment.

- **Kivy Framework:**
  - I chose Kivy due to its ease of use and flexibility for developing user interfaces in Python.
  - Kivy provides a wide range of UI components and layouts, allowing us to create intuitive interfaces for both administrators and forensic officers.
- **Implementation Approach:**
  - I designed separate screens or panels for administrators and forensic officers to cater to their distinct functionalities and requirements.
  - Admin panel features include options for data management, system configuration, and user management.
  - Forensic officer interface focuses on authentication tasks, providing a streamlined experience for conducting biometric identification.
- **Usability and Accessibility:**
  - Throughout the implementation process, I prioritized usability and accessibility to ensure a seamless experience for users.

- User interface elements were designed with clear labels, intuitive navigation, and consistent layout to facilitate ease of use.

By leveraging the Kivy framework, I was able to develop a user-friendly and accessible interface that meets the requirements of administrators and forensic officers, enabling efficient management and utilization of the dental biometric system.

4.5 Testing Methodology

4.5.1 Testing Objectives:

The objectives of the testing phase in dental biometric project are to ensure the reliability, accuracy, and performance of the system. Specifically, i aim to:

1. **Evaluate System Accuracy:**

I **a**ssess the system's ability to accurately identify and authenticate individuals based on their dental biometric data. This includes measuring the system's false acceptance rate (FAR) and false rejection rate (FRR).

2. **Measure Performance:**

I Evaluate the speed and efficiency of the system in processing biometric data and returning identification results. Performance metrics may include response time, throughput, and resource utilization.

4.5.2 Test Scenarios:

For testing dental biometric system, I consider a range of scenarios and use cases to ensure comprehensive coverage of its functionality and behavior. These scenarios include:

1. **Normal Cases:**

- Admin login and access to the system's functionalities.
- Adding, updating, and deleting data in the MySQL database through the admin panel.
- Registration of new forensic officers by the admin.
- Forensic officer login and access to biometric identification features.
- Successful biometric identification of individuals using dental biometric data.

4.5.3 Testing Environment:

For testing dental biometric project, I set up a dedicated testing environment consisting of:

1. **Software:**
    - Operating system: Linux (Kali).
    - Python environment with necessary dependencies including the Kivy framework.
    - MySQL database for storing and managing biometric data.

To perform testing, I created test cases based on the defined scenarios and executed them in the testing environment. l documented the results of each test case, including any issues encountered and their resolutions.

4.6. Testing Procedures

Understood. Let's proceed with writing relevant test cases based on the Testing Methodology section provided earlier. We'll start with Functional Testing.

4.6.1 Functional Testing:

Test Case 1: Admin Login

Test ID	**TC-1**
Description	Verify that administrators can successfully log in to the system.
Preconditions	Admin credentials are available, and the system is accessible.
Test Steps	1. Navigate to the login page of the system. 2. Enter valid admin username and password. 3. Click on the login button.
Expected Result	The system should authenticate the admin credentials and grant access to the admin panel.
Pass Criteria	Admin successfully logs in, and the admin panel is displayed.
Actual Result	Admin successfully logs in, and the admin panel is displayed.
Verdict	Pass

Test Case 2: Adding Details

Test ID	**TC-2**
Description	Verify that administrators can successfully add details including name, age, gender, state, picture, and radiograph image to the system.
Preconditions	Admin credentials are available, and the system is accessible.
Test Steps	1. Log in to the admin panel. 2. Navigate to the section for adding details. 3. Enter valid name, age, gender, state, and upload a picture and radiograph image. 4. Click on the submit button.
Expected Result	The system should successfully add the details to the database.
Actual Result	Details including name, age, gender, state, picture, and radiograph image are added to the system.
Verdict	Pass

Test Case 3: Updating Details

Test ID	TC-3
Description	Verify that administrators can successfully update details for a user. To update, the administrator first searches for the record. If found, they can view the details and then update at least one detail.
Preconditions	Admin credentials are available, and the system is accessible.
Test Steps	1. Log in to the admin panel. 2. Navigate to the section for updating details. 3. Search for the user record using appropriate search criteria. 4. If the record is found, view the details. 5. Update at least one detail (e.g., name, age, gender, state, picture or radiograph file). 6. Click on the update button.
Expected Result	The system should successfully update the details for the user.
Actual Result	Details for the user are updated with the changes made by the administrator.
Verdict	Pass

Test Case 4: Deleting Record

Test ID	TC-4
Description	Verify that administrators can successfully delete a record from the system. To delete the record, the administrator first searches for the record. If found, they can proceed to delete it.
Preconditions	Admin credentials are available, and the system is accessible.
Test Steps	1. Log in to the admin panel. 2. Navigate to the section for deleting records. 3. Search for the record using appropriate search criteria. 4. If the record is found, select it for deletion. 5. Confirm the deletion action.
Expected Result	The system should successfully delete the record from the database.
Actual Result	The selected record is deleted from the system.
Verdict	Pass

Test Case 5: Registering Forensic Officer

Test ID	TC-5
Description	Verify that administrators can successfully register a forensic officer by entering their name and password.
Preconditions	Admin credentials are available, and the system is accessible.

Test ID	TC-5
Test Steps	1. Log in to the admin panel. 2. Navigate to the section for registering forensic officers. 3. Enter the name and password for the forensic officer. 4. Click on the register button.
Expected Result	The system should successfully register the forensic officer with the provided name and password.
Actual Result	The forensic officer is registered with the entered name and password.
Verdict	Pass

Test Case 6: Forensic Officer Login and Access Biometric Screen

Test ID	TC-6
Description	Verify that forensic officers can successfully log in to the system and access the biometric screen.
Preconditions	Forensic officer credentials are available, and the system is accessible.
Test Steps	1. Log in to the system using forensic officer credentials. 2. Navigate to the biometric screen.
Expected Result	The forensic officer should be able to log in successfully and access the biometric screen without any issues.
Actual Result	The forensic officer successfully logs in and gains access to the biometric screen.
Verdict	Pass

Test Case 7: Biometric Identification by Forensic Officer

Test ID	TC-7
Description	Verify that forensic officers can successfully perform biometric identification by uploading a radiograph, and the system provides the result.
Preconditions	Forensic officer credentials are available, and the system is accessible.
Test Steps	1. Log in to the system using forensic officer credentials. 2. Navigate to the biometric identification section. 3. Upload a radiograph image for biometric identification. 4. Initiate the identification process.
Expected Result	The system should process the radiograph image and provide the identification result (e.g., match or no match).
Actual Result	The system successfully processes the radiograph image and provides the identification result.
Verdict	Pass

Quantitative Results: During testing, the dental biometric system demonstrated high accuracy rates in biometric identification. Processing times were also within acceptable limits, with an average identification time of under 3 seconds per radiograph image.

Conclusion And Future Work

Conclusion:

The dental biometric system developed encompasses essential features such as user authentication, data management, and biometric identification. It enables administrators to efficiently manage user data and forensic officers to conduct biometric identification based on dental characteristics.

Future Work:

In future iterations, integrating hardware components for direct teeth scanning could enhance the system's usability and efficiency. This would enable real-time data acquisition, streamlining the identification process. Additionally, expanding the dataset to include a diverse range of dental characteristics and conditions would improve the system's accuracy and robustness. Moreover, leveraging a larger dataset could facilitate the development of predictive models for estimating age, particularly useful when premortal radiograph data is unavailable. These enhancements would further advance the capabilities and applications of the dental biometric system, contributing to its broader adoption and impact in various domains.

Appendix

Use case Diagram

Fig: Use case diagram of DBS

Domain Model

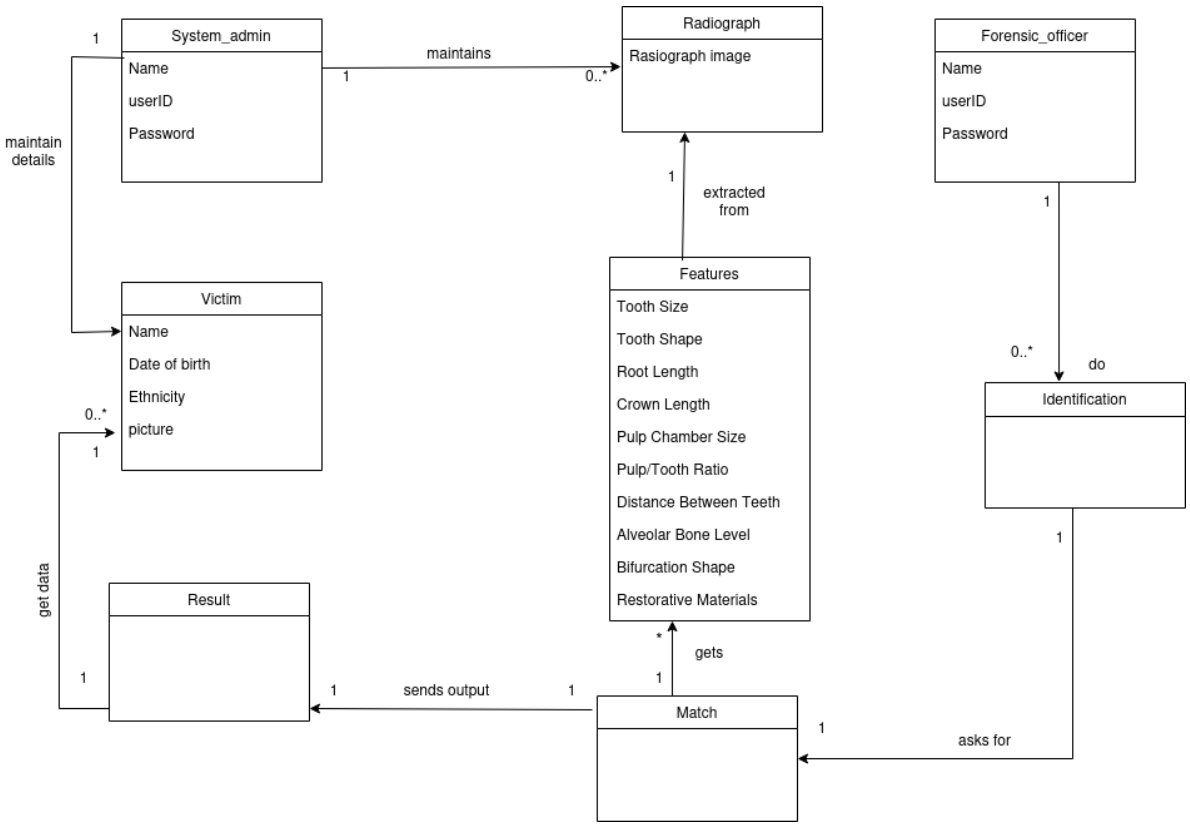

Fig : Domain model of DBS

Class Diagram

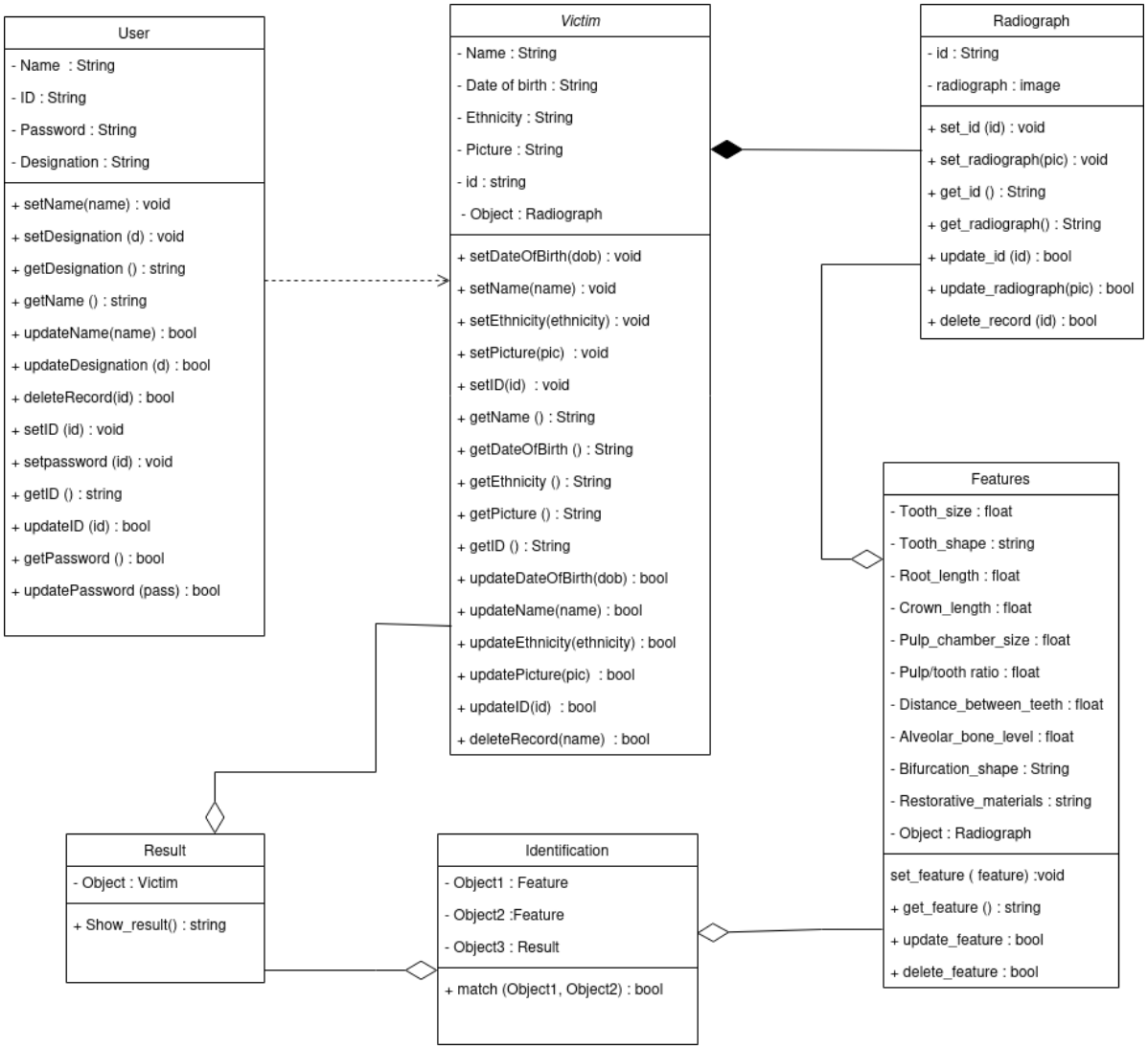

Fig: Class Diagram of DBS

System Sequence Diagrams

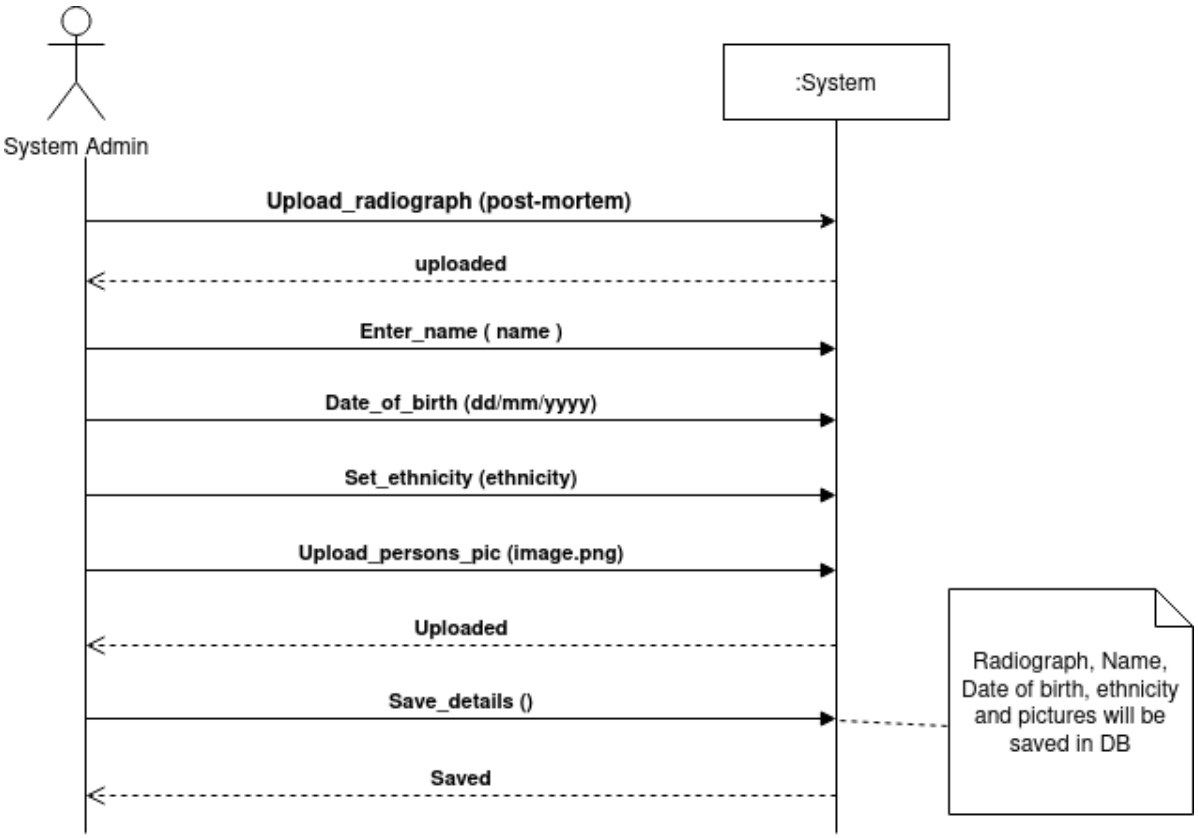

Fig: SSD of enter details and radiograph

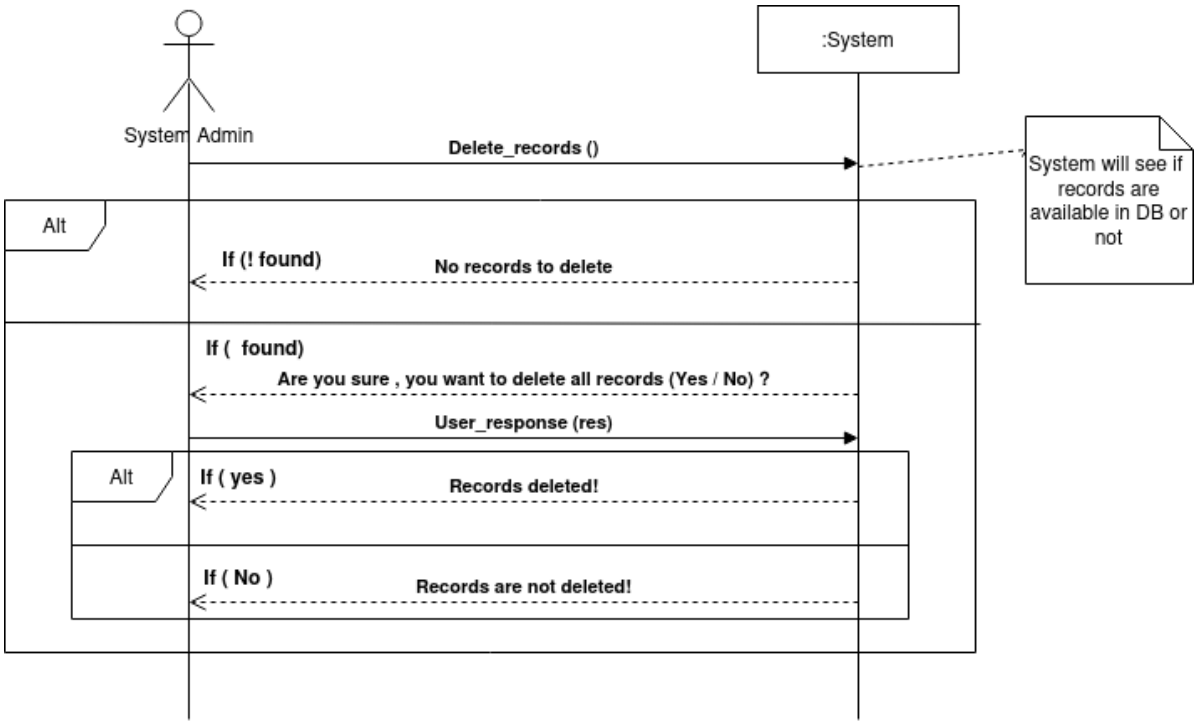

Fig: SSD of delete all records

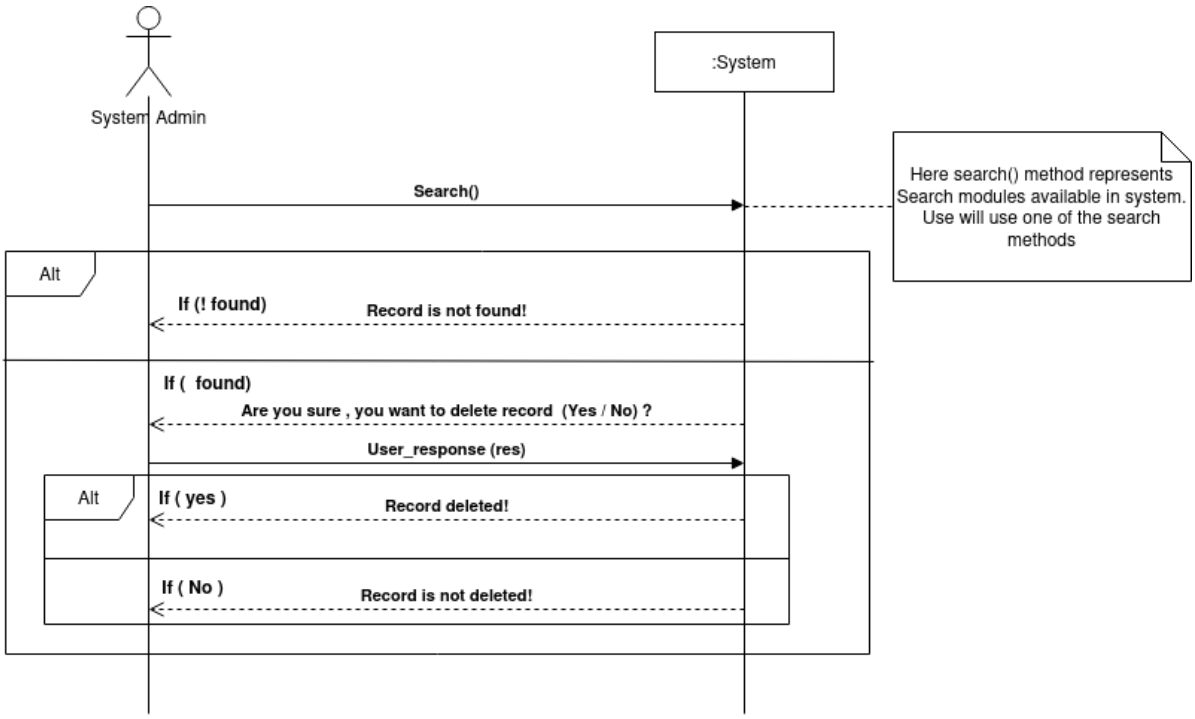

Fig: SSD of delete specific record

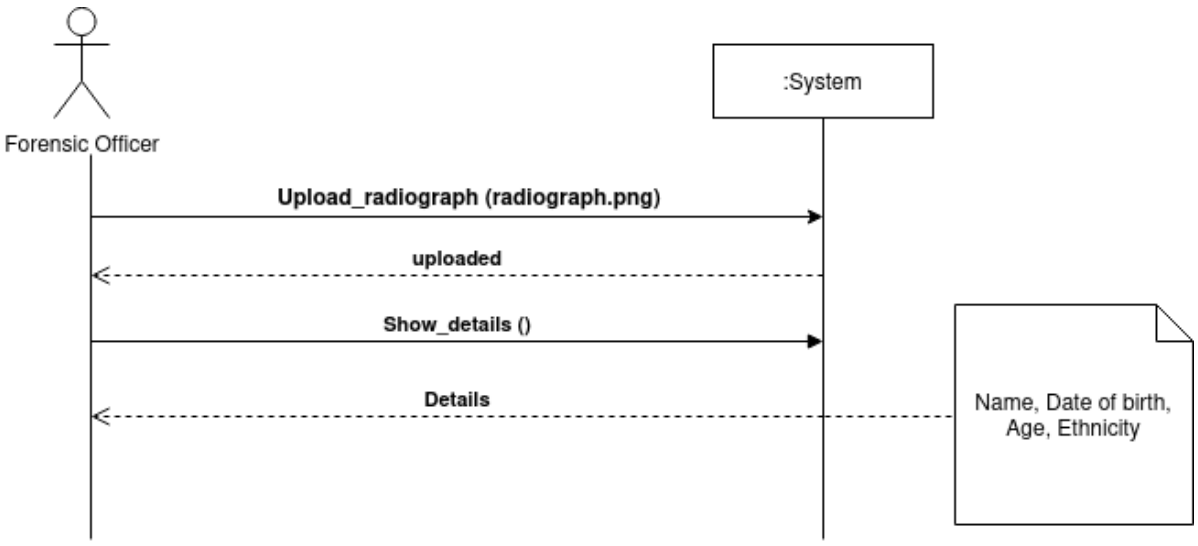

Fig: SSD of find details

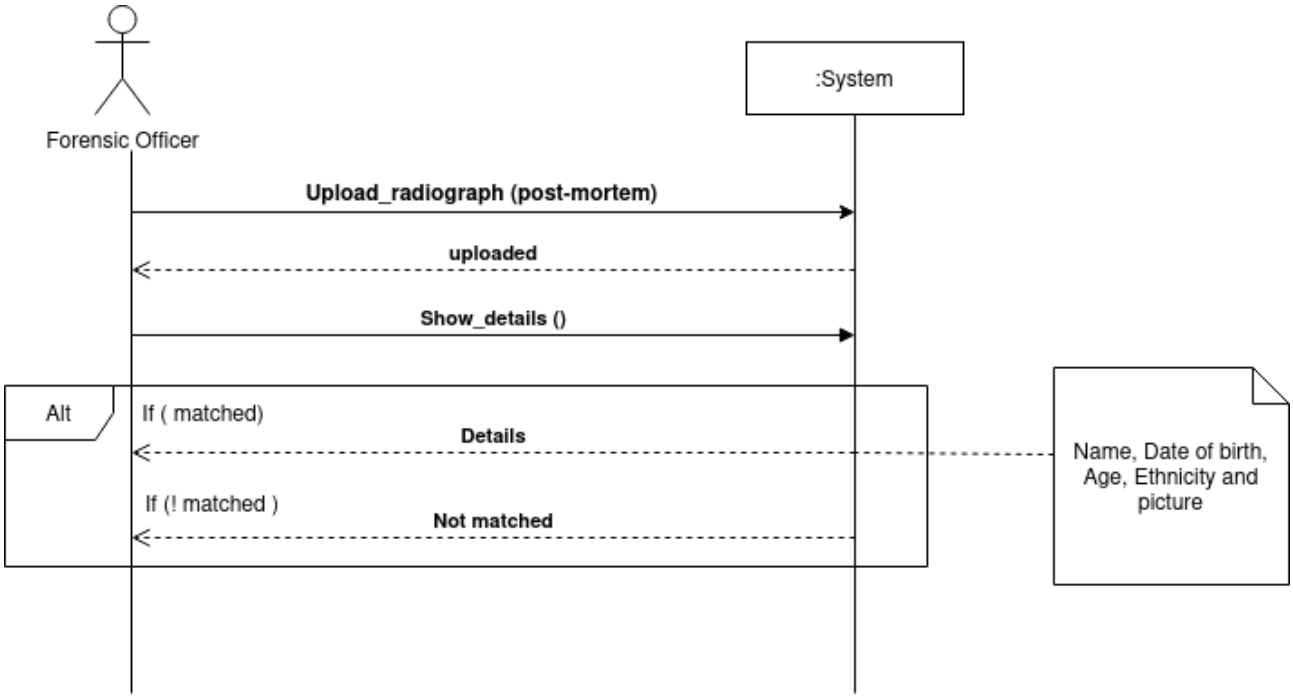

Fig: SSD identify person

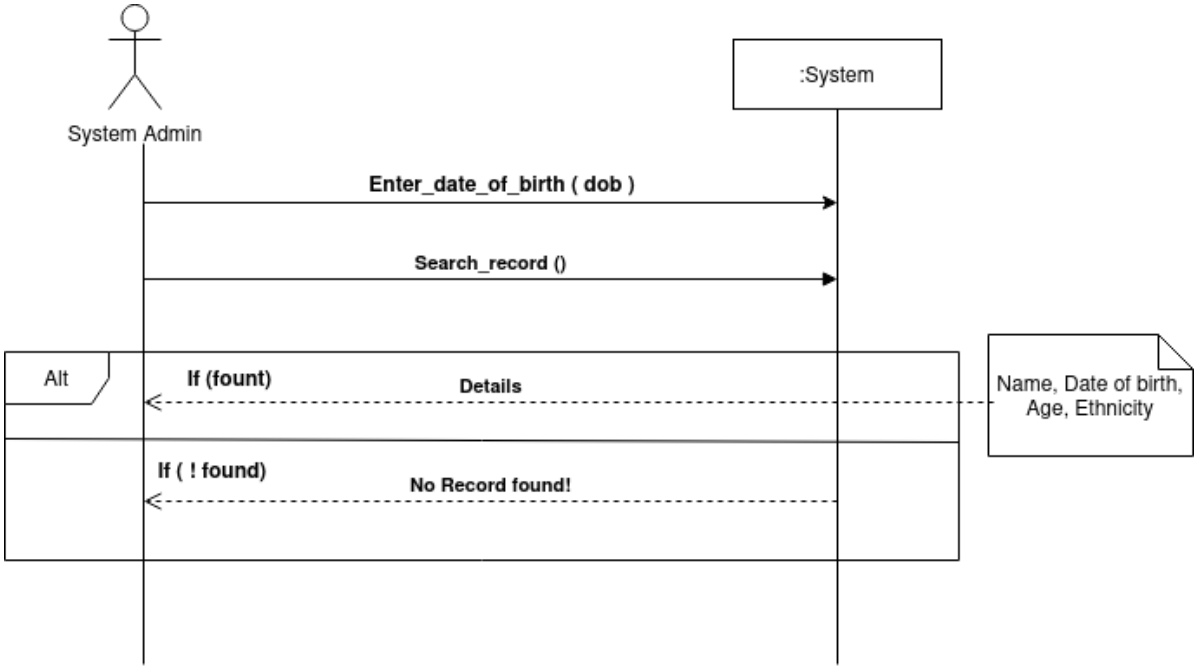

Fig: SSD of Search by date of birth

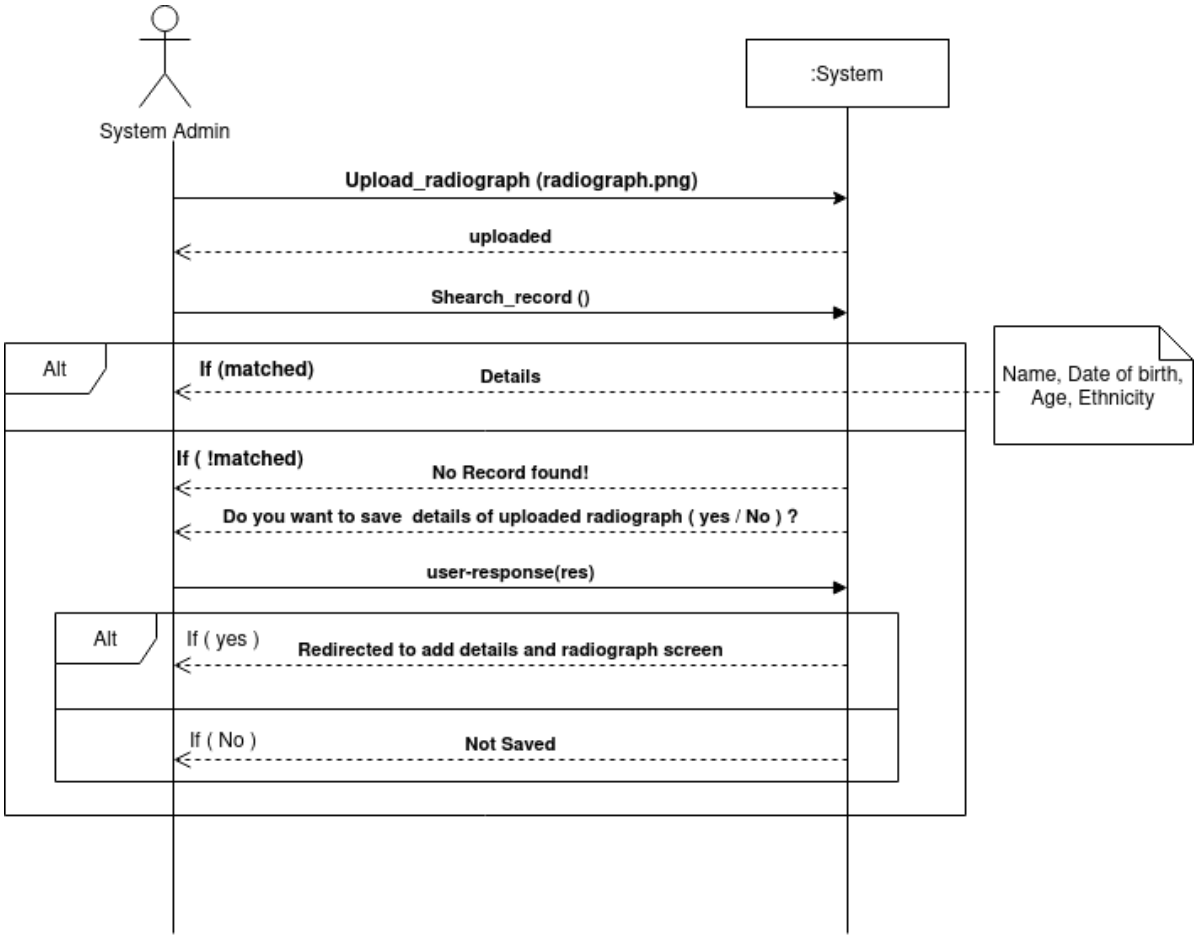

Fig: SSD of search by radiograph

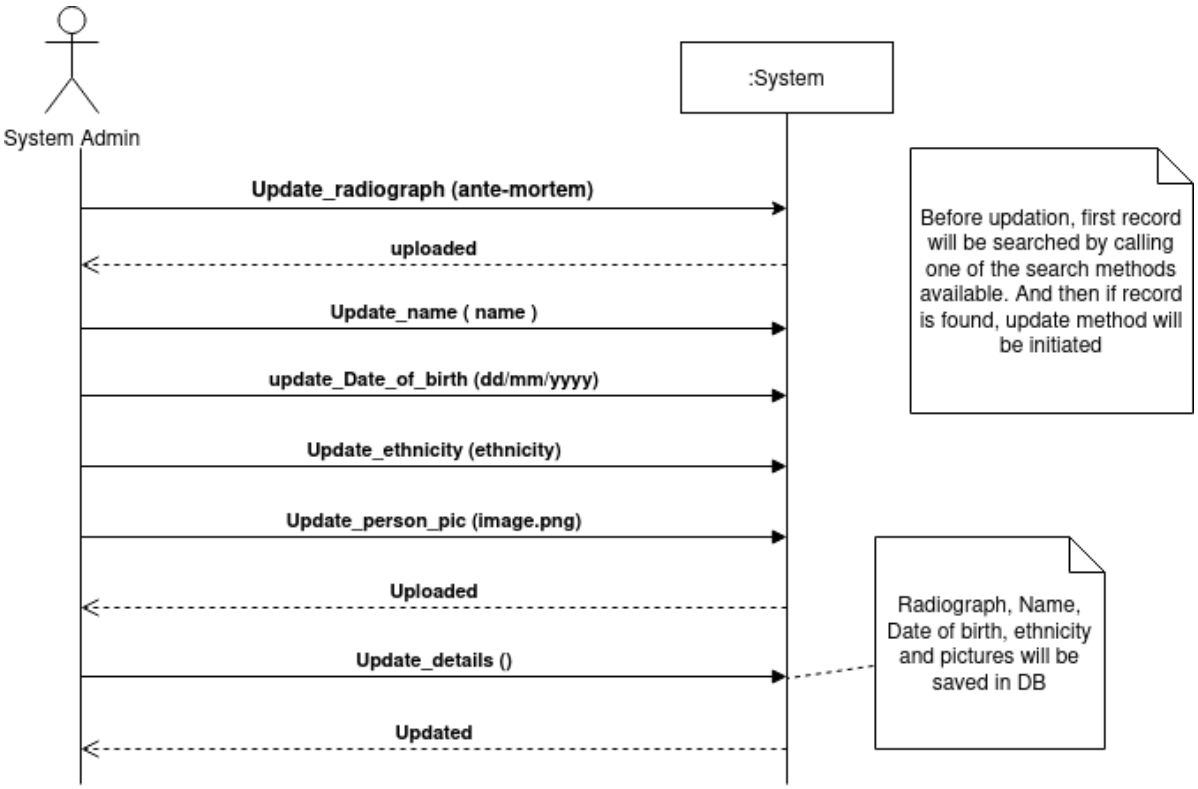

Fig: SSD of update details

Sequence Diagrams

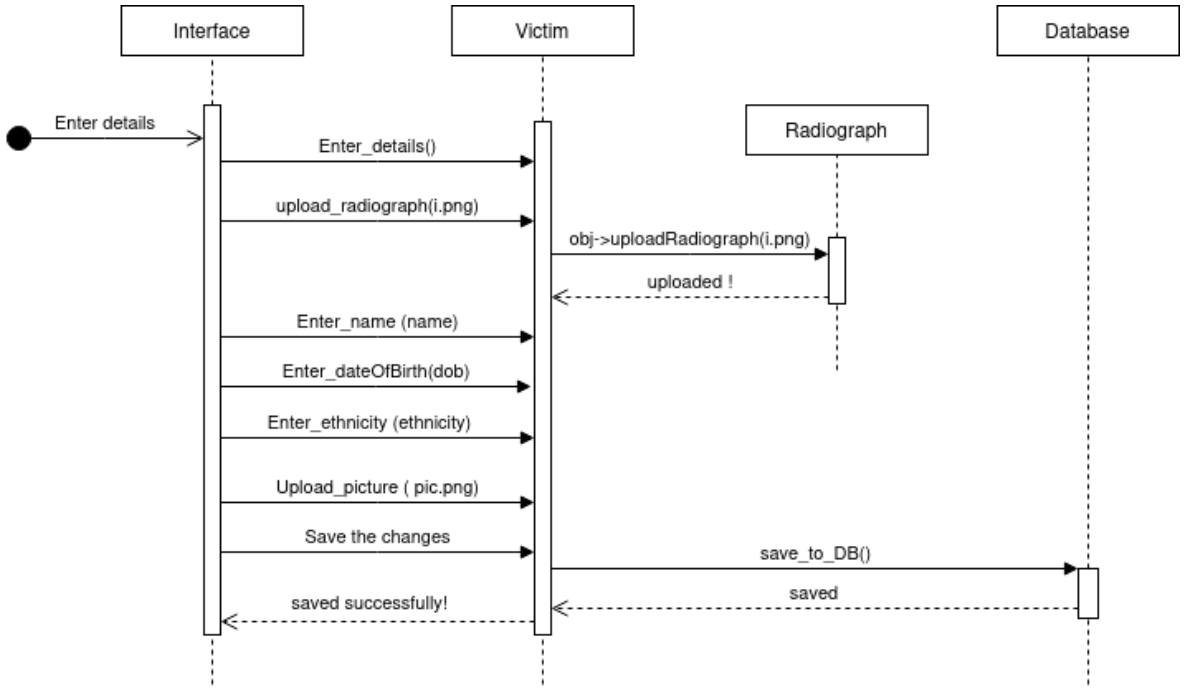

Fig: SD of enter details and radiographs

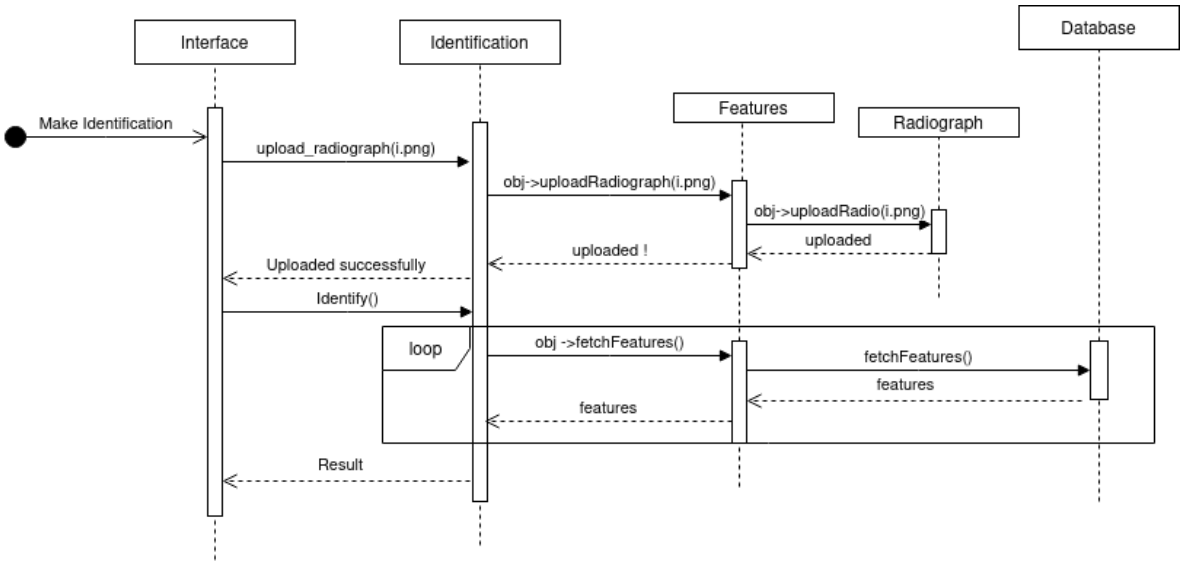

Fig: SD of Identify a person

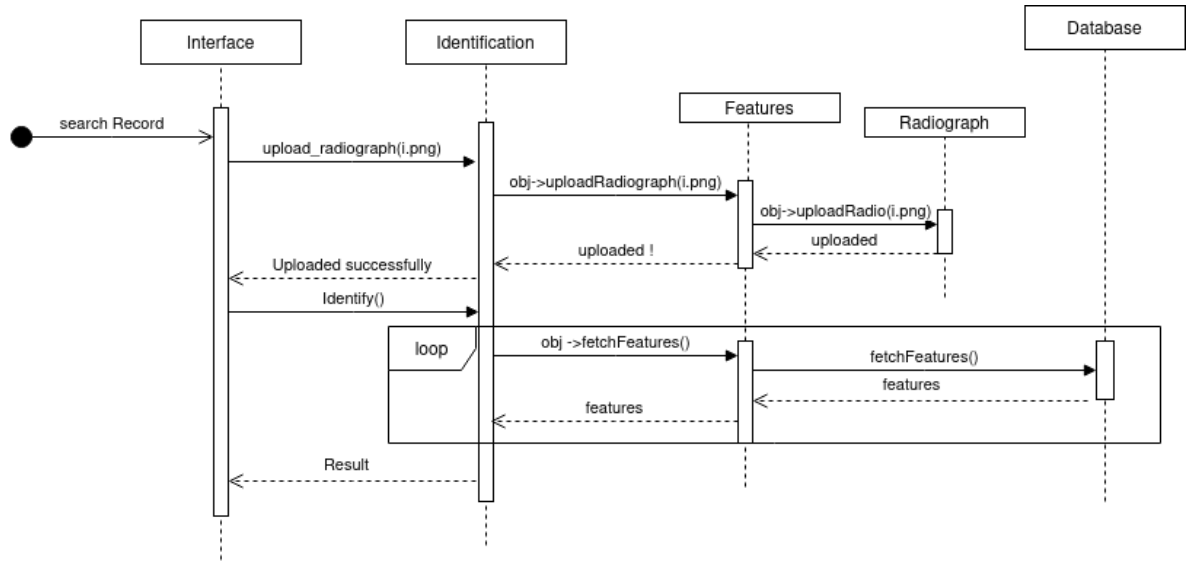

Fig: SD of search by radiograph

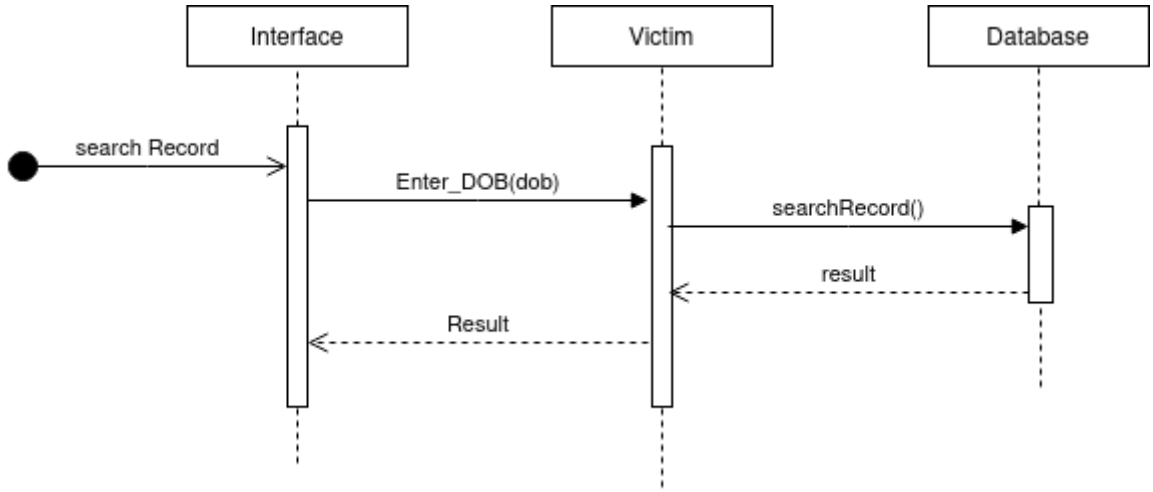

Fig: SD of search by date of birth

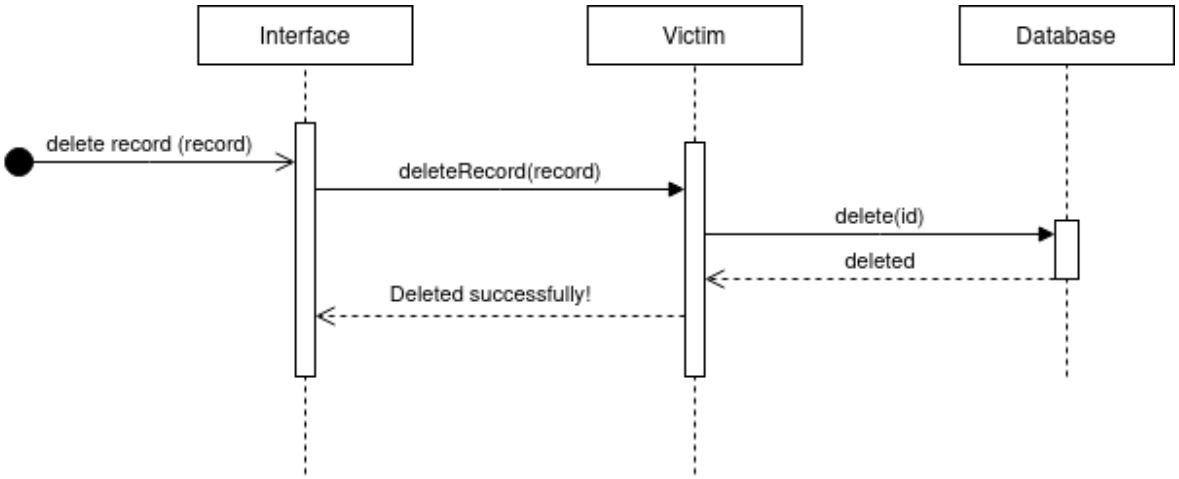

Fig: SD of delete record

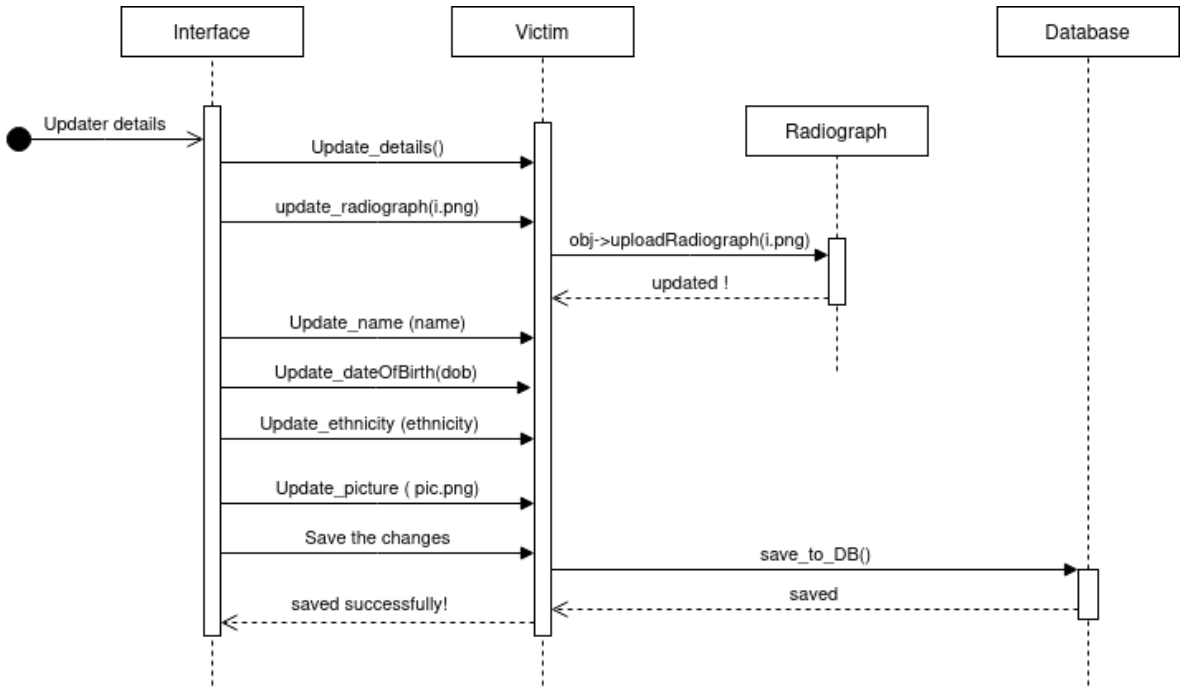

Fig: SD of Update details and radiograph

Schema

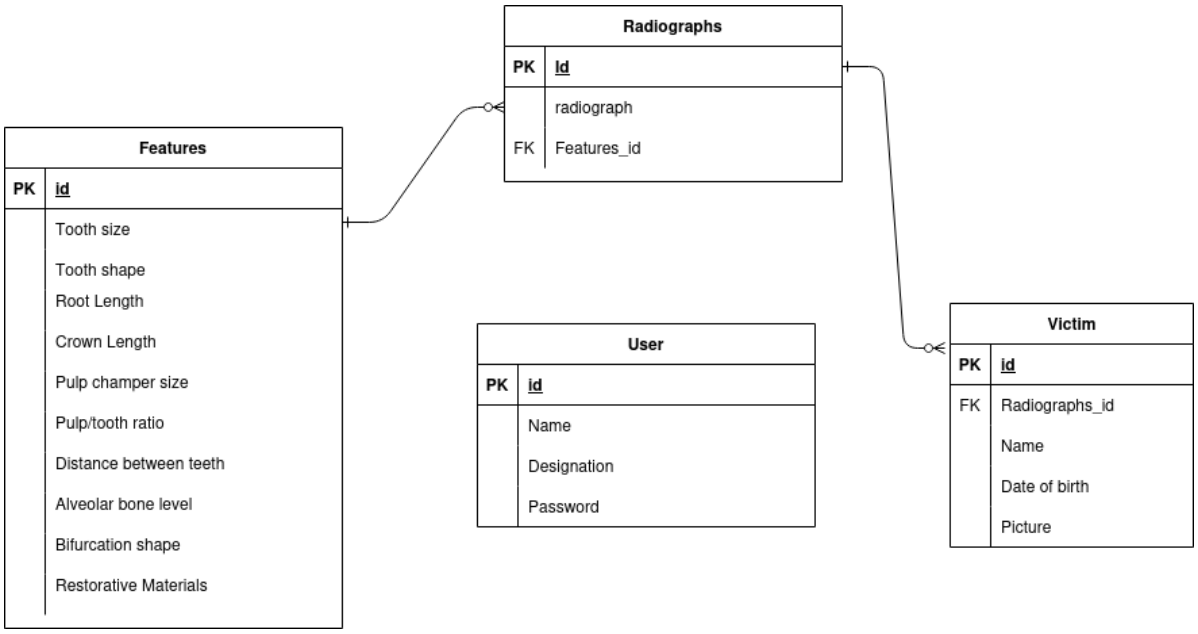

Fig: Schema of DBS