 DOI:10.5281/zenodo.17795962

Title

DESIGN AND IMPLEMENTATION OF VEILFIND: AN AI-ASSISTED DIGITAL SYSTEM FOR BIOMETRIC IDENTIFICATION AND VERIFICATION OF ACCIDENT VICTIMS

Author

ATUPELE BAKILI

Co-Author

MR. MTENDE MKANDAWIRE

Issued November 2026 Certificate

AR2026QYM30S1

publications

ABSTRACT

The identification of accident victims who arrive at hospitals unconscious, severely injured, or without identity documents can be difficult when information is held in separate institutional records and identification depends on manual checks. This paper presents VeilFind, a proposed and implemented web-based prototype intended to support biometric identification and case coordination among citizens, hospitals, police, and system administrators. The platform is designed around role-specific dashboards and workflows for citizen enrolment, document submission, hospital-side victim record capture, police accident reporting, and administrative management. Its technology stack, as documented in the project report, includes React, TypeScript, Tailwind CSS, Vite, Supabase, and GitHub. The design also describes an AI matching capability based on facial and document embeddings, with match confirmation intended to inform subsequent improvement of the matching process. The report documents functional test cases covering registration and role assignment, biometric enrolment, hospital matching, accident logging, administrative approval, role-based access, data privacy, and responsive presentation; all are recorded as passed. However, detailed test logs, independent accuracy measurements, performance benchmarks, formal user-study data, and live integration with national registration, hospital, or police production databases are not provided. The work is therefore best understood as a software prototype demonstrating coordinated workflows and an AI-assisted identification concept, rather than a validated national biometric service.

Keywords: accident victim identification, biometrics, facial recognition, artificial intelligence, Supabase, role-based access control, emergency response, Malawi.

INTRODUCTION

The timely identification of people involved in road traffic accidents and other emergencies is important for emergency care, family notification, police investigations, and related legal or administrative processes. When a victim is unconscious, severely injured, or not carrying identity documents, identification may depend on manual searches, enquiries, or public appeals. These methods can take time and may be inconclusive, particularly when an incident occurs away from the victim's home or community.

The project report identifies fragmented information management between hospitals, police, and national registration authorities as a further challenge. Each institution may maintain records for its own operational needs, while authorised staff may not have a shared channel for checking relevant information during an emergency. This can contribute to duplicated effort and delays in establishing a victim's identity.

VeilFind was developed as a digital platform concept to bring selected identification and case-management workflows into one system. It provides separate interfaces for citizens, hospital personnel, police officers, and administrators. The proposed identification workflow uses facial data and document information to generate embeddings for comparison with enrolled citizen records. The platform is intended to support, not replace, formal identity verification and the established procedures of authorised institutions.

Background of the Study

The project focuses on the practical problem of identifying accident victims who cannot reliably identify themselves. Its proposed workflow starts with citizen enrolment, where identity details, supporting documents, and facial images can be submitted. During an emergency, hospital personnel can capture or upload a victim image and request potential matches. Police users can record an accident, associate victims with an incident, and follow case status.
Administrators manage user access and review submitted registrations.

The project report refers to national registration infrastructure and the National Registration Bureau (NRB) as the intended source of authoritative identity records. It does not demonstrate a live connection to an NRB production database. Accordingly, the integration described in this paper is treated as a design objective and not as an operational government integration.

RESEARCH OBJECTIVES

The overall objective is to design and implement a unified digital platform for biometric

identification and verification workflows involving citizens, hospitals, police, and administrators.

- Provide a citizen-facing enrolment process for personal details, identity documents, and facial biometric data.
- Support hospital personnel in capturing victim information and requesting AI-assisted candidate matching.
- Provide police users with accident reporting, victim linking, and case-status management functions.
- Provide administrative tools for user approval, access management, system monitoring, and reporting.
- Apply role-based access controls and Row-Level Security (RLS) to restrict access to information according to user responsibilities.
- Demonstrate a matching workflow based on face and document embeddings, with match confirmation intended to support iterative improvement.

SYSTEM OVERVIEW

VeilFind is described in the project report as a secure, multi-role web application. The four principal user groups are citizens, hospital staff, police officers, and administrators. The citizen area supports enrolment and document submission; the hospital area supports victim capture and matching; the police area supports accident and case records; and the administrative area supports approvals, user management, monitoring, and analytics.

RELATED WORK AND LITERATURE

The project report frames accident victim identification as a problem involving both biometric technology and coordination between institutions. It discusses traditional approaches such as manual document checks, family enquiries, fingerprints, and DNA profiling, noting that these approaches may be slow or difficult to use in urgent circumstances. The report also refers to research on automated facial recognition for post-mortem identification, including work attributed to *Michalski et al. (2024), Khoo et al. (2020), and Broach et al. (2017).* The report summarises these studies as indicating that facial recognition may assist identification, while also noting that performance depends on image quality and the condition of the face.

The source report further refers to the use of national identity systems and to emergency-response applications such as mySOS and Namola. These examples are included as contextual references for digital public-safety and emergency-support services. The project's proposed contribution is not a new biometric algorithm; rather, it is the consolidation of citizen enrolment, hospital victim capture, police incident records, and administrative oversight within a shared application workflow.

A limitation in the supplied project report is that several studies named in its literature review do not have complete corresponding bibliographic entries in its reference list. In particular, full publication details for *Michalski et al. (2024), Khoo et al. (2020),* and Broach et al. (2017) were not supplied. These citations should be completed and verified before formal academic or journal submission.

Identified gap

The gap identified by the project is the absence, in the described workflow, of a common digital interface through which authorised stakeholders can coordinate victim identification and accident-case information. VeilFind addresses this design gap by bringing together role-specific functions and an AI-assisted matching concept. The current project report does not establish that the platform has been connected to external agency systems or that it has reduced real-world identification times.

METHODOLOGY

The project report states that VeilFind was developed using an Agile software development approach. Agile was selected because requirements could evolve during development and because the platform contains several related modules for different user groups. The report describes iterative development and feedback as part of the development rationale.

Research and development approach

The work followed a software design and

implementation approach. The project requirements were organised around the four user groups and their principal tasks. The design was then expressed through a system architecture, use-case diagram, data-flow diagram, and class design. The implementation was developed as a web application using the technologies listed in Section 1.3. Functional checks were documented for the principal user and administrative workflows.

Scope of evaluation

The evaluation evidence available in the supplied report consists primarily of a test-case table in which eight functional areas are marked as passed. The report does not include raw test execution logs, screenshots tied to each individual test, sample sizes, measured biometric accuracy, response-time distributions, load-test results, or formal survey records. Consequently, the evaluation in this paper reports the documented outcomes without treating them as independently audited measurements.

Ethical, privacy, and security considerations

The project handles categories of information that may be highly sensitive, including identity details, facial images, and accident-related records. The report describes role-based access and Row-Level Security as safeguards intended to limit access to authorised users. Any real deployment would also require clear lawful authority, informed and appropriate enrolment procedures, strict purpose limitation, retention and deletion rules, auditability, human review of potential matches, and controls against false identification. A potential AI match should not by itself be treated as conclusive identity verification.

SYSTEM DESIGN AND DEVELOPMENT

System architecture

The architecture described in the project report is layered. The presentation layer provides separate dashboards for citizens, hospitals, police, and administrators. The application and API layer handles authentication, role-specific workflows, accident reporting, and biometric-processing requests. The AI and intelligence layer is intended to generate face and document embeddings and compare them to enrolled records. The data layer uses Supabase PostgreSQL for application records and related data. A security layer applies authentication, encryption, and access controls across the system.

Use-case design

The use-case design identifies the main actors and their interactions with the platform. Citizens use registration and enrolment functions; hospital personnel use victim-record and biometric-scan functions; police personnel manage accident and case records; and administrators manage accounts and system-level functions.

Data-flow design

The data-flow diagram presents the major processes described in the report, including login and registration, verification, biometric scans, user management, and accident-case uploads. It provides a high-level view of how information moves between the system and its user roles.

Class design

The class design in the source report depicts the principal data entities and their relationships. It is intended to support the management of user accounts, citizen records, accident information, and related system data.

Functional modules

User Management

- Handles user registration and login.
- Manages account roles and access permissions for citizens, hospitals, police officers, and administrators.

Citizen Biometric Enrolment

- Allows citizens to submit personal identity details and supporting documents.
- Captures and stores facial images for subsequent identity matching.

Hospital Victim Identification

- Enables hospitals to capture or upload victim information.
- Supports AI-assisted identification by matching victim information against enrolled citizen records.

Police Accident Management

- Allows police officers to create and manage accident records.
- Associates victims with specific incidents and tracks investigation and identification status.

AI Matching and Intelligence

- Generates facial and document embeddings for identity matching.
- Returns potential candidate matches for further verification.
- Supports the intended use of confirmed matches to improve future model performance.

Administration

- Enables administrators to approve and manage user accounts.
- Provides system activity monitoring, administrative reporting, and audit functions.

Biometric matching workflow

The matching workflow described in the report begins when a hospital user submits an image of an unidentified victim. The system is intended to generate a facial embedding and compare it with embeddings associated with enrolled citizen records. Candidate records are then presented with confidence information for review. A hospital user can confirm a match, and the report describes confirmed matches as feedback for a continual-learning process.

The supplied report does not provide the name or version of a face-recognition model, the embedding dimensions, similarity metric, decision threshold, training dataset description, or measured false-acceptance and false-rejection rates. The implementation should therefore be described as an AI-assisted matching workflow in the project design, not as a scientifically validated biometric identification engine.

Security and access control

The report identifies Row-Level Security (RLS) and role-based access control as key safeguards. The intention is that users see only the dashboards and records relevant to their responsibilities. The backend code excerpt also shows a staff-account creation flow that checks a staff access code before creating an account and assigning a staff role. The supplied material does not include a complete security assessment, penetration-test report, or independent verification of all database policies.

IMPLEMENTATION

The project was implemented as a web application using React and Tailwind CSS for the user interface, TypeScript for application logic, Vite as the build tool, and Supabase for backend services, authentication, and PostgreSQL data storage. GitHub is identified as the version-control platform. The source report also refers to an AI Gateway for embedding generation and matching.

User interface

The supplied report includes screenshots of the landing page, sign-in and account-creation interfaces, and dashboards for citizen registration, hospital victim records, police accident reporting, and administration.

Selected implementation details

The frontend source excerpt demonstrates route organisation for citizen and staff interfaces. It includes route guards that check whether a user is authenticated and whether the user has a citizen, staff, or administrator role before rendering the corresponding layout. The backend excerpt shows a server-side staff-registration function that validates required fields and an access code, creates an authentication account through Supabase, and assigns the staff role in a user_roles table.

These excerpts illustrate selected application-routing and staff-account-management logic. They do not constitute the complete source code for the biometric matching service, database schema, or all application modules. The full implementation would need to be reviewed alongside the deployed code and configuration to verify the exact production behaviour.

RESULTS AND EVALUATION

Functional test results

The supplied project report records eight functional test areas as passed. Table 1 reproduces the reported test areas and expected outcomes. The status values are presented as recorded in the project report; detailed execution evidence was not included in the supplied document.

System Testing Results

User Registration and Role Assignment

- Expected outcome: Successful user registration with the correct role-based access.
- Reported status: **Passed**.

Citizen Biometric Enrolment

- Expected outcome: Facial embedding successfully generated and stored.
- Reported status: **Passed**.

Hospital AI Matching

- Expected outcome: Returns potential matches within seconds, accompanied by confidence scores.
- Reported status: **Passed**.

Police Accident Logging

- Expected outcome: Accident records are successfully created and linked to relevant victims.
- Reported status: **Passed**.

Admin User Approval and Management

- Expected outcome: Administrators can approve or reject registrations and manage appropriate user access.
- Reported status: **Passed**.

Role-Based Access Control

- Expected outcome: Users can only access dashboards and functions authorised for their assigned roles.
- Reported status: **Passed**.

Security (Data Privacy and Row-Level Security)

- Expected outcome: Prevention of unauthorised access to protected data.
- Reported status: **Passed**.

Responsive Design

- Expected outcome: The system interface works on desktop and mobile devices.
- Reported status: **Passed**.

Interpretation of results

The recorded test outcomes indicate that the project report's selected workflows were exercised and marked as successful in the development environment. The tests cover account access, citizen enrolment, hospital matching, police reporting, administrative management, access control, and responsive presentation. They provide preliminary functional evidence for the prototype.

The reported pass status for hospital matching does not, on its own, establish biometric accuracy or reliability. No ground-truth dataset, number of test images, identity-matching benchmark, confidence-threshold analysis, or false-match statistics are provided. Similarly, the reported security result is not a substitute for an independent security audit. Further testing is required before the system can be used for decisions involving real people.

EVALUATION LIMITATIONS

- The project report does not provide raw test logs, test dates, execution counts, or defect statistics.
- No measured biometric accuracy, false-match rate, or false-non-match rate is supplied.
- No response-time benchmark or load and scalability test results are supplied.
- No formal user survey, participant count, or quantitative usability score is documented.
- Live integration with the NRB, hospital information systems, and police production databases is not demonstrated.
- The source report describes a continual-learning capability but does not provide model-training records or

measured improvement over time.

DISCUSSION

VeilFind brings together several workflows that are commonly handled by different organisational units: citizen enrolment, hospital-side victim information capture, police accident reporting, and administrative account management. The role-specific design offers a coherent basis for coordinating these activities within one application. The architecture also separates the user interface, application services, AI-related processing, data storage, and security responsibilities.

The project's central technical proposition is the use of facial and document embeddings to help identify victims when ordinary identity documents are unavailable. This could support emergency personnel by returning candidate records for human review. However, biometric matching is probabilistic and can produce incorrect candidates. Image quality, facial injuries, lighting, age differences, and demographic variation may affect performance. For this reason, the platform should support authorised human verification and alternative identification methods rather than automatically treating a model output as a confirmed identity.

The system's practical value also depends on institutional integration, data quality, governance, and operational readiness. A prototype that stores its own citizen records cannot independently verify identities against authoritative government data. Formal agreements, secure APIs, privacy safeguards, incident-response processes, and operational support would be required before any inter-agency deployment.

FUTURE WORK

- Develop and validate authorised integration with national registration, hospital, and police information systems.
- Extend the platform with a mobile application for field use by police and emergency medical personnel.
- Introduce SMS and email notifications to next of kin only through approved, verified workflows and appropriate consent or legal authority.
- Develop analytics for accident trends and case-management oversight.
- Provide offline or low-connectivity support for remote areas, with secure synchronisation controls.
- Evaluate additional biometric modalities, such as fingerprints or iris recognition, where lawful and technically appropriate.
- Conduct controlled biometric evaluation using documented datasets, ground-truth labels, and clearly reported accuracy and error measures.
- Conduct security, privacy, usability, performance, and accessibility testing before any operational pilot.

CONCLUSION

This paper has presented VeilFind, a web-based prototype designed to support biometric identification and case coordination for accident victims through role-specific functions for citizens, hospitals, police, and administrators. The project report describes citizen enrolment, document submission, hospital victim capture and matching, police accident reporting, administrative management, and role-based access controls. The documented technology stack includes React, TypeScript, Tailwind CSS, Vite, Supabase, and GitHub.

The supplied report records eight functional test areas as passed, providing preliminary evidence that selected application workflows operated in the development environment. Nevertheless, the available evidence does not establish biometric accuracy, production-level security, measurable reductions in identification time, or live interoperability with government and institutional databases. VeilFind should therefore be regarded as an implemented prototype and a foundation for further development. Its progression toward real-world use depends on reproducible technical evaluation, strong data governance, authorised institutional integration, and careful human oversight of biometric matches.

REFERENCES

1. World Bank. (2021). The State of Emergency Medical Services in Sub-Saharan Africa. Washington, DC: World Bank Group. https://documents1.worldbank.org/curated/en/356231613491787852/pdf/The-State-of-Emergency-Medical-Services-in-Sub-

Saharan-Africa.pdf

2. World Bank & UN-Habitat. (2023–2025). Digital Solutions for Public Safety and Emergency Management in Africa. [Full publication details and URL were not supplied in the project report.]
3. Government of Malawi. (2023–2028). National Digital Economy Strategy. Ministry of Information and Digitalization. [Full publication details and URL were not supplied in the project report.]
4. mySOS. (n.d.). mySOS Emergency Response Platform (South Africa). https://mysos.co.za/
5. Namola. (n.d.). Namola Emergency Help and Family Safety App. https://www.namola.com/