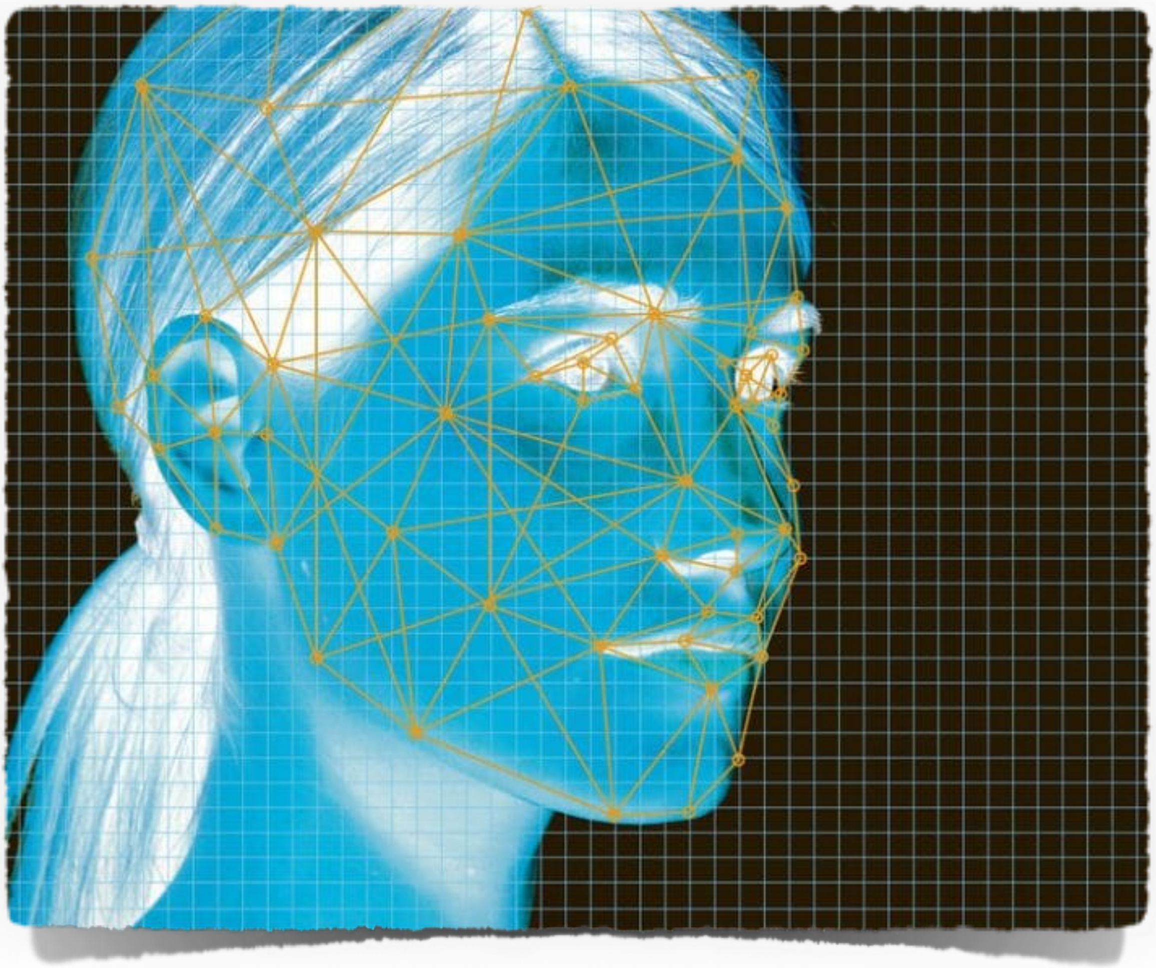
I.S.A.B.E.L



Intelligent Security Algorithm for Biometric enabled Encryption & Localisation

University of Medical Sciences and Technology

Abubakr Osama Abubakr

23 February 2022

Proposal number: 2022-03

CONTENTS

INTRODUCTION

"With **Biometric security**. *Your new password is* **your identity."**

A security system that extracts biometric data from individual faces and generates embeddings(encodings).

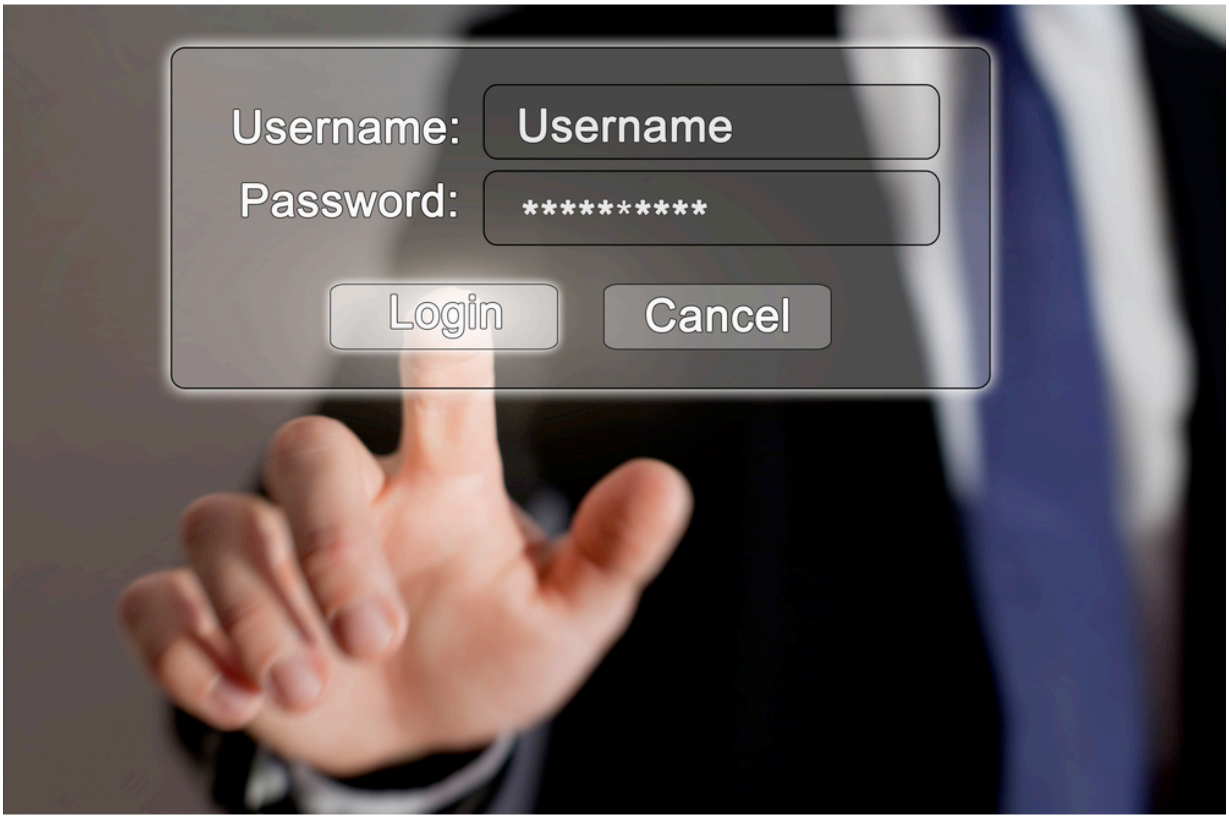
A generated embedding is then converted to a SHA-256 hash which provides users with encryption functionality (eg. file encryption, generating private keys and secure user authentication).

Abubakr Osama Abubakr
Semester 6, Bachelor of *Computer Science.*
Faculty of Computer Science.

24 February **2022**

PROBLEM STATEMENT

Over the years, traditional text based password have become susceptible to theft, brute-force attacks and credential loss. This created several vulnerabilities within legacy systems.



Our current password systems no matter how complex are susceptible to loss, interception or synthesis.
These issue open a up a can of vulnerabilities and creates daunting hurdles for user.

OBJECTIVES

▸ Primary Objectives

- Employ a ***computer-vision*** algorithm to enable user ***verification*** and ***identification***.
- Define a ***cryptographic*** hash function derived from ***user biometric*** data.
- Utilise ***biometric*** enabled ***transcription*** to handle ***non-volatile*** user credentials.
- Facilitate offline access to ***secure operations*** (eg: *storage, allocation , deallocation*).
- Outline a biometric-based approach to achieve total ***decentralisation*** of credential storage.

▸ Secondary Objectives

- Enhance current security standards through ***model encryption practices***.
- Provide ***error and effort free*** authentication an intuitive interface.
- Deploy ***user-centric*** designs to address individual ***preferences*** and ***access limitations***.
- Increase ***verificational complexity*** by using ***2-factors*** authentication.

METHODOLOGY

TECHNOLOGY

To achieve our goal of providing user identification and secure authentication we will implement a face detection and identification algorithm.

ARCHITECTURE

The algorithm will extract face encoding during a test run / operation and cross reference the encoding against a registry of known faces. This registry will be created during pre-training and then new faces will cross referenced against the registry, deemed either as an existing entry or new entry. The system computes an estimate of expected face encoding from multiple sets of images and this expected Value x will represent the encoding of the face, when a test is ran a distance algorithm(Euclidean distance) will assess the likely hood of an entry being that exact face. Beyond face recognition each unique face encoding will be linked to a randomly generated SHA-256 Hash, this would be achieved via dictionary list. Users will be able to utilise these face generated hashes to encrypt and decrypt data, essentially functioning as secure portable lossless secondary key.

THE FRAMEWORK

To achieve these results we will utilise 2 libraries

- **OpenCV:**
  Provides the underlying core computer vision functionalities for the program.
- **OS:**
  Library to manipulate the OS and provide OS specific functionality (File creation, deletion, movement, cloning, etc.)
- **FASTAPI:**
  Enables essential API services that allow for cross compatibility and ease off utilisation.

PROGRAMMING LANGUAGE

Our Language choice for the implementation of this project is the “**python**” *programming language.*

PROJECT SCOPE

Enable User Verification services.

Perform User-Authenticated operations.

Provide user-secured cryptographic operations.

Provide a lossless secure credential system.

EXPECTED OUTCOMES

- The development of a standalone security service that provides independent and secure authentication services.

- Centralisation and compilation of independent security services through one mode of authentication.

- Integration of our Biometric Security system into existing security services.

- Face Encryption and verification services.