Web-Based Facial Authentication System

INFORMATION ASSURANCE AND SECURITY

Prepared By :

- Yosr Boussarsar
- Islem Hamzaoui
- Eya Essid
- Eya Trabelsi
- Wadii Selman

TABLE OF CONTENT

INTRODUCTION

- Facial authentication is taking the web by storm, offering a ***secure*** and ***convenient*** way to ***log in*** to applications and access online services.
- This report sheds light on the ***core concepts*** of web-based facial authentication systems, exploring their unique characteristics and how they ***function*** within the web environment.

MAIN COMPONENTS

- **Web Interface:** This user-friendly interface on a web browser allows users to interact with the facial authentication system. It typically includes a webcam capture functionality and instructions for the user.
- **Client-Side Processing (Optional):** In some systems, basic facial feature extraction or preprocessing might occur on the user's device before sending data to the server.
- **Secure Communication Channel:** Encrypted communication protocols like HTTPS ensure the safe transmission of facial data between the user's device and the server.

MAIN COMPONENTS

- **Server-Side Processing:** The core functionalities reside on the server. Here's what happens:

    1. **Facial Recognition Engine:** This engine, powered by machine learning algorithms, analyzes the captured facial image and extracts key features.
    2. **Feature Database:** A secure database on the server stores authorized users' facial feature representations.
    3. **Matching and Verification:** The extracted features are compared against the database using matching algorithms.

- **Authentication Decision:** Based on the matching score, the system determines whether to grant access or prompt for alternative credentials.

FUNCTIONAL FLOW

- **Webpage Access:** A user visits a website or application requiring facial authentication.
- **Web Interface Interaction:** The user interacts with the web interface, potentially granting permission to access the webcam.
- **Facial Image Capture:** The webcam captures a live image of the user's face
- **Data Transmission (Optional):** In some cases, preprocessed facial data might be sent to the server.
- **Secure Communication**:Encrypted protocols ensure secure data transfer between the user's device and the server.

FUNCTIONAL FLOW

.

- **Server-Side Processing:** The server performs facial feature extraction, compares features with the database, and makes an authentication decision.
- **Authentication Response:** The server sends a response back to the web interface, granting access or prompting for further action.
- **Access Granted/Denied:** Based on the server's response, the web interface displays a success message or prompts for alternative login methods.

FACIAL RECOGNITION– A KEY COMPONENT

The **facial recognition process**, a key component of web-based authentication systems, utilizes biometric technology to analyze and identify individuals based on facial features.

- It starts with capturing facial images and extracting unique characteristics, which are then converted into mathematical templates for comparison with stored data. Matching algorithms assess similarity to authenticate users, granting or denying access accordingly.
- Continuous refinement mechanisms enhance accuracy over time.

The next section will focus on this process.

FACIAL RECOGNITION PROCESS

MAIN COMPONENTS

- **Image Acquisition:** The system begins by capturing a facial image using a camera.
- **Face Detection:** This stage identifies the presence and location of a face within the captured image. Algorithms analyze the image for specific features like eyes, nose, and mouth to isolate the face region.
- **Feature Extraction:** Once a face is detected, relevant facial features are extracted. These features can be geometric (distances between facial landmarks) or textural (patterns of wrinkles or blemishes).
- **Feature Comparison:** The extracted features are compared against a database of known faces. This database stores facial feature data of authorized individuals.
- **Matching and Recognition:** A matching algorithm compares the extracted features with entries in the database. If a sufficient match is found, the system recognizes the individual.

THE MATH AND ALGORITHMS BEHIND FACIAL RECOGNITION

Chapter 1: **The Biometric Concept:**

Our facial recognition process begins with facial detection, the crucial first step. Here, the system needs to identify the presence and location of a face within the captured image.

- **Algorithm: Haar Cascade Classifier**

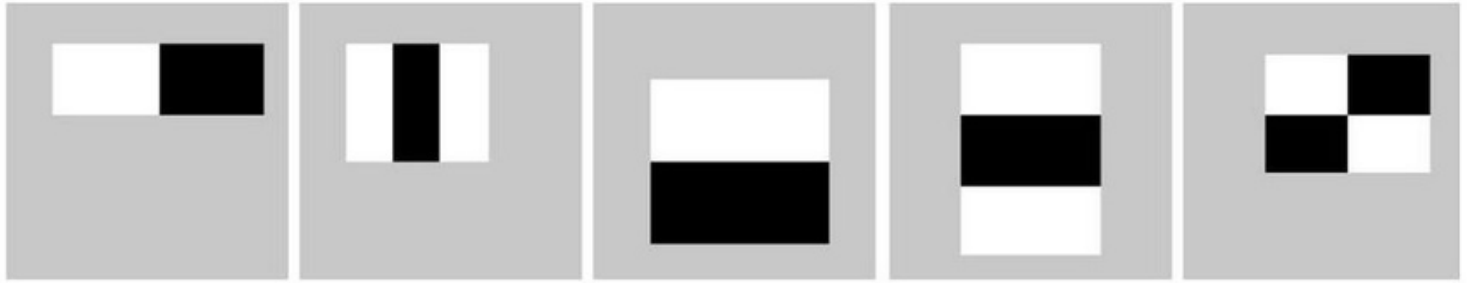
(Inescapable for Real-Time Systems)

This machine-learning algorithm thrives in real-time environments.

It dissects the image into Haar features, which are simple edge and line patterns.

By efficiently identifying these patterns within the image, the Haar cascade classifier can pinpoint the presence of a face.

HAAR CASCADE



(a) Edge Feature (b) Line Feature (c) Edge Feature (d) Line Feature (e) Four-Rectangle Feature

THE MATH AND ALGORITHMS BEHIND FACIAL RECOGNITION

Chapter 2: Dimension Reduction - Capturing the Essence

Once a face is detected, we need to extract its unique characteristics for recognition. However, facial images are high-dimensional, containing a large number of pixels. Here's where dimension reduction techniques come into play.

- **Algorithm: Principal Component Analysis (PCA)**

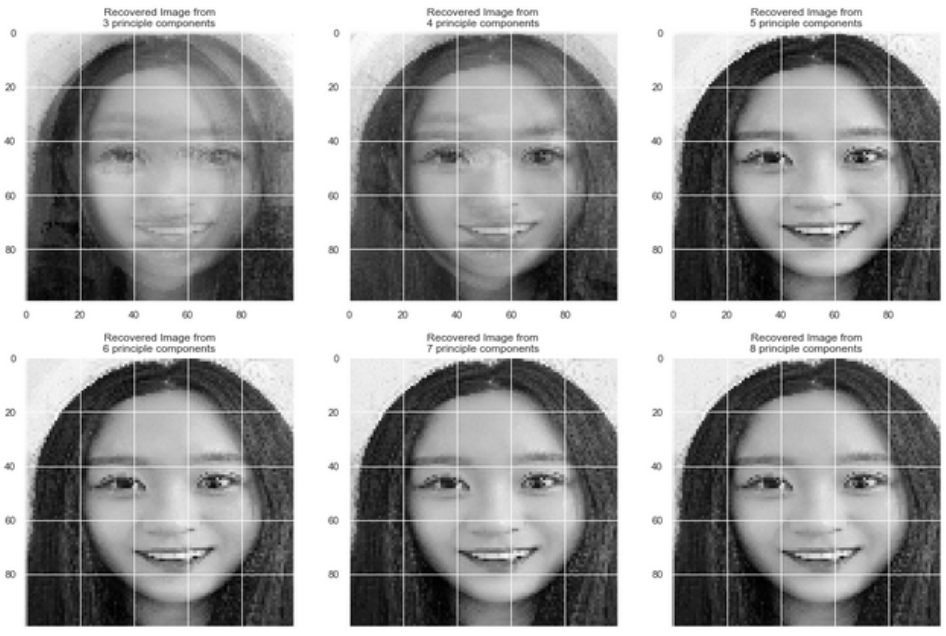
PCA, also known as Eigenfaces, tackles the high dimensionality challenge. It analyzes the variations within a set of facial images and identifies the most significant patterns that distinguish one face from another PCA.

PRINCIPLE COMPONENT ANALYSIS

Then projects these high-dimensional images into a lower-dimensional subspace, capturing the essence of a face while reducing processing requirements. While PCA offers a solid foundation, future advancements might involve:

Sparse Representation Techniques:

These techniques aim to represent facial features using a combination of only a few basis vectors, potentially achieving even greater compression compared to PCA.



THE MATH AND ALGORITHMS BEHIND FACIAL RECOGNITION

Chapter 3: Matching Algorithms - The Recognition Arena

- Now that we have a compact face representation, it's time for recognition.
- Matching algorithms compare the extracted features (Eigenfaces) of the unknown individual with the known faces stored in the database

- **Algorithm 1: Eigenface (PCA) Matching**

(A Classic Approach) Building upon the dimension reduction stage, PCA matching compares the projected facial image (Eigenface) of the unknown person against the Eigenfaces in the database.
The system identifies the closest match, potentially recognizing the individual.

THE MATH AND ALGORITHMS BEHIND FACIAL RECOGNITION

- **Algorithm 2: Local Binary Patterns (LBP) Matching**

- LBP offers an alternative approach.
- It focuses on capturing the local textural variations within the facial image.
- By analyzing small image regions and encoding pixel intensity patterns, LBP creates a unique feature descriptor.
- The system then compares the LBP features of the unknown face with those stored in the database for recognition.
- **LBP is a robust technique, particularly in scenarios with variations in lighting conditions.**

LOCAL BINARY PATTERNS

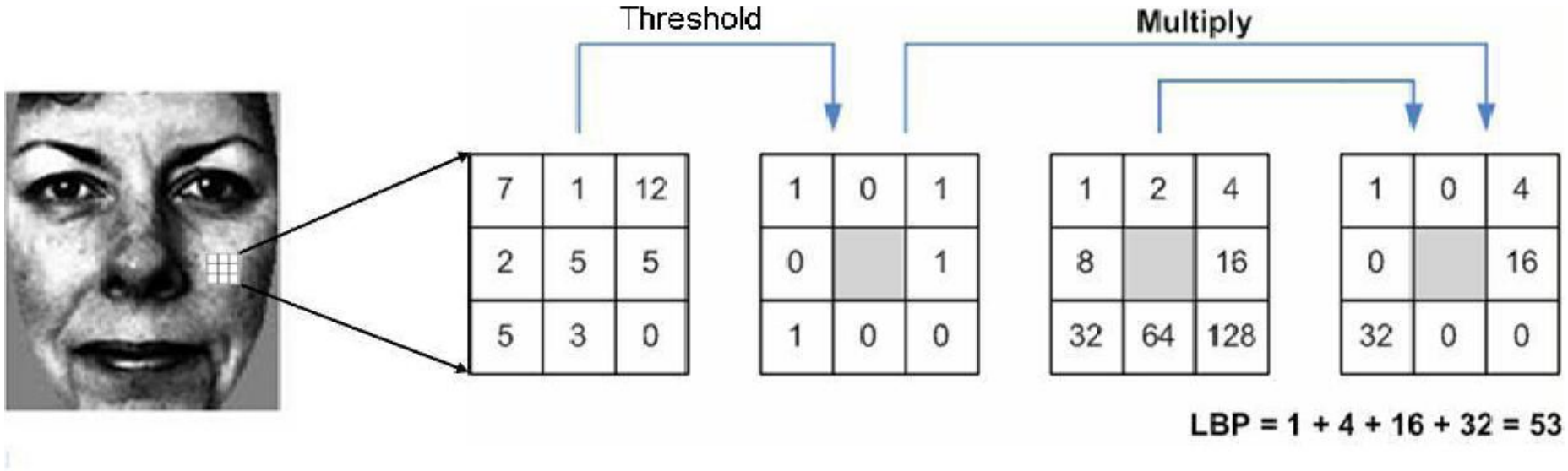
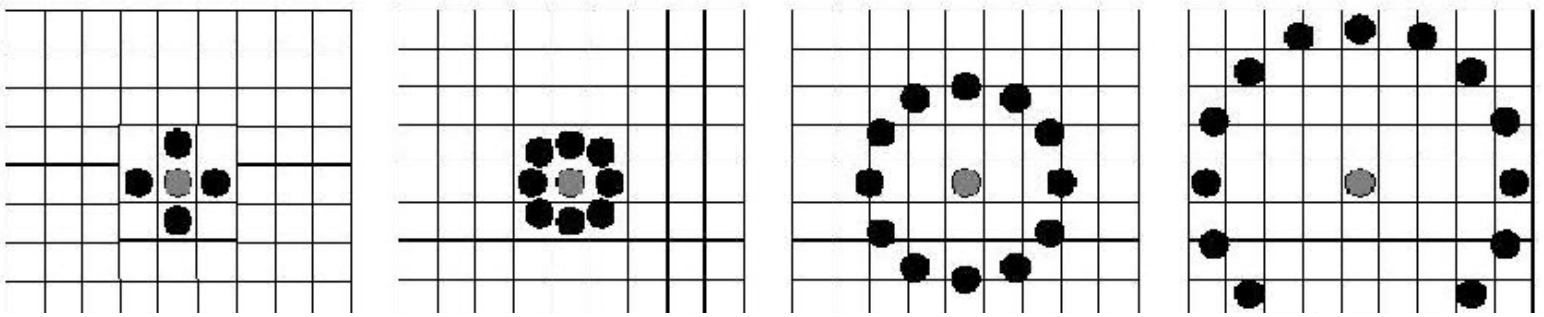


Fig. 1. Example of an LBP calculation



THE MATH AND ALGORITHMS BEHIND FACIAL RECOGNITION

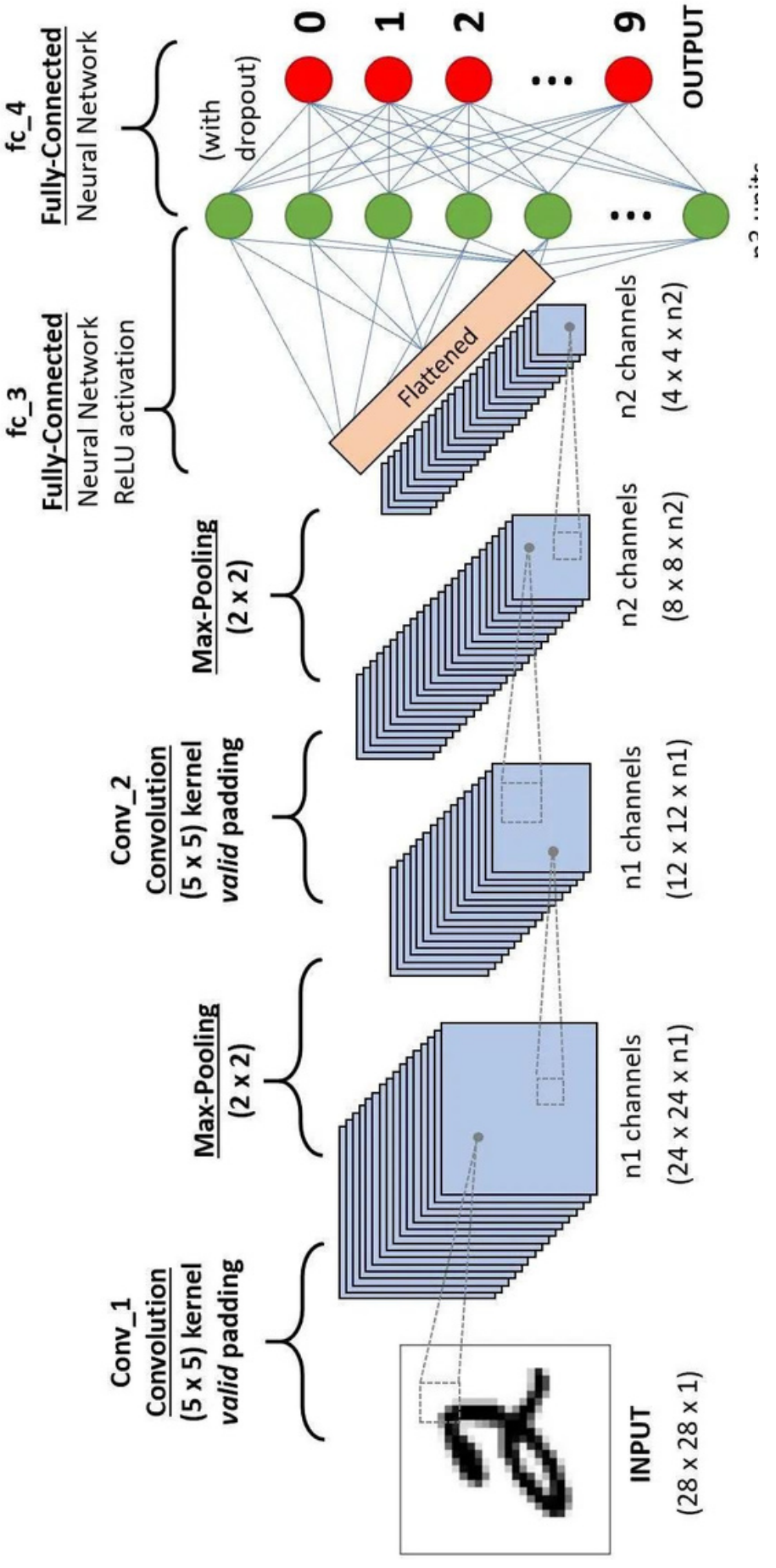
Chapter 4: Deep Learning For the Facial Recognition

While PCA and LBP offer strong foundations, facial recognition is witnessing a paradigm shift toward deep learning techniques, particularly

Convolutional Neural Networks (CNNs):

- CNNs eliminate the need for predefined features.
- Unlike traditional methods, they function as intelligent feature detectors, analyzing spatial relationships between pixels in face images.
- Specialized CNN layers capture the arrangement of features like eyes and nose, progressing from recognizing basic shapes to intricate facial details through a learning process.

CONVOLUTIONAL NEURAL NETWORKS



BIBLIOGRAPHY AND REFERENCES

1. LI, S.Z., JAIN, A.K. (2011). HANDBOOK OF FACE RECOGNITION. SPRINGER SCIENCE & BUSINESS MEDIA.

2. TURK, M., PENTLAND, A. (1991). "EIGENFACES FOR RECOGNITION." JOURNAL OF COGNITIVE NEUROSCIENCE, 3(1), 71-86.

3. ISO/IEC 19794-5:2005 INFORMATION TECHNOLOGY BIOMETRIC DATA INTERCHANGE
FORMATS - PART 5: FACE IMAGE DATA

4.TURK, M., & PENTLAND, A. (1991). EIGENFACES FOR RECOGNITION. JOURNAL OF COGNITIVE NEUROSCIENCE, 3(1), 71-86.

5.VIOLA, P., & JONES, M. (2001). RAPID OBJECT DETECTION USING A BOOSTED CASCADE OF SIMPLE FEATURES. PROCEEDINGS OF THE IEEE COMPUTER SOCIETY CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION.

6.GOODFELLOW, I., BENGIO, Y., & COURVILLE, A. (2016). DEEP LEARNING. MIT PRESS. BISHOP, C. M. (2006). PATTERN RECOGNITION AND MACHINE LEARNING. SPRINGER.

7.JAIN, A. K., ROSS, A., & NANDAKUMAR, K. (2016). INTRODUCTION TO BIOMETRICS. SPRINGER.

Thank You