Dynamic Human Authentication System

Mohin Pasha Mohammad[a], Sai Keerthi Domakonda[a], Sai Rishi Kiran Mannava[a]

[a]*Purdue University Fort Wayne, Computer Science Department, Fort Wayne, 46805, Indiana, USA*

Abstract

The project aims to achieve a Dynamic Human Authentication System utilizing the Local Binary Patterns Histogram (LBPH) Algorithm to enhance security in organizations. Focused on preventing unauthorized access, the system uses real-time face recognition technology. It involves storing authorized personnel images in a database and alerting security when an unrecognized individual attempts entry. The project emphasizes the use of Python, OpenCV, and IP cameras, showcasing a high accuracy rate in detecting unauthorized entries, thereby significantly improving security in sensitive environments.

Keywords: Dynamic Human Authentication, Local Binary Patterns Histogram (LBPH), Face Recognition

1. Introduction

In today's highly competitive world, ensuring comprehensive security is crucial for the survival of any organization. Security threats can come in various forms, including virtual intrusion through unethical hacking and physical intrusion involving illegal access to premises. These threats can potentially cause irrecoverable losses to businesses. To address this need, there is a growing necessity to automate security processes and enhance the capabilities of security personnel.

One promising solution is the development of a Dynamic Human Authentication System. This software aims to identify and monitor individuals entering a facility, particularly those visiting for the first time, and promptly report such instances to security officials. The system utilizes advanced technology, including the Local Binary Patterns Histogram (LBPH) Algorithm, to achieve this task. It maintains a database of authorized personnel within the organization and generates alerts when an unknown individual attempts to access restricted areas.

While facial recognition technology has made significant strides in authentication, dynamic human recognition presents unique challenges. This software seeks to provide a tailored solution for each entrance gate, accurately identifying every unique person entering or exiting, recording their entry/exit times, and capturing photos/videos as needed. If a new person is detected, the system immediately alerts security personnel, who can then decide whether to allow or restrict access. Furthermore, the system continuously learns from its historical data to improve its recognition capabilities for known individuals.

The solution also considers factors such as the optimal number and resolution of cameras required for each gate, making it a scalable and open-source solution. This Dynamic Human Authentication System is particularly suited for organizations like ISRO and DRDO, as well as any firms that prioritize high-end, end-to-end security.

2. Motivation

The motivation behind this work is to develop an automated solution to eliminate physical intrusions into high-security organizations such as DRDO and ISRO, which play a crucial role in the nation's welfare and development. The primary goal is to prevent illegal physical intrusions that could potentially lead to security threats and data breaches. The software aims to enhance security by allowing constant monitoring of individuals entering and exiting these facilities without relying solely on human security personnel. This approach also reduces the possibility of human error in security decisions.

2.1. Problem Description

The problem is the unauthorized physical intrusion into secure premises, which could result in severe consequences, including acts of terrorism or espionage. The goal is to create a system that can identify and distinguish between authorized and unauthorized individuals attempting to enter these facilities. The system must be capable of generating alerts and notifying security personnel in real-time when an unauthorized person is detected.

2.2. Applications

The proposed system has applications in high-security organizations such as DRDO, ISRO, and other critical facilities. It aims to prevent security breaches, terrorist attacks, and data theft by automating the process of identifying and monitoring individuals entering these premises.

2.3. Challenges

The challenges in this work include:

Develop robust facial recognition algorithms capable of accurately identifying individuals.

Ensuring the security and integrity of the software to prevent unauthorized access and manipulation.

Integrating hardware components like cameras and Raspberry Pi effectively.

Handling the scalability and adaptability of the system for various entrance points and sizes.

Minimizing false positives and negatives in the authentication process.

3. Problem Statement

The problem is the unauthorized physical intrusion into secure premises, which could result in severe consequences, including acts of terrorism or espionage. The goal is to create a system that can identify and distinguish between authorized and unauthorized individuals attempting to enter these facilities. The system must be capable of generating alerts and notifying security personnel in real-time when an unauthorized person is detected. The perpetrators try to explode the firms to cause irrecoverable losses to enemies. There comes the necessity to automate the process of providing security. Security personnel's responsibility must be robust to fight against the creation of deliberate havoc. This prototype aims to accomplish this task by being most efficient at providing security. The stranger is identified and is precluded from entering the premises.

3.1. Related Work

Current alerting systems are often limited to home use and lack scalability for organizational needs. Addressing this gap, ALARM.COM specializes in providing comprehensive monitoring systems designed for internal security on an organizational level. Unlike typical home-focused solutions, ALARM.COM's services are tailored to meet the demands of businesses, offering advanced features and scalability. Their systems enable efficient monitoring, real-time alerts, and a heightened level of security measures, ensuring that organizations can effectively manage and respond to security threats across their entire infrastructure. ALARM.COM stands as a robust solution, bridging the gap to provide advanced security measures for organizational settings. Two approaches are considered: A software-oriented approach using the OpenCV library and the LBPH face recognizer for facial recognition. Hardware-oriented approach using a Raspberry Pi module for facial recognition and data storage. The software-oriented approach involves using computer vision techniques to detect and recognize faces in real time, comparing them to images in the database. The hardware-oriented approach offloads the facial recognition task to a Raspberry Pi module, which interacts with cameras and stores recognized faces in the database.

4. Background Concepts

4.1. Current System

In the current security landscape, there is a need for alerting systems that can provide security not only at the home level but also at the organizational level. Existing applications like FrontPoint, ADT, Google Nest, Brinks, Adobe, Vivint, and SmartHome are available in the market but are not easily extendable to the needs of organizations. These systems often require technical expertise for installation and maintenance and can be expensive. Additionally, they may not be user-friendly for the average person. ALARM.COM is one company that offers monitoring systems for internal security, focusing on aspects such as stock monitoring in warehouses, intrusions, and inventory theft or misutilization. It provides alerts to the relevant authorities in case of security breaches.

4.2. Proposed System

The proposed Dynamic Human Authentication System aims to address the limitations of existing security systems. It is a software solution designed to detect individuals entering a campus or facility for the first time and immediately report their presence to security officials. The system's goal is to prevent potential security threats posed by unknown individuals. It uses the Local Binary Patterns Histogram (LBPH) Algorithm for facial recognition and maintains a database of authorized personnel. When an individual not in the database attempts to access a restricted area, the system generates an alert for security personnel. Face detection is a critical part of this system's operation.

4.3. Existing Applications

Several alarming software solutions are available, but many of them are designed for home-level security and are limited in scalability. Some of these applications include Frontpoint, Simplisafe, ADT, Vivint. SmartHome, Brinks, Google Nest Service, Ring Alarm Security System, and Adobe. While they offer features like fire and smoke detection, they often have limitations: They are not easily scalable to the institutional level.

They often come with paid services.

Professional installation may be the only option

4.4. Biometric and Identity Management Solutions

In the broader context of security and identity management, companies like MorphoTrak and Cross Match Technologies play a significant role. They provide biometric and identity management solutions to various markets, including law enforcement, border control, driver licenses, civil identification, and facility/IT security. These solutions encompass fingerprint identification systems, facial recognition systems, and iris recognition, among others. This highlights the importance of biometrics and advanced identity verification technologies in security systems.

5. Data Utilization

The data section introduces the Local Binary Patterns Histogram (LBPH) Algorithm as a robust technique in computer vision and facial recognition. It plays a pivotal role in capturing and analyzing intricate texture patterns within facial images. LBPH is a key component of biometric systems, allowing computers to recognize individuals based on the unique features present in their faces. The data used in this project consists of face images of individuals. These face images are organized

into a dataset where each person's images are stored in a separate directory. This dataset is used for training a face recognition model to recognize different individuals based on their facial features.

The Local Binary Patterns Histogram (LBPH) Algorithm is indeed a widely used technique in computer vision, particularly in the field of facial recognition. It is known for its ability to capture intricate texture patterns within facial images, making it a robust choice for biometric systems. Here's a detailed description of the components mentioned in your query:

LBPH Algorithm:

- Description: Local Binary Patterns (LBP) is a texture descriptor that focuses on the local patterns of pixel intensities in an image. LBPH extends LBP by considering the patterns in local regions and constructing histograms of these patterns.

- Characteristics: LBPH is robust to variations in lighting conditions, facial expressions, and poses. It breaks down the face image into small local regions and describes the texture pattern in each region independently, providing a more detailed representation.

Role in Computer Vision and Facial Recognition:

- LBPH plays a pivotal role in facial recognition by capturing and analyzing texture patterns within facial images. It is used to recognize individuals based on the unique features present in their faces.

Data Used in the Project:

- Description: The dataset used in this project comprises face images of individuals. These images are organized into a structured dataset where each person's images are stored in a separate directory.

- Sources: The source of the dataset could vary, and it may come from publicly available datasets for facial recognition (e.g., Labeled Faces in the Wild, CelebA, etc.) or proprietary datasets collected for a specific project.

- Size: The size of the dataset could vary depending on the number of individuals, the number of images per person, and the overall diversity of the dataset. It could range from a few hundred to several thousand images.

- Attributes: Each image in the dataset is likely to have attributes such as pixel values, facial landmarks, and possibly labels indicating the identity of the person.

- Characteristics: The dataset is specifically designed for training a face recognition model. It should cover a wide range of variations in facial expressions, poses, and lighting conditions to ensure that the trained model is robust.

Training a Face Recognition Model: - Purpose: The dataset is used to train a face recognition model that can identify different individuals based on their facial features.

- Process: The training process involves feeding the images into the LBPH algorithm, which extracts features from the facial textures. These features are then used to train a machine learning model (e.g., a classifier) that can predict the identity of a person based on their facial image.

- Evaluation: The trained model is likely evaluated on a separate set of images to assess its accuracy and generalization to new, unseen data.

6. Data Exploration

LBPH operates by thoroughly examining pixel-level patterns within a facial image. This process begins by segmenting the face image into smaller, manageable blocks. Each block undergoes a meticulous analysis to extract local texture information. For every pixel within a block, LBPH compares its intensity to that of its neighboring pixels.

The pixel's intensity is classified as follows:

If the pixel's intensity is greater than or equal to that of the central pixel, it's assigned a binary value of 1.

Conversely, if the pixel's intensity is lower than that of the central pixel, it's assigned a binary value of 0.

This binary labeling of pixels is performed for each pixel in each block, leading to the creation of multiple 8-bit binary patterns. These binary patterns are crucial as they represent unique facial textures within specific regions of the face.

The data preparation steps involve organizing the face images into directories, converting them to grayscale, and resizing them to a consistent size.

Organizing Data: The dataset is structured with subdirectories, where each subdirectory corresponds to a specific person. This organization makes it easier to label and process the images.

Image Preprocessing: Images are converted to grayscale using OpenCV's cv2.cvtColor() method.

Image Resizing: Images are resized to a consistent size (e.g., 130x100 pixels) using OpenCV's cv2.resize() method.

6.1. Methodologies

Local Binary Patterns Histogram (LBPH) Algorithm:

Segmentation:

The face image is divided into smaller blocks to facilitate a localized analysis of texture patterns.

Pixel Intensity Comparison:

For each pixel within a block, LBPH compares its intensity to that of its neighboring pixels.

If the pixel's intensity is greater than or equal to the central pixel, it is assigned a binary value of 1; otherwise, it is assigned a binary value of 0.

Binary Patterns Creation:

This binary labeling process is performed for each pixel in each block, resulting in the creation of multiple 8-bit binary patterns.

These binary patterns represent unique facial textures within specific regions of the face.

6.2. Reflections

The effectiveness of the LBPH algorithm and the data preparation steps can be evaluated through the following metrics:

Feature Extraction: The LBPH algorithm successfully extracts intricate texture patterns from facial images, creating informative binary patterns for localized regions.

Feature vectors are generated based on these patterns, capturing unique facial characteristics.

Model Training: A machine learning model (e.g., a classifier) is trained using the extracted features from the dataset.

The organized data, grayscale conversion, and resizing contribute to creating a robust training set.

Accuracy and Performance: The trained model is evaluated on a separate test set to measure its accuracy in recognizing individuals.

Metrics such as accuracy, precision, recall, and F1 score can be used to assess the performance of the facial recognition system.

Robustness: LBPH's robustness to variations in lighting, facial expressions, and poses is assessed by testing the model on images with different conditions.

Computational Efficiency: The efficiency of the image preprocessing steps (grayscale conversion and resizing) is considered, ensuring that the model training process is computationally efficient.

Real-world Applicability: The trained model can be further tested in real-world scenarios, assessing its performance on unseen data and its suitability for deployment in practical applications.

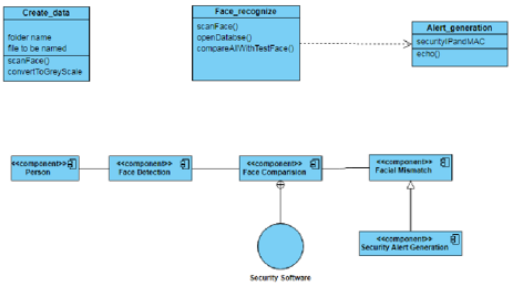


Figure 1: Class and Component Diagrams

7. Data Preprocesing

LBPH relies on four critical parameters, each carefully chosen to optimize its performance:

Radius: The radius parameter defines the extent of the circular local binary pattern around the central pixel. In most cases, a radius of 1 is chosen to ensure fine-grained texture analysis.

Neighbors: This parameter dictates the number of neighboring sample points considered when constructing the circular local binary pattern. A value of 8 is a common choice, although it can be adjusted depending on the application's computational requirements.

Grid X: Grid X determines the number of horizontal cells into which the facial image is divided. Increasing the number of cells results in a finer grid and a more detailed feature vector, usually set to 8.

Grid Y: Grid Y is similar to Grid X but controls the number of vertical cells. Like Grid X, it is often set to 8 for an effective feature representation.

These parameters play a pivotal role in defining how LBPH analyzes and extracts facial texture patterns from different facial regions, contributing to its success in facial recognition.

8. Methodology (Approach/ Procedure)

The LBPH Algorithm is characterized by a systematic process that captures and represents facial textures with remarkable accuracy. It employs the following steps:

Image Block Segmentation: The facial image is divided into smaller blocks to facilitate local texture analysis.

Binary Pattern Extraction: For each pixel within a block, LBPH compares its intensity to that of its neighboring pixels. This comparison results in an 8-bit binary pattern, which captures the unique texture characteristics of that pixel's surroundings.

Global Feature Extraction: These local binary patterns are concatenated to create a global description of the entire face. This holistic representation effectively encapsulates the facial texture.

For face recognition, the chi-squared distance metric is employed to compare histograms of binary patterns. This distance measure assesses the similarity between two histograms, providing a reliable basis for identifying individuals based on their facial features.

LBPH is renowned for its effectiveness in facial recognition due to its capability to capture distinctive texture patterns across various regions of the face. This robustness allows it to perform well even in scenarios with variations in facial expressions, lighting conditions, and pose.

Agile Software Development

Agile software development is an umbrella term for a set of frameworks and practices based on the values and principles expressed in the Manifesto for Agile Software Development and the 12 Principles behind it. Agile software development is more than frameworks such as Scrum, Extreme Programming or Feature-Driven Development (FDD).

When you approach software development in a particular manner, it's generally good to live by these values and principles and use them to help figure out the right things to do given your particular context.

Spiral Methodology

The spiral model is a systems development lifecycle (SDLC) method used for risk management that combines the iterative development process model with elements of the waterfall model.

The spiral model enables gradual releases and refinement of a product through each phase of the spiral as well as the ability to build prototypes at each phase. The most important feature of the model is its ability to manage unknown risks after the project has commenced; creating a prototype makes this feasible.

8.1. Algorithm

The LBPH Algorithm, each time it iterates, considers nine values present in the form of 3*3 matrix which contain the intensity of each pixel from a block after dividing the face into several blocks.

It is interested in the central value. The central pixel value i.e., Threshold is compared with all the neighboring pixel val-

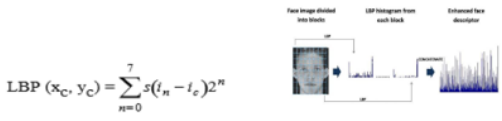


Figure 2: LBP Formula and Image Processing

ues. A new matrix is constructed by placing a 1 if the pixel value is greater than or equal to the central one and a 0 if not.

Then from the first position the 1's and 0's are concatenated to from an array of binary numbers which is converted to the decimal system.

The newly formed matrix will have previously obtained decimal number as its central value. This central value is the texture descriptor of the 3*3 matrix considered above.

A histogram is constructed using the texture descriptors extracted from the above step. These descriptors are then concatenated to form a global description of the face.

To compare histograms, chi-squared distance is employed.

9. Experiment

9.1. ML Experiment

Cascade Classifier Parameters: scaleFactor, minNeighbors, and minSize are used for face detection. These parameters balance sensitivity and specificity in face detection.

LBPH Face Recognizer: Parameters like radius, neighbors, and $grid_x$ and $grid_y$ are not explicitly defined.

Threshold for Face Recognition: Set as if prediction[1] ¡ 70. Determines when a face is considered a match.

Camera Settings: The default laptop camera is used with cv2.VideoCapture. The camera source can be adjusted based on the setup.

Pop-Up Messages: The messagebox module is used for pop-up messages. Displays messages like "Face matched, welcome person name" and "Intruder detected."

Miscellaneous Settings: Grayscale conversion and image resizing applied to camera frames. Aligns input with LBPH face recognizer requirements.

Control Flow: Continuous loop captures frames until 'Escape' key presses. Releases camera and closes OpenCV windows upon exit.

9.2. Training Dataset

Source: Real-world images or videos with diverse face variations.

Size: Sufficient data to cover various scenarios (lighting, poses, expressions).

Labeling: Identify individuals for face recognition training.

Preprocessing: Grayscale conversion and resizing to align with LBPH requirements.

Annotations: Include bounding boxes or labels for faces in each image.

9.3. Test Dataset

Source: Real-world images or videos, possibly distinct from training data.

Size: Represents scenarios not explicitly covered in training.

Labeling: Annotated faces for evaluating recognition accuracy.

Preprocessing: Grayscale conversion and resizing for consistency.

Annotations: Ground truth labels for evaluation purposes

10. Model Evaluation

In practical applications, the LBPH Algorithm serves as the foundation for facial recognition systems. To identify individuals accurately, multiple facial images of each person are captured from different angles, under various lighting conditions, and with varying expressions. During the verification or identification process, the subject stands in front of a camera, and the captured image is compared against the stored facial images in a database.

The advantages of employing LBPH-based facial recognition systems are substantial:

Non-Intrusiveness: Facial recognition can be conducted without any physical contact, making it non-intrusive and comfortable for individuals.

Distance Recognition: LBPH-based systems can identify individuals from a considerable distance, even without the person's knowledge.

Surveillance Applications: LBPH is particularly valuable in surveillance applications. It can be employed to search for wanted criminals, identify suspected terrorists, or locate missing persons.

Furthermore, LBPH can be integrated with other biometric techniques to bolster the security and authentication capabilities of a system. When deploying facial recognition systems in real-world scenarios, several factors must be considered, including subject motion, camera focus, and environmental conditions.

Model evaluation encompasses a comprehensive assessment of recognition accuracy and performance. Key metrics such as accuracy, precision, recall, F1-score, and others are employed to gauge the system's effectiveness in recognizing and verifying individuals based on their facial features.

10.1. Evaluation Techniques and Metrics for LBPH-Based Facial Recognition

In assessing LBPH-based facial recognition, key metrics include accuracy, precision, recall, and F1-score, derived from a confusion matrix. Specificity gauges the system's ability to identify negatives accurately. The Receiver Operating Characteristic (ROC) curve visualizes the trade-off between true positive and false positive rates, with the Area Under the Curve (AUC) summarizing its performance. Beyond metrics, evaluating LBPH involves considering subject motion, camera focus, and environmental conditions, ensuring the system's robustness in real-world scenarios. Continuous monitoring and periodic reevaluation are vital for maintaining effectiveness and reliability in dynamic environments.

11. Output

Figure 3: Image Registration

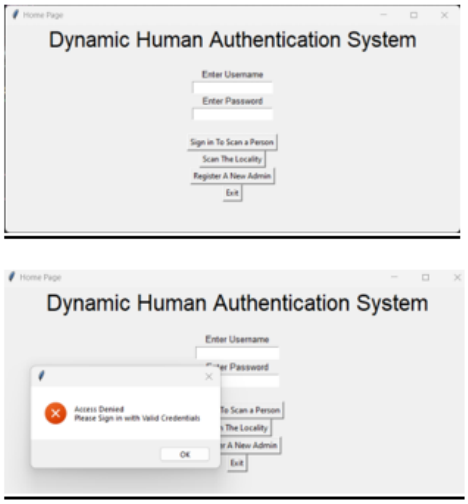


Figure 4: Signup and Login

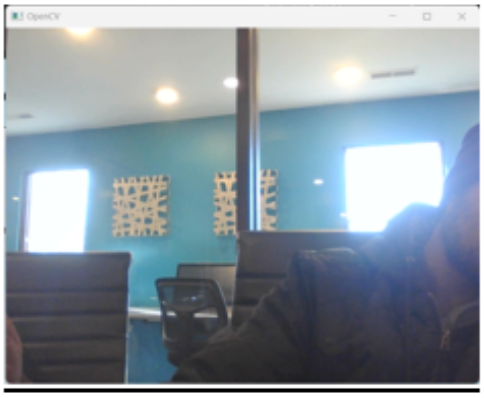
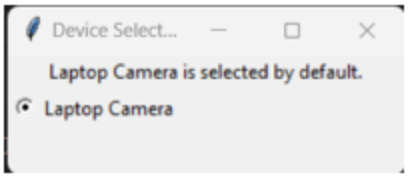


Figure 5: Data Creation



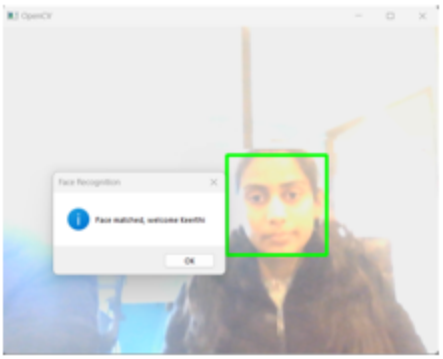


Figure 6: Image Recognition

12. Conclusions

The objective behind developing this software is to automate the responsibility of the security department which monitors the physical intrusion. Sometimes the security person might become corrupt and release sensitive information. There comes the need for automation because software is a blind slave to the programmer. It promptly does the task specified and reports the results. Also, it reduces the burden on human beings. This prototype does the same with ease. The automated check system is highly essential because havoc can't be anticipated and if it occurs, difficult to experience. Already, the biometric system of tracking and authorization drastically changed the scenario of monitoring and is highly prevalent. The Dynamic Human Authentication is equally important and effective. In the future, a better enhancement is ready to take place in this direction as

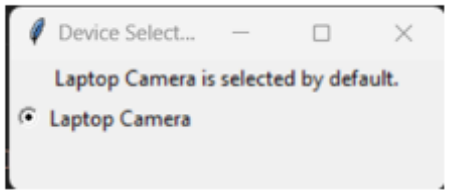


Figure 7: Image scanning the locality

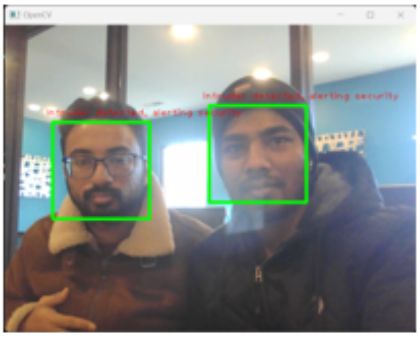


Figure 8: Image scanning the locality

the research is going on to tighten the security system at the basic level. With an accuracy of above 90 percent, this system is ready to compete and connect.

12.1. Limitations

The software's reliance on automated detection may face challenges in complex scenarios or unusual situations. False positives/negatives may occur, impacting reliability. Additionally, the system's effectiveness is contingent on accurate programming, and potential biases might be introduced. Integration with existing security measures and adaptability to diverse environments could pose challenges.

12.2. Further Work

Future enhancements may focus on refining the detection algorithm to minimize false alarms. Incorporating advanced AI techniques for nuanced threat analysis and integrating with external systems could enhance overall security. Continuous monitoring and updates are vital, and user-friendly features, such as SMS prompts for owners during intrusions, can augment the system's usability and responsiveness.

13. References

https://www.sih.gov.in/sih2020PS/QWxs/U29mdHdhcmU=/RHRlIG9mIElUICYgQ3liZXIgU2VjdXJpdHksIERSRE8=/QWxs
https://towardsdatascience.com/face-detection-in-2-minutes-using-opencv-python-90f89d7c0f81
https://realpython.com/face-detection-in-python-using-a-webcam/
https://towardsdatascience.com/a-guide-to-face-detection-in-python-3eab0f6b9fc1
https://adeshpande3.github.io/A-Beginner
https://www.analyticsvidhya.com/blog/2018/12/guide-convolutional-neural-network-cnn/
https://en.wikipedia.org/wiki/$Digital_image_processing$
http://www.ncsa.illinois.edu/People/kindr/phd/PART1.PDF