IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Face and Liveness Detection Based Smart Bank Locker

Seema Francis Bansode[1] and Dr. R. G. Dabhade[2]
Student, Department of VLSI & Embedded System (E&TC)[1]
Professor, Department of VLSI & Embedded System (E&TC)[2]
Matoshri College of Engineering and Research Centre, Eklhare, Nashik, Maharashtra, India

Abstract: *With the increasing theft in banks, the security has become an important aspect in banking region. Most of the Bank lockers are currently protected by key locking, some password-based locks or using some digital locks which is insecure and unreliable. So, in this paper we are implementing bank locker using face recognition system. Face recognition is an effective and successful security technique whose accuracy can be improved by combining other technologies. For facial recognition, this project uses the CNN algorithm.*

In this project, only authenticated user can access the lockers as faces are stored for the individual identity of a person. Facial recognition alone cannot determine whether the person is real or not. Therefore, liveness detection is implemented. In liveness detection, the system detects if it interacts with a real person or a spoof artefact used by other person such as a face photo. To detect whether the person is live or not the project uses eye blink detection. The project identifies whether the user is authentic or not. If not then, the locker will not open instead it will raise an alert and it will send a text SMS to the admin that somebody is trying to open their locker and immediately the system will capture photograph of that person and that photograph will be emailed to the user. In this way, the system provides high security, theft protection and alert of bank locker.

Keywords: Facial recognition

I. INTRODUCTION

Human face detection is the most promising field of image processing that has a vast area of research oriented real-life applications. In the real world the concept is widely used for the content annotation, access control, profiling and potential discrimination in the web world. There is always constructive scope of new inventions in the field of technology which is as vast as galaxy on its own. This leads to the better future. There has been a supportive development in the field of technology by the humans since the beginning of mankind. The motive was in rapid development and also in the advancement of technology to ensure the minimization of risk that is prone along with the new inventions which would make life easier, better and much faster. The main intention of face detection is to find out the human face in the given input. The Psychological process of locating the human face in the visual frame is also possible. It is also categorized as a special case of object class detection. The Eigen face approach is considered as a promising technique of face detection. In the field of marketing the facial image detection is playing a role of huge interest for the users. It has always been an issue of personal authentication that needs to be fixed for the purpose of access control of the info-security in the wider context via physical security. Researchers found that the face detection is an issue that needs to be taken into consideration. In terms of appearance, human face has high degree of variability, making it a dynamic object of study. Application of face detection is found in crowd surveillance, video conferencing, biometrics etc. The concept of human face detection makes it difficult for computer vision. Detected face is stored with high level of secrecy and certainty. Assuring that the data is safe, is the most important aspect under discussion. The image data consists of properties associated with, such as high level of redundancy, bulk capabilities and also high correlation between the pixels. In today's world of connectivity and smart devices there is an urgent need to modify our existing day to day objects and make them smart, also it is not the era when we can blindly trust the old and conventional security measures, specifically speaking is our door locks. To change and modernize any object we need

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

to eliminate its existing drawbacks and add extra functionality. The major drawbacks in a common door lock are that anyone can open a conventional door lock by duplicating or stealing the key and its simply impossible if we want our friends and family to enter our house, without being actually present over there. Thus, why not just eliminate these problems. So, to simply convert this normal door lock into a smart lock, which can open the door whenever we turn up in front of the gate or when we want it to open up for someone else without being physically present, we need to modify the door. So, an era has come where devices can interact with its users and at the same time ensure of their safety and keep improvising themselves. Users could operate on a touchscreen to select entering the house by recognizing the face or motors and/or adding a digital number pad to take inputs from the user or adding Infra-Red or Bluetooth modules to operate these devices. For face recognition, an image will be captured by a pi camera and pre-processed by Raspberry pi like converting, re-sizing and cropping. Then face detection and recognition are performed. Once the face is recognized by the classifier based on a prestored image library, the image will be sent to a remote console waiting for house owner's decision. For the passcode part, users could enter or reset passcode through a keypad. Since 2010 the industry has seen a dawn of work being done in fields of Artificial Intelligence, Machine Learning, Neural Networks, IoT, Big Data Analytic all with a common goal to make things easier, self-supervising and to interconnect all kinds of devices by making everyday objects interconnected and interoperable. A need has been felt in the field of digitalizing conventional security tools and thus a lot of work has been modelled on making daily life locks smart by introducing locks movable with the help of stepper. An intensive study of literates implementing Smart Locks had been done and literature implementing Door Locks with the help of GSM phones and stepper motors have been studied. Also, literature regarding smart display have been thoroughly reviewed. The fault in existing models is a complexity of a system and unnecessarily relying on extra components. Our model is unique with its one-of-a-kind combination of functionalities offered and the simplicity of the model. A major difference is in the overhead reduction by the application as it detects the face out of the image and sends it directly to application program interfaced with our application, which has not been provided in any existing model and the efficient use of solenoids, which also eliminates the use of stepper motors. So, we have avoided the use of unnecessary components like stepper motors and drivers as done in existing models and also, we have given newer and unprecedented features of facial recognition as an access point control system with a combination of relay module with a solenoid to open the gate and unique and interactive User Interface. Also, rather than using a low-quality Raspberry Pi Interfaced Camera we have used USB attachable HD Webcam to do efficient and reliable facial recognition. The objectives of the proposed work are to implement a working model of a smart door and to give solutions to the problem faced by people in day-to-day incidents of burglary or losing the key and also to promote and ignite the work being done on IOT systems and implementing it with the help of key research areas of Neural Networks and IoT APIs and protocols. This model is allowing people to add more functionality to it and thus induce more research work in the field of AI, Machine Learning, IoT and lot more. Liveliness detection has been a very active research topic in fingerprint recognition and iris recognition communities in recent years. But in face recognition, approaches are very much limited to deal with this problem. Liveliness is the act of differentiating the feature space into live and non-living. Imposters will try to introduce a large number of spoofed biometrics into system. With the help of liveliness detection, the performance of a biometric system will improve. It is an important and challenging issue which determines the trustworthiness of biometric system security against spoofing.

1.1 LITERATURE REVIEW

J. Maatta, A. Hadid, M. Pietikainen have suggested 'Face spoofing detection from single image using microtexture analysis'. The proposed method uses multi-scale local binary patterns to look at the texture of facial images. This approach is strong, computationally fast and doesn't require user-cooperation. Additionally, the texture features that are used for spoofing detection can even be used for face recognition. Viewpoints, occlusions, aging of subjects and complicated outdoor lighting are challenges in face recognition.

A. K. Singh, P. Joshi and G. C. Nandi have proposed 'Face recognition with liveness detection using eye and mouth movement'. The liveness module utilizes face macro features, especially eye and mouth movements so as to get random challenges and observing the user's response on this. Except for the eye and mouth imposter attacks, experimental results suggest that the system can detect liveness when subjected to all or any of these attacks. Eye and mouth imposter

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

attacks can bypass the liveness test but it creates massive changes in face structure. As a result, the biometric identification module may fail to recognise or incorrectly classifies the results.

G. Pan, L. Sun, Z. Wu, and S. Lao - 'Eyeblink-based anti-spoofing in face recognition from a generic web-camera'. They propose a real-time liveness detection approach against photograph spoofing in face recognition, by recognizing spontaneous eye blinks, which could be a non-intrusive manner. A generic camera collects 15 frames per second and outputs two frames of faces that can be used as a spoofing clue. Two captured frames in multiple frames to test liveness, so user should be highly co-operative.

Junyan Peng, Patrick P. K. Chan has proposed 'Face liveness detection for combating the spoofing attack in face recognition'. To tackle the spoofing attack, a face liveness detection approach using the High Frequency Descriptor was proposed. The extra illumination is added, which may raise the energy of high frequency components of a true face by exposing more details of the hair and skin, and lower it by causing a glisten on the planar surface. The difference of the energy of high frequency components between images with and without the illumination is calculated. Experimental results show that this method has robustness only if the resolution of the attack media is high.

Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti presented the paper 'Biometric liveness detection: Challenges and Research Opportunities'. Spoofs like people's facial photos, masks, and videos, which are easily available on social media, can easily target biometric systems. In challenge– response liveness detection, users must, as an example, repeat a phrase or blink their eyes to make sure that random instructions are performed properly.

D. Garud and S. S. Agrawal presented a way for Face Liveness Detection. Within the proposed work, method is discussed to detect the spoofing attack. Spoofing methods like photo, mask or video image is easily recognized by this method. This method depends on illumination and a few other characteristics of face which are helpful to detect spoofed face. Proposed work detects the live face using illumination characteristics in MATLAB tool fed to the SVM classifier.

1.2 PROBLEM STATEMENT

A face recognition based system can used for bank locker security but it can be easily hacked if somebody uses photograph of a person. As a solution, in addition to face recognition, a liveness detecting system is required.

1.3 OBJECTIVE

1) To study existing bank locker method.
2) To design the system architecture for proposed system.
3) To implement the proposed system using machine learning.
4) To analyze and evaluate the design module

1.4 MOTIVATION

Automatic face recognition has been a challenging task for the research community. It has been extensively adopted by the applications including biometrics, surveillance, security, identification, and authentication. Face recognition usually exploit high-dimensional information which makes it computationally intensive. The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology In general, face recognition algorithms are not able to differentiate live face from not live face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph. In order to guard against such spoofing, a secure system needs liveliness detection

II. SYSTEM DEVELOPMENT

2.1 DESIGN METHODOLOGY

2.1.1 INTRODUCTION

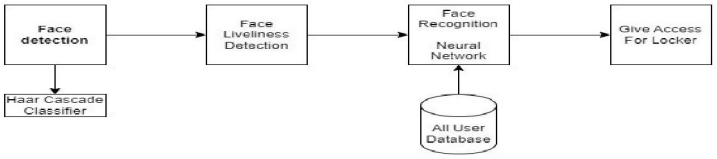
The system works in real time through a webcam as follows:

1. Detect faces in each frame generated by the webcam.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

2. For each detected face, detect eyes.
3. Detect liveness of the face i.e. eyes are blinking or not.
4. Recognize face and access the respective locker of the user.

The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. The face recognition can be used for bank locker security but it can be easily hacked if somebody uses photograph of person, so there is need for liveliness detection along with face Recognition The proposed framework that combines Face Net with liveness detection is shown in Figure1 In above block diagram we are going to detect face using haar cascade classifier which algorithm for detection of face. After detection of face, system will decide the face is real or fake by using liveness detection technique. Liveness detection technique is the act of differentiating the feature space into live and non-living In this system we need a way to detect faces and eyes in real-time. So we are using -cascade classifier to performs these tasks. In this haar cascade classifier Cascade is a machine learning object detection algorithm used to identify objects in an image or video. For face detection module, a three-layer feed forward artificial neural network with Tanh activation function is proposed that combines AdaBoost to detect human faces so that face detecting rate is rather high. For face alignment module, a multilayer perceptron (MLP) with linear function (three-layer) is proposed, and it creates 2D local texture model for the active shape model (ASM) local searching



2.1.2 PROPOSED SYSTEM

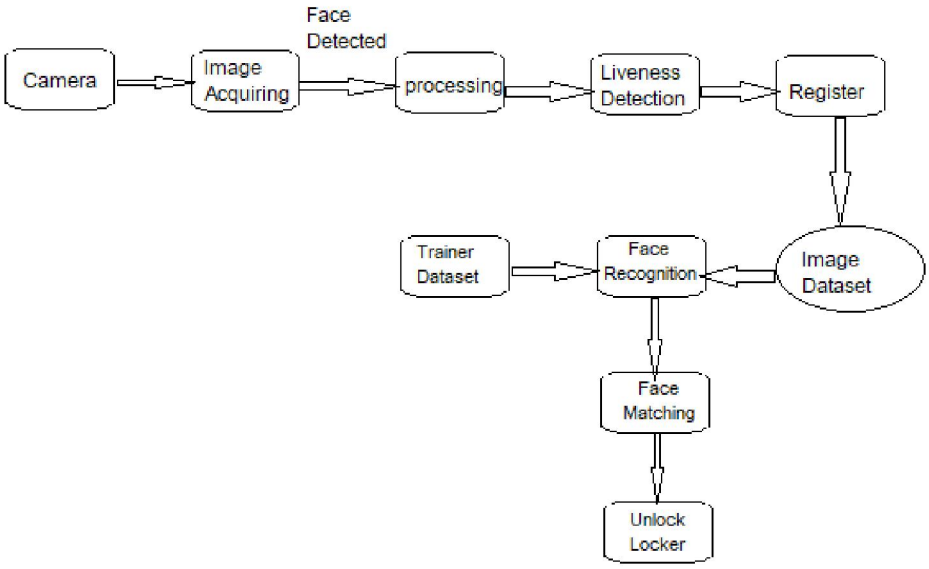


Fig. Architecture Diagram

In this diagram we are going to implement eye-blink detection & face recognition Based on LBPH algorithm and neural network. The algorithm works in real time through a webcam and displays the person's name. The program runs as follows:

[1] Detect faces in each frame generated by the webcam.
[2] For each detected face, detect eyes.
[3] Detect liveness of the face i.e. eyes are blinking or not
[4] Recognize face and access the respected locker of the user

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

III. SYSTEM HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Requirements:

- Processor – I3 / I5
- Speed – 2.6 GHz
- RAM – 4 GB(min)
- Hard Disk - 128 GB SSD
- Monitor – SVG

Software Requirements:

- Operating System - Windows / Linux
- Front End – python Django
- Database - My SQL 5.0

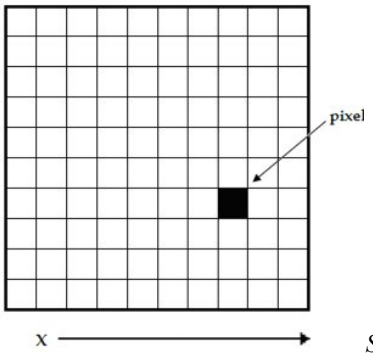
3.1 Image processing in Python

As the name says, image processing means processing the image and this may include many different techniques until we reach our goal.

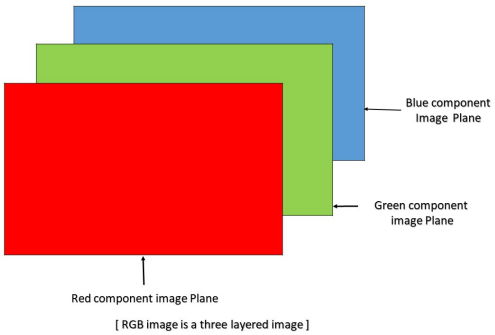
The final output can be either in the form of an image or a corresponding feature of that image. This can be used for further analysis and decision making.

But what is an image?

An image can be represented as a 2D function F(x,y) where x and y are spatial coordinates. The amplitude of F at a particular value of x,y is known as the intensity of an image at that point. If x,y, and the amplitude value is finite then we call it a digital image. It is an array of pixels arranged in columns and rows. Pixels are the elements of an image that contain information about intensity and color. An image can also be represented in 3D where x,y, and z become spatial coordinates. Pixels are arranged in the form of a matrix. This is known as an **RGB image**.



Source



There are various types of images:

RGB image: It contains three layers of 2D image, these layers are Red, Green, and Blue channels.

Grayscale image: These images contain shades of black and white and contain only a single channel.

Classic image processing algorithms

1. Morphological Image Processing

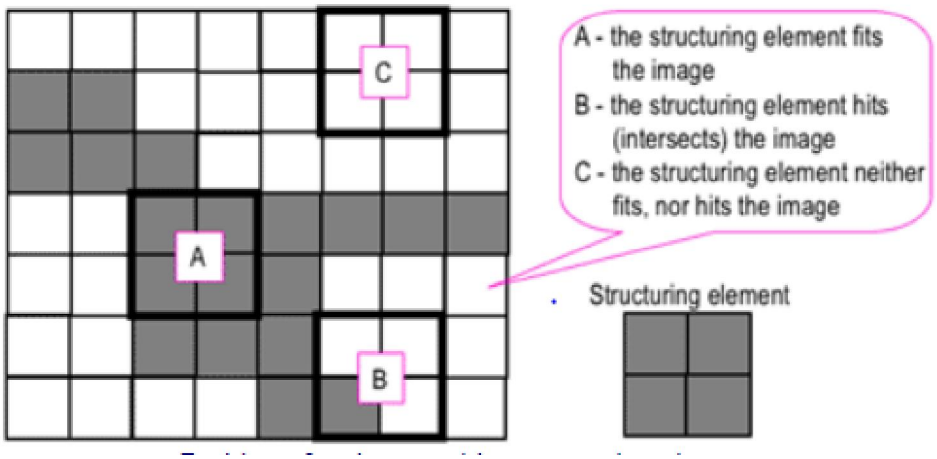
Morphological image processing tries to remove the imperfections from the binary images because binary regions produced by simple thresholding can be distorted by noise. It also helps in smoothing the image using opening and closing operations.

Morphological operations can be extended to grayscale images. It consists of non-linear operations related to the structure of features of an image. It depends on the related ordering of pixels but on their numerical values. This technique analyzes an image using a small template known as **structuring element** which is placed on different possible locations in the image and is compared with the corresponding neighbourhood pixels. A structuring element is a small matrix with 0 and 1 values.

Let's see the two fundamental operations of morphological image processing, **Dilation and Erosion:**

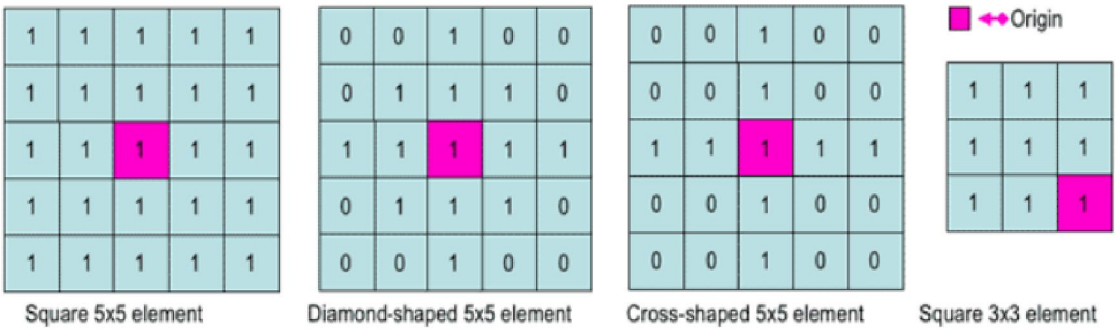
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

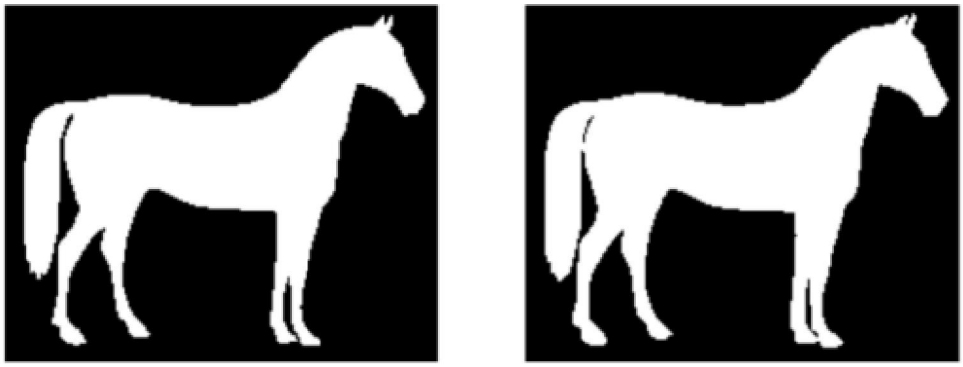
dilation operation adds pixels to the boundaries of the object in an image
erosion operation removes the pixels from the object boundaries.
The number of pixels removed or added to the original image depends on the size of the structuring element.
At this point you may be thinking "what is a structuring element?" Let me explain:
Structuring element is a matrix consisting of only 0's and 1's that can have any arbitrary shape and size. It is positioned at all possible locations in the image and it is compared with the corresponding neighbourhood of pixels.



Source

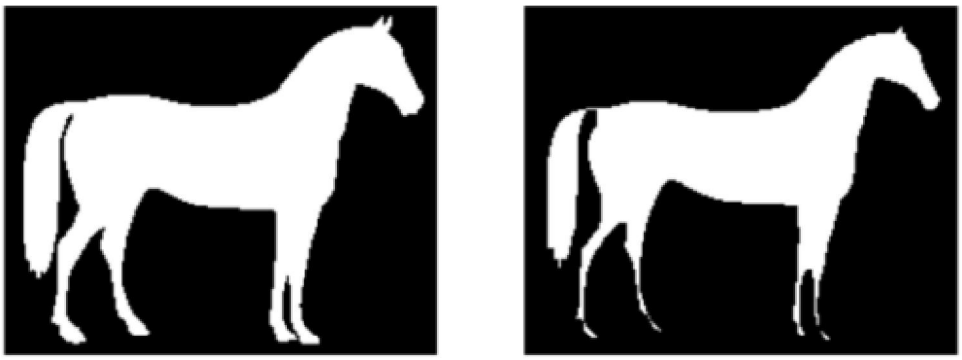
The square structuring element 'A' fits in the object we want to select, the 'B' intersects the object and 'C' is out of the object.
The zero-one pattern defines the configuration of the structuring element. It's according to the shape of the object we want to select. The center of the structuring element identifies the pixel being processed.





Dilation | Source

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024



Erosion | Source

2. **Gaussian Image Processing**

Gaussian blur which is also known as gaussian smoothing, is the result of blurring an **image** by a **Gaussian** function.

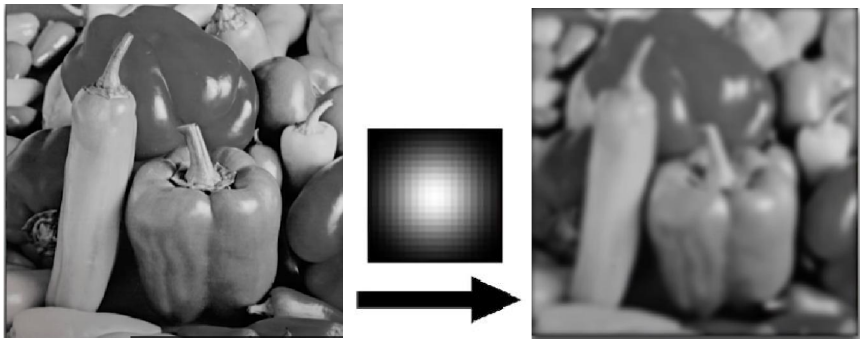
It is **used to reduce image noise and reduce details**. The visual effect of this blurring technique is similar to looking at an image through the translucent screen. It is sometimes used in computer vision for image enhancement at different scales or as a data augmentation technique in deep learning.

The basic gaussian function looks like:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

In practice, it is best to take advantage of the Gaussian blur's separable property by dividing the process into two passes. In the first pass, a one-dimensional kernel is used to blur the image in only the horizontal or vertical direction. In the second pass, the same one-dimensional kernel is used to blur in the remaining direction. The resulting effect is the same as convolving with a two-dimensional kernel in a single pass. Let's see an example to understand what gaussian filters do to an image.

If we have a filter which is normally distributed, and when its applied to an image, the results look like this:



Original Filter Result

You can see that some of the edges have little less detail. The filter is giving more weight to the pixels at the center than the pixels away from the center. Gaussian filters are low-pass filters i.e. weakens the high frequencies. It is commonly used in edge detection.

3. Fourier Transform in image processing

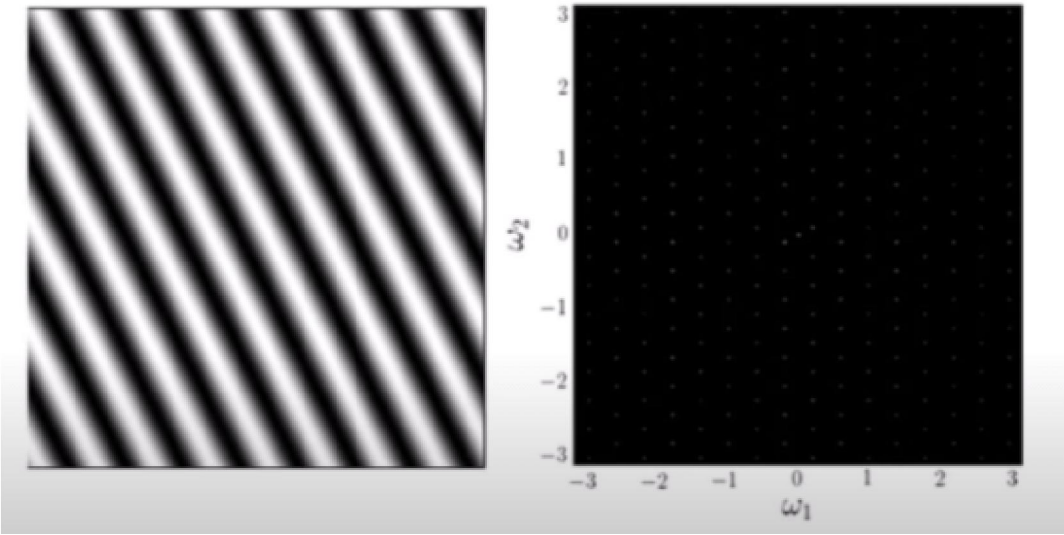
Fourier transform breaks down an image into sine and cosine components.

It has multiple applications like image reconstruction, image compression, or image filtering.

Since we are talking about images, we will take discrete fourier transform into consideration.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Let's consider a sinusoid, it comprises of three things:
Magnitude – related to contrast
Spatial frequency – related to brightness
Phase – related to color information
The image in the frequency domain looks like this:



Source

The formula for 2D discrete fourier transform is:

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y)\, e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

In the above formula, f(x,y) denotes the image.
The inverse fourier transform converts the transform back to image. The formula for 2D inverse discrete fourier transform is:

$$f(x, y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v)\, e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}$$

4. Edge Detection in image processing

Edge detection is an image processing technique for finding the boundaries of objects within images. It works by detecting discontinuities in brightness.
This could be very beneficial in extracting useful information from the image because most of the shape information is enclosed in the edges. Classic edge detection methods work by detecting discontinuities in the brightness.
It can rapidly react if some noise is detected in the image while detecting the variations of grey levels. Edges are defined as the local maxima of the gradient.
The most common edge detection algorithm is **sobel edge detection algorithm**. Sobel detection operator is made up of 3*3 convolutional kernels. A simple kernel Gx and a 90 degree rotated kernel Gy. Separate measurements are made by applying both the kernel separately to the image.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

$$Gx = \begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} * Image\ matrix$$

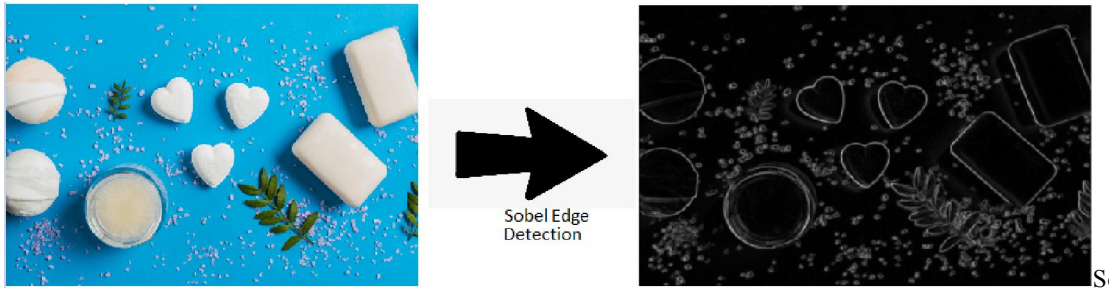
And,

$$Gy = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * Image\ matrix$$

* denotes the 2D signal processing convolution operation.

Resulting gradient can be calculated as:

$$G = sqrt(Gx^2 + Gy^2)$$



Source

5. Wavelet Image Processing

We saw a Fourier transform but it is only limited to the frequency. Wavelets take both time and frequency into the consideration. This transform is apt for non-stationary signals.

We know that edges are one of the important parts of the image, while applying the traditional filters it's been noticed that noise gets removed but image gets blurry. The wavelet transform is designed in such a way that we get good frequency resolution for low frequency components. Below is the 2D wavelet transform example:

Source

Image processing using Neural Networks

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

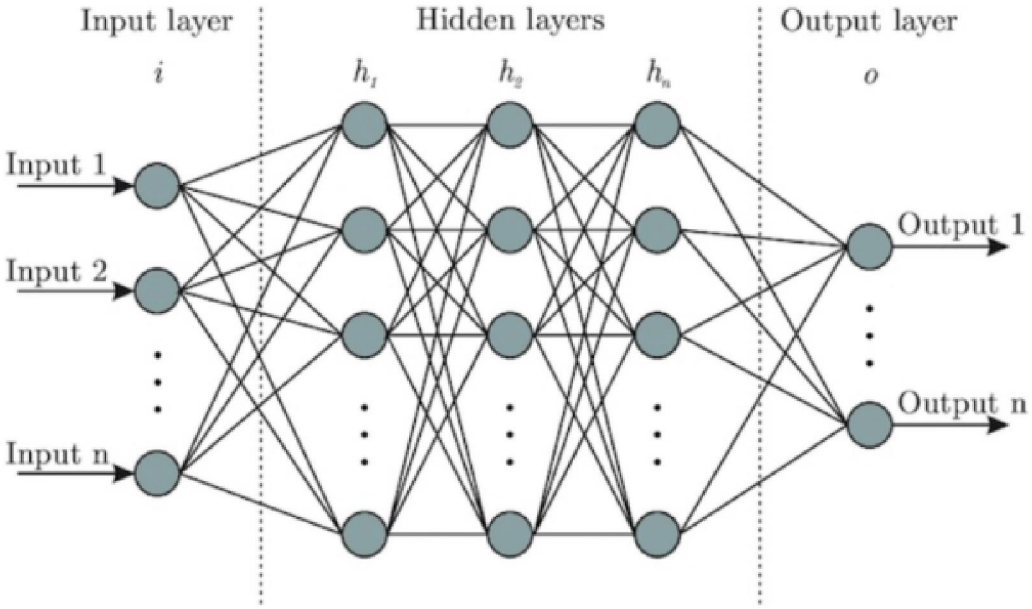
Neural Networks are multi-layered networks consisting of neurons or nodes. These neurons are the core processing units of the neural network. They are designed to act like human brains. They take in data, train themselves to recognize the patterns in the data and then predict the output.

A basic neural network has three layers:

Input layer

Hidden layer

Output layer



Basic neural network | Source

The input layers receive the input, the output layer predicts the output and the hidden layers do most of the calculations. The number of hidden layers can be modified according to the requirements. There should be atleast one hidden layer in a neural network.

The basic working of the neural network is as follows:

Let's consider an image, each pixel is fed as input to each neuron of the first layer, neurons of one layer are connected to neurons of the next layer through channels.

Each of these channels is assigned a numerical value known as weight.

The inputs are multiplied by the corresponding weights and this weighted sum is then fed as input to the hidden layers.

The output from the hidden layers is passed through an activation function which will determine whether the particular neuron will be activated or not.

The activated neurons transmits data to the next hidden layers. In this manner, data is propagated through the network, this is known as Forward Propagation.

In the output layer, the neuron with the highest value predicts the output. These outputs are the probability values.

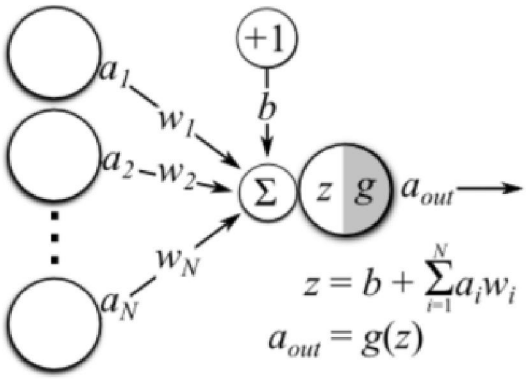
The predicted output is compared with the actual output to obtain the error. This information is then transferred back through the network, the process is known as Backpropagation.

Based on this information, the weights are adjusted. This cycle of forward and backward propagation is done several times on multiple inputs until the network predicts the output correctly in most of the cases.

This ends the training process of the neural network. The time taken to train the neural network may get high in some cases.

In the below image, **ai's** is the set of inputs, **wi's** are the weights, **z** is the output and **g** is any activation function.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024



Operations in a single neuron |

Here are some guidelines to prepare data for image processing.

More data needs to be fed to the model to get the better results.

Image dataset should be of high quality to get more clear information, but to process them you may require deeper neural networks.

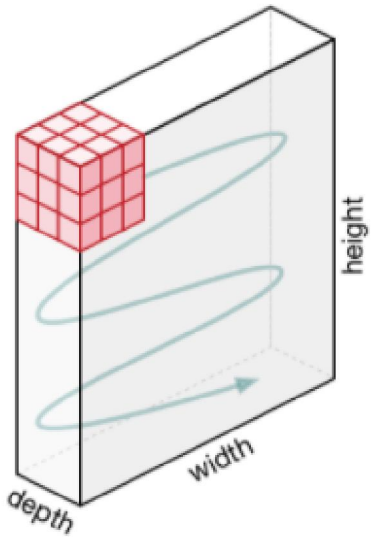
In many cases RGB images are converted to grayscale before feeding them into a neural network.

Types of Neural Network

Convolutional Neural Network

A convolutional neural network, ConvNets in short has three layers:

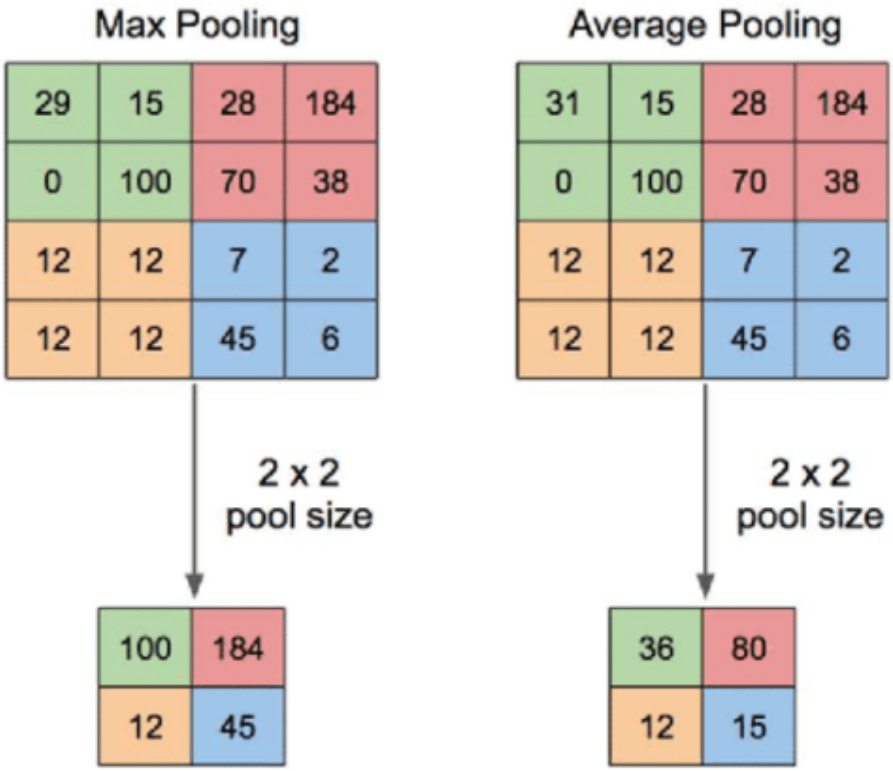
Convolutional Layer (*CONV*): They are the core building block of CNN, it is responsible for performing convolution operation.The element involved in carrying out the convolution operation in this layer is called the **Kernel/Filter (matrix).** The kernel makes horizontal and vertical shifts based on the **stride rate** until the full image is traversed.



Movement of the kernel |

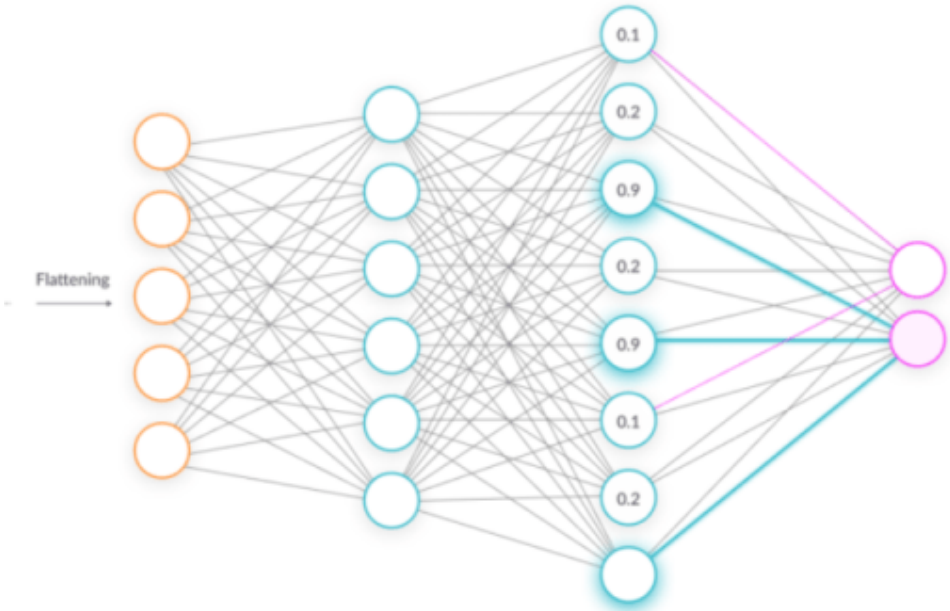
Pooling Layer (*POOL*): This layer is responsible for dimensionality reduction. It helps to decrease the computational power required to process the data. There are two types of Pooling: Max Pooling and Average Pooling. Max pooling returns the maximum value from the area covered by the kernel on the image. Average pooling returns the average of all the values in the part of the image covered by the kernel.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024



Pooling operation |

Fully Connected Layer (*FC*): The **fully connected layer** (**FC**) operates on a flattened input where each input is connected to all neurons. If present, **FC layers** are usually found towards the end of **CNN** architectures.

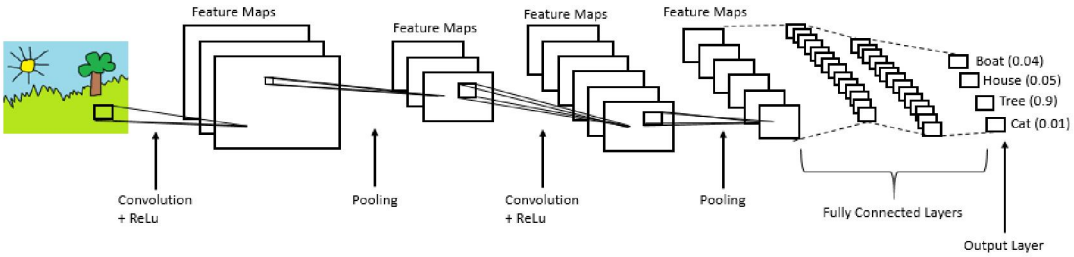


Fully connected layers |

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

CNN is mainly used in extracting features from the image with help of its layers. CNNs are widely used in image classification where each input image is passed through the series of layers to get a probabilistic value between 0 and 1.



Generative Adversarial Networks

Generative models use an unsupervised learning approach (there are images but there are no labels provided).

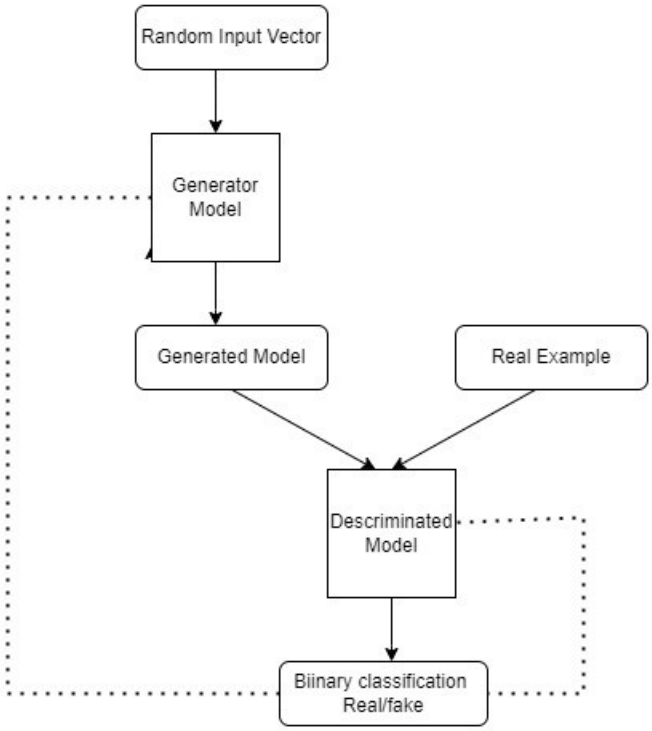
GANs are composed of two models **Generator** and **Discriminator.** *Generator* learns to make fake images that look realistic so as to fool the discriminator and *Discriminator* learns to distinguish fake from real images (it tries not to get fooled).

Generator is not allowed to see the real images, so it may produce poor results in the starting phase while the discriminator is allowed to look at real images but they are jumbled with the fake ones produced by the generator which it has to classify as real or fake.

Some noise is fed as input to the generator so that it's able to produce different examples every single time and not the same type image. Based on the scores predicted by the discriminator, the generator tries to improve its results, after a certain point of time, the generator will be able to produce images that will be harder to distinguish, at that point of time, the user gets satisfied with its results. Discriminator also improves itself as it gets more and more realistic images at each round from the generator.

Popular types of GANs are Deep Convolutional GANs(DCGANs), Conditional GANs(cGANs), StyleGANs, CycleGAN, DiscoGAN, GauGAN and so on.

GANs are great for image generation and manipulation. Some applications of GANs include : Face Aging, Photo Blending, Super Resolution, Photo Inpainting, Clothing Translation.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Image processing tools

1. OpenCV

It stands for Open Source Computer Vision Library. This library consists of around 2000+ optimised algorithms that are useful for computer vision and machine learning. There are several ways you can use opencv in image processing, a few are listed below:

Converting images from one color space to another i.e. like between BGR and HSV, BGR and gray etc.

Performing thresholding on images, like, simple thresholding, adaptive thresholding etc.

Smoothing of images, like, applying custom filters to images and blurring of images.

Performing morphological operations on images.

Building image pyramids.

Extracting foreground from images using GrabCut algorithm.

Image segmentation using watershed algorithm.

2. Scikit-image

It is an open-source library used for image preprocessing. It makes use of machine learning with built-in functions and can perform complex operations on images with just a few functions.

It works with numpy arrays and is a fairly simple library even for those who are new to python. Some operations that can be done using scikit image are :

To implement thresholding operations use **try_all_threshold()** method on the image. It will use seven global thresholding algorithms. This is in the **filters** module.

To implement edge detection use **sobel()** method in the **filters** module. This method requires a 2D grayscale image as an input, so we need to convert the image to grayscale.

To implement gaussian smoothing use **gaussian()** method in the **filters** module.

To apply histogram equalization, use **exposure** module, to apply normal histogram equalization to the original image, use **equalize_hist()** method and to apply adaptive equalization, use **equalize_adapthist()** method.

To rotate the image use **rotate()** function under the **transform** module.

To rescale the image use **rescale()** function from the **transform** module.

To apply morphological operations use **binary_erosion()** and **binary_dilation()** function under the **morphology** module.

3. PIL/pillow

PIL stands for Python Image Library and **Pillow** is the friendly PIL fork by Alex Clark and Contributors. It's one of the powerful libraries. It supports a wide range of image formats like PPM, JPEG, TIFF, GIF, PNG, and BMP.

It can help you perform several operations on images like rotating, resizing, cropping, grayscaling etc. Let's go through some of those operations

To carry out manipulation operations there is a module in this library called **Image.**

To load an image use the **open()** method.

To display an image use **show()** method.

To know the file format use **format** attribute

To know the size of the image use **size** attribute

To know about the pixel format use **mode** attribute.

To save the image file after desired processing, use **save()** method. Pillow saves the image file in *png* format.

To resize the image use **resize()** method that takes two arguments as width and height.

To crop the image, use **crop()** method that takes one argument as a box tuple that defines position and size of the cropped region.

To rotate the image use **rotate()** method that takes one argument as an integer or float number representing the degree of rotation.

To flip the image use **transform()** method that take one argument among the following: Image.FLIP_LEFT_RIGHT, Image.FLIP_TOP_BOTTOM, Image.ROTATE_90, Image.ROTATE_180, Image.ROTATE_270.

Read also

Essential Pil (Pillow) Image Tutorial (for Machine Learning People)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

4. NumPy

With this library you can also perform simple image techniques, such as flipping images, extracting features, and analyzing them.

Images can be represented by numpy multi-dimensional arrays and so their type is **NdArrays**. A color image is a numpy array with 3 dimensions. By slicing the multi-dimensional array the RGB channels can be separated.

Below are some of the operations that can be performed using NumPy on the image (image is loaded in a variable named **test_img** using imread).

To flip the image in a vertical direction, use **np.flipud(test_img).**

To flip the image in a horizontal direction, use **np.fliplr(test_img).**

To reverse the image, use **test_img[::-1]** (the image after storing it as the numpy array is named as <img_name>).

To add filter to the image you can do this:

Example: **np.where(test_img > 150, 255, 0)**, this says that in this picture if you find anything with 150, then replace it with 255, else 0.

You can also display the RGB channels separately. It can be done using this code snippet:

To obtain a red channel, do **test_img[:,:,0]**, to obtain a green channel, do **test_img[:,:,1]** and to obtain a blue channel, do **test_img[:,:,2].**

IV. WORKING

SYSTEM ANALYSIS

A. Existing system : The existing system protects vaults through simple lock and keys. Each locker consists of two keys, one key is the master key which is with the bank manager the other one is with the customer. And the vault room key will be with the bank manager and a spare key will be left with the cashier. Every time a customer has to manually sign a record before entering the vault room for accessing his vault. Certain but limited private banks have evolved to use code combinations or fingerprint.

B. Proposed System

In this proposed system it is attention on the human face for recognizing expression. Many techniques are available to recognize the face image. This technique can be adapted to real time system very easily. The system briefly displays the schemes of capturing the image from web cam, detecting the face, processing the image to recognize few results.

C. Advantages of Proposed System

• System used for locker security.
• Security against vulnerabilities such as spoofing, tampering, masquerade attack etc.
• There is no retention of the template or image.
• Improved authentication, security assurance. Maintaining Privacy and secrecy. • It can be implemented in large scale application and public domain with required authorization.

4.1 Algorithm Details:

An input layer, an output layer, and numerous hidden layers make up the used CNN's architecture. The hidden layers typically consist of convolutional layers, pooling layers, fully connected layers, and normalization layers (ReLU).The flow of CNN to process an input image and classify the faces based on face encodings is shown below.

Given an image, the face recognition module returns the 128-dimension face encoding for each face in the image which is compared with the known face encodings. Finally, we have an output, which is whether the input face matches the face in the dataset.

HAAR feature-based cascade classifiers based on the "Rapid Object Detection using a Boosted Cascade of Simple Features" is a machine learning approach in which a cascade function is trained using a large number of positive and negative images. It is then used to detect objects in other images. Here, this method is used for face detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

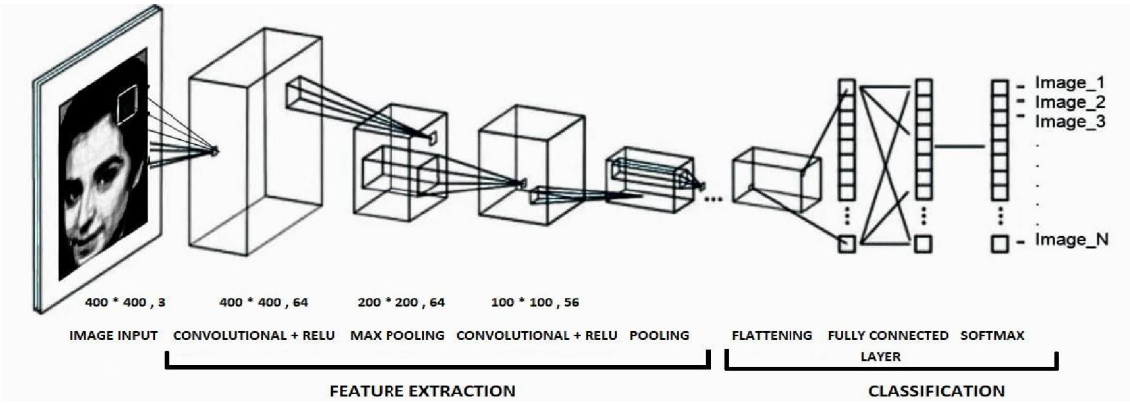


Figure 2: Architecture of Convolutional Neural Network (CNN) model

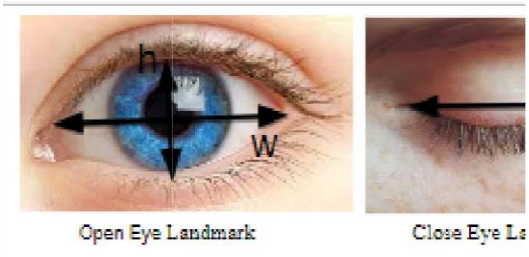


Figure 3: Liveness Detection

The eye blink detection technique is used to identify liveness. Eye blink detection algorithm uses eye aspect ratio as given in equation. Eye aspect ratio is approximately constant while the eye is open, but will rapidly fall to zero when a blink is taking place.

Eye Aspect Ratio:

Eye Aspect Ratio = w/hwhere,

'w' is the width of the eye

'h' is the height of the eye

Euclidean Distance Formula:

Euclidean Distance $d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2}$ where,

"d" is the Euclidean distance (here, d is 'h' or 'w')

(x1, y1) is the coordinate of the first point of the eye

(x2, y2) is the coordinate of the second point of the eye

Modules:

Image Acquisition: The camera is interfaced to locker which is controlled by python interface.

Face Detection: Facial landmarks can be used to detect the face of person.

Liveness Detection: Eye blink detection algorithm can be used to detect liveness.

Face Recognition: Neural network can be trained to recognize faces of user.

Access Control: Finally access control is achieved based on face and liveness detection.

V. RESULT AND CONCLUSION

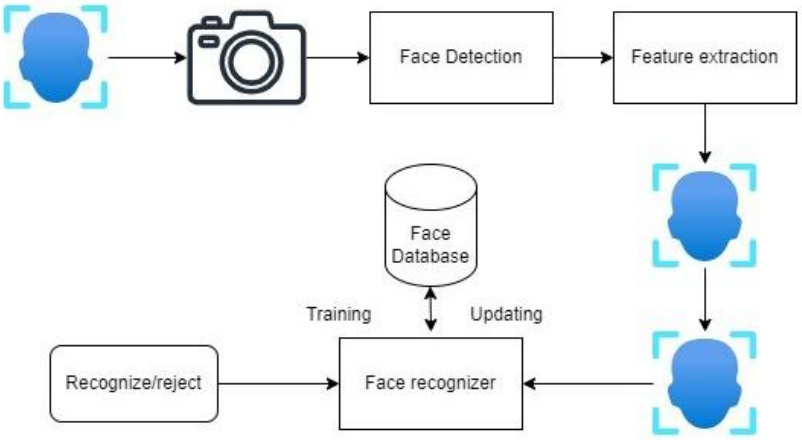
The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology In general, face recognition algorithms are not able to differentiate live face from not live face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph.on order to guard against such spoofing, a secure system needs liveness detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology In general, face recognition algorithms are not able to differentiate live face from not live face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph.on order to guard against such spoofing, a secure system needs liveness detection.

Result:

The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology In general, face recognition algorithms are not able to differentiate live face from not live face which is a major security issue. It is an easy way to spoof face recognition systems by facial pictures such as portrait photograph.on order to guard against such spoofing, a secure system needs liveness detection.



Conclusion

The authentic face detection for security assurance is the method implemented that generalizes the privacy concerns of the confidential data that requires secrecy conviction. The proposed method can be improved in terms of security assurance i.e., working in the area of face recognition for high level data authentication and security. This system provides a simple path for the future development of novel and more secured face liveliness detection approach for bank locker security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

VI. SUMMARY

6.1 ADVANTAGES

Following are some advantages of bank locker security system:

1. Provides high security.
2. Low cost.
3. Easy to implement.
4. No hack or crack to system.
5. Easy to use.
6. Fully automatic system.
7. Theft protection and alert

6.2. LIMITATIONS

1) One of the biggest disadvantages of online shopping is that this shopping the product is a delay in delivery sometimes.
2) Lack of interactivity.
3) Internet must.
4) Totally online system

6.3. APPLICATIONS

This system can be used in following areas:

1. In offices.
2. In Bank Lockers.
3. In identification.
4. In Jewellery shops
5. All that places when unique identity & high security is required.

6.4 Future Scope

1. The System can be implemented in embedded processors such as raspberry PI
2. Additional Securities can be used such as fingerprint recognition
3. The System can be further extended to other banking services

REFERENCES

[1]. "Face Spoofing Detection From Single images Using MicroTexture Analysis", Maatta, A. Hadid, M. Pietikainen.

[2]. K. Singh, P. Joshi and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement".

[3]. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink - based anti-spoofing in face recognition from a generic webcamera," in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[4]. J. Peng and P. P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," 2014 International Conference on Wavelet Analysis and Pattern Recognition.

[5]. Akhtar, Zahid & Micheloni, Christian & Foresti, G.L.. (2015). Biometric Liveness Detection: Challenges and Research Opportunities. IEEE Security & Privacy. 13. 63-72. 10.1109/MSP.2015.116.

[6]. D. Garud and S. S. Agrwal, "Face liveness detection," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016.

[7]. M. Co¸skun, A. U¸car, O. Yildirim and Y. Demir, "Face recognition based on convolutional neural network," 2017 International Conference on Modern Electrical and Energy Systems (MEES),IEEE; 2017

[8]. Li, L.; Feng, X.Y.; Jiang, X.Y.; Xia, Z.Q.; Hadid, A. Face anti-spoofing via deep local binary patterns. In Proceedings of the IEEE International Conference on Image Processing, Beijing, China, 17–20 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 101–105.