FILECOFFER: DECEPTION DETECTION AND FILE LOCKING MECHANISM USING FACE RECOGNITION POSTULATED ON HAAR CASCADES IN WINDOWS OS

*

Mohamed Afri Habeeb Mohamed
Department of Computer Technology
Madras Institute of Technology
Anna University
2021503029

Shivani Suresh
Department of Computer Technology
Madras Institute of Technology
Anna University
2021503050

Mugundh J B
Department of Computer Technology
Madras Institute of Technology
Anna University
2021503524

Shyamala R B
Department of Computer Technology
Madras Institute of Technology
Anna University
2021503558

***Abstract*—Deception is a complex and cunning act of humans, and detecting it can be challenging for social work professionals such as therapists and law enforcement officers.Neurotechnologies, such as recording electromagnetic signals from the brain, can provide valuable insights into a person's state of mind and level of deception. Machine learning models can be trained to detect changes in behavior, such as eye movements and gestures, and are becoming increasingly popular in deception detection.Psychological factors, such as a person's emotional state or personality traits, can also affect their ability to deceive or be detected. As such, some deception detection systems take these factors into account in their analysis.Finally, facial features have also been explored as a potential indicator of deception. Machine vision techniques can be used to study facial features from photos and score them based on factors such as eye movements and smiles.Overall, deception detection technology is a rapidly evolving field, and social work professionals should stay up-to-date with the latest techniques and approaches to effectively detect and address deception in their work.**

***Index Terms*—Deception-Detection, Lie-Detection, Machine-Vision, Machine-Learning, Visual Morphology, Face-Recognition**

I. Introduction

Despite the importance of detecting deception in social professions such as teaching and psychology, current methods rely heavily on human interpretation and are prone to error. There is a need for an automated deception detection system that is more accurate and reliable, and that eliminates psychological factors to provide more precise results. Additionally, this system should provide a straightforward indication of deception almost immediately, without significant processing time. Deception detection is an important area of research that has practical applications in law enforcement, security, and other fields. In recent years, there has been growing interest in using machine vision to analyze human physiognomy as a means of detecting deception. Machine vision, also known as computer vision, is a branch of artificial intelligence that uses algorithms and statistical models to analyze visual data from cameras and other sensors. By analyzing human physiognomy, which refers to the physical characteristics of a person's face, researchers can identify subtle cues that may indicate deception, such as changes in facial expressions, pupil dilation, and other physiological responses. To develop a deception detection system using machine vision, researchers must first collect a large dataset of video recordings of individuals engaged in truthful and deceptive behavior. They can then use machine learning algorithms to analyze the data and identify patterns of physiological response that are associated with deception.

One of the main advantages of machine vision-based deception detection is that it can be used in a non-invasive manner. Unlike other methods of deception detection, such as polygraph tests, machine vision does not require physical contact with the subject being analyzed. This makes it a more attractive option for use in settings such as airports or other public spaces, where traditional methods may be impractical. To develop a machine vision-based deception detection system, researchers typically begin by collecting a dataset of videos of individuals engaged in truthful and deceptive behavior. They may use actors to simulate different scenarios, or collect footage from real-world situations where deception may occur, such as interviews with suspects or witnesses. Once a dataset has been compiled, researchers can use machine learning algorithms to identify patterns of physiological response that are associated with deception. These algorithms may use a variety of techniques, such as deep learning or neural networks, to analyze the data and identify subtle changes in facial expressions, pupil dilation, or other physiological responses that may indicate deception.

One potential limitation of machine vision-based deception detection is that it may be less effective in detecting highlevel or strategic deception, where individuals may deliberately alter their behavior to avoid detection. Additionally, there may be cultural or individual differences in facial expressions and physiological responses that could affect the accuracy of the system.

II. Literature Review

Based on research by Vikram et al., builds a system to detect and recognize facial parts through images using the viola jones algorithm. The Viola-Jones face detection method has real-time detection rates created by Paul Viola and Michael Jones. To detect the eye area with Viola-Jones is determined with darker areas than the rest of the face based on the model you have, and the eyebrows will be removed. This paper uses Matlab to implement Haar Cascade classification as the main part of face detection determined by Haar features. The feature sought by the detection framework universally involves the number of image pixels in a rectangular area and provides an accuracy of 92

Another research by Gupta et al. created a face detection system that applies the Viola-Jones method using the Python programming language. This method combines the concepts of Haar, Integral Image, and AdaBoost features to be processed into a Cascade Classifier. The main part of this algorithm is computation and feature selection. In this Viola-Jones method, the Haar feature is used as a descriptor and then combines Integral Image and AdaBoost to find and select feature values and form a Cascade Classifier. Finally, Cascade Classifier is used to detect faces in images. The system can detect faces well with an accuracy rate of 90.0 for facial images and 75.5 for non-face images.

The following research by Leal et al. describes that when someone lies, it will immediately be followed by an increase in the number of blinks in the eye. Blink rate monitoring can be done non-intrusively through a camera that captures blinks and monitors retinal occlusion. Thus, in this study, observation for liars may not only be related to the blink of an eye. But also in some subtle movements after someone answers a question or tells a lie .

III. Proposed Work

Section A deals with the proposed architecture and Section B deals with the proposed algorithm. Section C deals with the theories and tools used for our project

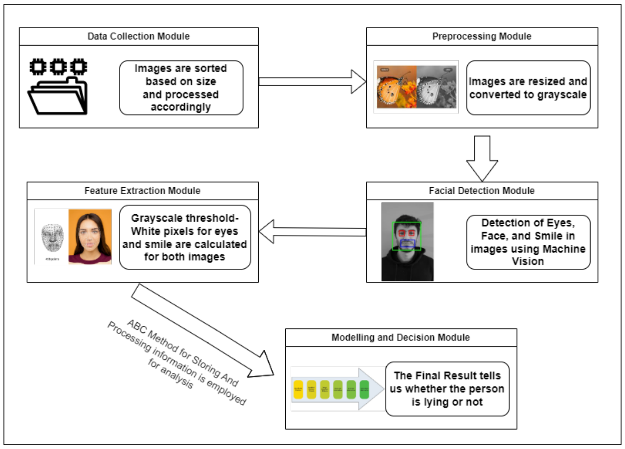
Data Collection Module
Images are sorted based on size and processed accordingly
Preprocessing Module
Images are resized and converted to grayscale
Feature Extraction Module
Grayscale threshold- White pixels for eyes and smile are calculated for both images
Facial Detection Module
Detection of Eyes, Face, and Smile in images using Machine Vision
ABC Method for Storing And Processing information is employed for analysis
Modelling and Decision Module
The Final Result tells us whether the person is lying or not

Fig. 1. Architecture Diagram Of Deception Detection

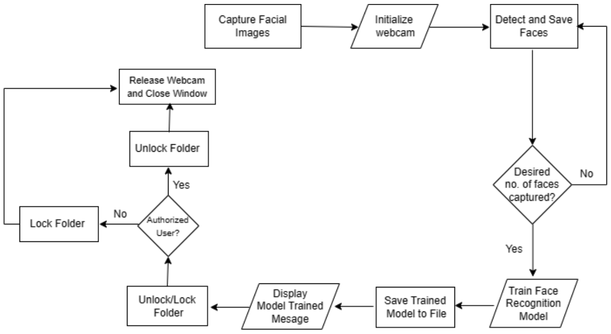
Capture Facial Images
Initialize webcam
Detect and Save Faces
Desired no. of faces captured?
No
Yes
Train Face Recognition Model
Save Trained Model to File
Display Model Trained Mesage
Unlock/Lock Folder
Authorized User?
No
Lock Folder
Yes
Unlock Folder
Release Webcam and Close Window

Fig. 2. Architecture Diagram Of FaceUnlockTech

A. Proposed Architecture

1) Deception Detector: The proposed architecture for the lie detector project involves using OpenCV to detect and compare facial expressions of an individual when telling the truth and when lying. The architecture includes various image processing steps, such as resizing the images and detecting facial features like the eyes and smile, which are then used to calculate changes in facial expressions. The results obtained from the analysis of these changes can then be used to infer whether the individual is telling the truth or lying. The proposed architecture detects facial features such as the face, eyes, and smile using pre-trained models and the detectMultiScale function. To improve the reliability of the detections, two new bounding boxes are created for the eyes and smile respectively.

The use of OpenCV and pre-trained models for detection helps to increase the accuracy of the results, while the counting of white pixels and size of the smile box provide a quantifiable measure for changes in facial expressions.

To calculate the changes in facial expressions between the two frames, the white pixels inside the eye and smile boxes are counted and compared. The fewer the white pixels in the eye box, the less open the eye, indicating a possible lie. The size of the smile box is used to determine the level of expressive mouth movement, with a smaller size indicating less movement and possibly a lie.

2) File Unlock: The system uses facial recognition technology to detect human faces in images and videos and generate a unique code for each face. This code is then compared to a database to determine whether to allow access to the individual. The lbpcascadefrontalface algorithm in OpenCV is used to detect frontal faces in images and videos. The system has four main functions - staticFaceDetectHaar, staticFaceDetectLbp, liveFaceDetectLbp, and liveFaceDetectHaar - that detect faces in static images and live video streams. The system allows users to add new faces to the database and trains the system using Local Binary Pattern Histogram (LBPH). The trained model is then used to predict and recognize faces in real-time. The system offers the advantage of quick access without any waiting time at the access point.

Fig. 3. Dataset for user authentication - converted to greyscale

In the case of a file unlock system, if the facial recognition technology and Haar cascades are implemented accurately and reliably, the system can provide enhanced security and convenience compared to traditional unlock methods. It can eliminate the need for passwords and provide a higher degree of security, as facial features are unique to each individual and cannot be easily replicated. However, the accuracy of the system may be impacted by various factors.

B. Proposed Algorithm

Algorithm 1 FindTheDeceit

```
Procedure ImageProcessing
$x$ ←Image with neutral expression
$y$ ←Test Image
Convert image ‘x’ and ‘y’ to grayscale and apply histogram equalization to enhance contrast.
Resize x and y and apply cascade classifier for face.
$UpperHalffaceArea \leftarrow img[fY : fY + fH/2, fX : fX + fW]$
$BottomHalffaceArea \leftarrow img[fY + fH/2 : fY + fH, fX : fX + fW]$
Apply cascade classifier for eyes and smile on the UpperHalffaceArea and BottomHalffaceArea of both images.
Draw bounding boxes around face, eyes and smile
end procedure
procedure DeceptionDetection
$pixels\_eyes$ ←white pixels in box around eyes
$pixels\_smile$ ←white pixels in box around eyes
if $pixels\_eyes\_x < pixels\_eyes\_yandpixels\_smile\_x < pixels\_smile\_y$ then
    Show message as “Person is lying”
else $\{pixels\_eyes\_x > pixels\_eyes\_yandpixels\_smile\_x > pixels\_smile\_y\}$
    Show message as “Person is lying”
end if
end procedure
```

Algorithm 2 FaceUnlockTech

```
Get the name of the folder to lock from the user.
Load the pre-trained face recognition model.
Initialize the webcam.
Start a loop that runs indefinitely.
Get a frame from the webcam.
Convert the frame to grayscale.
Detect faces in the frame.
If an authorized user is detected, unlock the folder.
If an authorized user is not detected, lock the folder.
Check for key press events.
Release the webcam and close the window.
```

C. Tools Used

1) Haar cascades: Haar Cascades are object detection algorithms that can be used to identify eyes, mouth, face, and other features of a human. One of the ways they do this is by using edge detection and line detection. More importantly, the algorithms are given a plethora of positive images, where in terms of face detection, a face is shown, and an equal number of negative images, where the face is not shown. It is trained to detect faces using these samples.6 Additionally, like a kernel or matrix, Haar Cascades use Machine Vision features to scan through an image to find these facial components.

2) Theory of Lie Detection: A lie detector is a system that is used to detect deception or dishonesty. It typically works by measuring physiological responses, such as changes in heart rate, blood pressure, and respiration, to determine whether a person is being truthful or deceptive. Lie detectors measure physiological responses to determine if a person is lying, such as changes in heart rate and respiration. Machine learning algorithms and libraries like OpenCV or scikit-learn can be used to analyze video streams and identify subtle changes in facial expressions, body language, or voice that may indicate deception. Additionally, sensors can be used to measure physiological responses, and Python libraries such as NumPy or SciPy can be used to analyze the sensor data and identify patterns or trends that may indicate deception. However, the accuracy of a lie detector can be affected by various factors such as the specific techniques and algorithms used, the training and experience of the person administering the test, and the individual characteristics of the person being

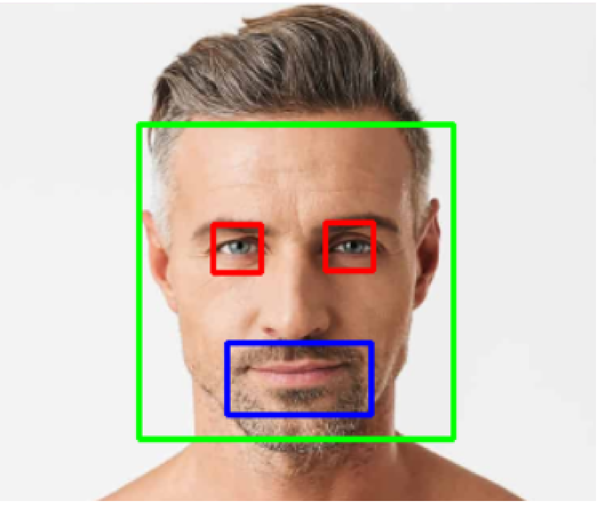

Fig. 4. Face,eyes and smile detection using Haar cascades

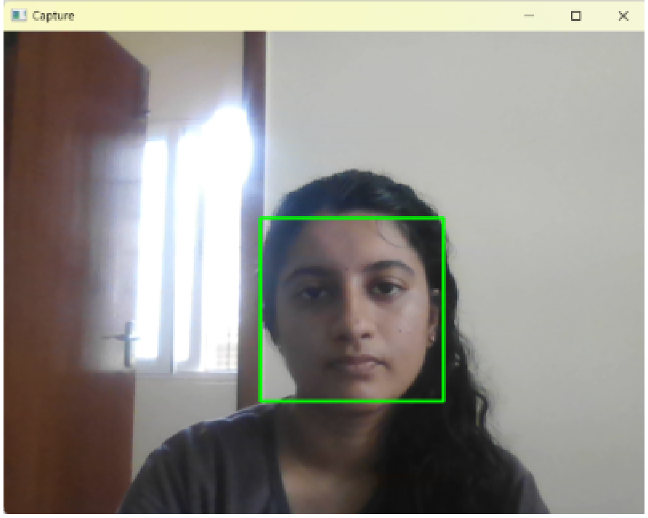

Fig. 5. Training the Face Model

tested.

3) ABC Method: The ABC method is a technique used in our lie detector to determine if a person is lying or telling the truth. It involves using a sample of a person's face when telling the truth (A) and a sample when telling a lie (B) to determine the unknown scenario (C). However, before the lie detector can determine C, it must be calibrated with A and B in a controlled environment that includes factors such as lighting, angle, and distance. If these factors are not controlled, noise in the video or image can be falsely flagged as part of the facial features, leading to inaccurate results. The ABC method is a recurring theme in the project, and it is important to ensure that the lie detector is properly calibrated and samples are taken in a controlled environment to ensure accurate results.

4) Shortest Job First: The SJF algorithm prioritizes the execution of files based on their size, giving smaller files priority over larger files to reduce overall processing time. When a file is requested for processing, it is compared to the sizes of other files in the queue, and smaller files are processed first while larger files are added to the end of the queue. However, this can lead to longer wait times for larger files, so some variants may use a threshold value to ensure larger files are not delayed excessively.

Overall, the SJF algorithm is a useful tool for file scheduling in certain contexts. By prioritizing smaller files, it can help to reduce overall processing time and improve system performance.

5) File Unlock using Facial Recognition: The proposed file unlock system using facial recognition would analyze the facial features of the user attempting to access a file and compare them to a pre-registered profile. This process would involve the use of image processing techniques such as Haar cascades. If the features match, the file is unlocked, and the user gains access.

Compared to traditional unlock methods that rely on passwords or PINs, this system eliminates the need for manual input and offers a higher degree of security since facial features are unique to each individual and cannot be easily replicated. This can make it more difficult for unauthorized access to occur. Additionally, it offers convenience, as users can simply look at the camera to unlock the file, which can save time and reduce the risk of forgotten or stolen passwords.

IV. Results

Our deception detection based file unlock system has been successfully implemented in the Windows Operating System. The system is made to allow only authorized users to access private files, thereby providing additional layer of security. The system was able to quickly analyse the falsities and lock the files making the system more secure. Immediate unlock was provided to authorized users after the comparison of their facial features with the database of authenticated user's images. The program is executed using Python and Microsoft Visual Studio Code which uses tkinter library to show pop up messages and Google Voice Assistant to announce the results of the deception test vocally.

V. Conclusion

The project is one in the context of operating systems, relating to the field of Protection and Security in Windows Operating systems. The project is mainly focussed to reduce the risk of unauthorized access thereby providing security by maintaining the image database of a specific user and authenticating them by a password set for each user. The proposed project, thus enhances the existing security in the Windows Operating Systems by using facial recognition based falsity detection to keep private files, safe and secure.

VI. References

[1] B. Singh, P. Rajiv and M. Chandra, ”Lie detection using image processing,” 2015 IEEE Transaction on Advanced Computing and Communication Systems, 2015, pp. 1-5

[2] D. -I. Noje and R. Malutan, ”Head movement analysis in lie detection,” 2015 IEEE Transaction on Grid, Cloud

and High Performance Computing in Science (ROLCG), 2015, pp. 1-4

[3] A. Thompson, ”The Cascading Haar Wavelet Algorithm for Computing the Walsh–Hadamard Transform,” in IEEE Signal Processing Letters, vol. 24, no. 7, pp. 1020-1023, July 2017

[4] S. Sumriddetchkajorn, A. Somboonkaew, T. Sodsong, I. Promduang, N. Sumriddetchkajorn and T. Prada-in, ”Simultaneous Analysis of Far Infrared Signals From Periorbital and Nostril Areas for Nonintrusive Lie Detection: Performance From Real Case Study,” in Journal of Lightwave Technology, vol. 33, no. 16, pp. 3406-3412, 2015

[5] A. A. Perdana et al., ”Lie Detector with Eye Movement and Eye Blinks Analysis Based on Image Processing using Viola-Jones Algorithm,” 2021 IEEE Transaction on Internet of Things and Intelligence Systems (IoTaIS) 2021, pp. 203-209

[6] S. Anwar, T. Batool and M. Majid, ”Event Related Potential (ERP) based Lie Detection using a Wearable EEG headset,” 2019 IEEE Transaction on Applied Sciences and Technology (IBCAST), 2019, pp. 543-547

[7] D. Kusumawati, A. A. Ilham, A. Achmad and I. Nurtanio, ”Vgg-16 And Vgg-19 Architecture Models In Lie Detection Using Image Processing,” 2022 IEEE Transaction on Information Technology, Information Systems and Electrical Engineering (ICITISEE), pp. 340-345

[8] T. A. Wibowo, M. Nasrun and C. Setianingsih, ”Lie Detector With Analysis Pupil Dilation And Eye Blinks Analysis Using Hough Transform And Decision Tree,” 2018 IEEE Transaction on Control, Electronics, Renewable Energy and Communications (ICCEREC), pp. 172-178

[9] Z. Labibah, M. Nasrun and C. Setianingsih, ”Lie Detector With The Analysis Of The Change Of Diameter Pupil and The Eye Movement Use Method Gabor Wavelet Transform and Decision Tree,” 2018 IEEE Transaction on Internet of Things and Intelligence System (IOTAIS) 2018, pp. 214-220

[10] S. V. Fernandes and M. S. Ullah, ”Use of Machine Learning for Deception Detection From Spectral and Cepstral Features of Speech Signals,” in IEEE Access, vol. 9, pp. 78925-78935, 2021

[11] Takeo Kanade. Computer recognition of human faces, volume 47. Birkh¨auser Basel, 1977

[12] Lawrence Sirovich and Michael Kirby. Low-dimensional procedure for the characterization of humanfaces. Josa a, 4(3):519–524, 1987.

[13] M. Turk and A. Pentland. Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1):71–86,Jan 1991

[14] Dong chen He and Li Wang. Texture unit, texture spectrum, and texture analysis. IEEE Transactionson Geoscience and Remote Sensing, 28(4):509–512, Jul 1990.

[15] X. Wang, T. X. Han, and S. Yan. An hog-lbp human detector with partial occlusion handling. In2009 IEEE 12th International Conference on Computer Vision, pages 32–39, Sept 2009.

[16] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman. Eigenfaces vs. fisherfaces: recognition usingclass specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence,19(7):711–720, Jul 1997

[17] P. Viola and M. Jones. Rapid object detection using a boosted cascade of simple features. In Proceed-ings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition.CVPR 2001, volume 1, pages I–511–I–518 vol.1, 2001

[18] Rainer Lienhart and Jochen Maydt. An extended set of haar-like features for rapid object detection.In Image Processing. 2002. Proceedings. 2002 International Conference on, volume 1, pages I–I.IEEE, 2002

[19] Meng Xiao He and Helen Yang. Microarray dimension reduction, 2009

[20] John P Lewis. Fast template matching. In Vision interface, volume 95, pages 15–19, 1995