Communication and Computer Engineering Research Magazine, Vol (1), No (1), 2024.

Elevating Smart Home Security and Personalization Through Advanced Face Detection Technology

Moataz M. Elsherbiny*, Ahmed M. Radwan*, Alaa H. Hussien, Hania A. Salah, Menna A. Galal, Mennatullah Y. Kewan, Nour M. Nasr, Nihal A. Zein, Ola R. Abdulrazeq, Yasmeen N. Saad, Youmna E. Fahmy, Sabry F. Saraya

Mansoura University, Faculty of Engineering, Computers and Communication Engineering Department, Mansoura, Egypt

*: Corresponding Author

Research Paper Data:

- *Paper ID:*
- *Submitted:*
- *Revised:*
- *Accepted:*

Abstract

According to who live now, security has emerged as the most crucial aspect of human existence. Right now, cost is the most important consideration. This approach is a great way to cut down on the expense of having outside observers track the movement. Face recognition technology can enhance security in smart homes by replacing traditional security systems with AI-based systems, providing a secure and convenient access control mechanism. The goal of this research is to create a facial detection-enabled door lock system for smart homes, preventing unwanted entry and boosting security in general. The suggested system is made to support many users and restrict access to those who have registered. The technology uses an impenetrable method to confirm that actual faces are there and excludes images that are either printed or digital. This project uses computer vision and artificial intelligence to help establish a quick, safe, and effective way to use facial recognition technology to increase the security of smart homes.

Keywords: *Smart Homes, Security, Face Recognition, IoT, Computer Vision, Ai* .

1. Introduction

An intelligent home security system is a combination of several advanced technology-driven components working together to improve your home’s security. It often includes video surveillance & security cameras Cyprus, providing real-time visual and video footage of your property, alarm systems to notify you of a potential security breach, motion sensors to detect an unusual movement in your property, smart locks and access control systems such as ID card access and parking access controls to ensure secure access to your premises, smart device integration to enable the plug-and-play smart home concept where all devices work together to communicate and coordinate, etc. However, these components are not isolated devices; rather, they are part of an interconnected network or cybersecurity mesh architecture that works with the goal of creating the ultimate smart home system. [1] Smart home security system benefits include Increased safety as Smart home security systems improve security in a number of ways by connecting various security components, including access control, security cameras, alarms, and more. For instance, you can monitor your home in real time and get alerts right away if something unusual happens. Remote management and observation When you are away from home, you may remotely monitor and manage your smart home system. Your IT solutions' integration with your smart home system has made this possible. Simplicity: All security components are connected through the smart home security system, making system management and control simple. [1] In the IoT platform for smart homes, computer vision can display additional security systems. It is able to identify someone who is at the wrong place at the wrong time and who might be harmful to the surroundings. [2] Facial recognition is a way of identifying or confirming an individual’s identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Many people are familiar with it via the FaceID feature that unlocks iPhones. Generally, facial recognition identifies and recognizes one person as the exclusive owner of the device, restricting access to others, without the need for a large library of images to establish an individual's identification. [3] It has a wide range of significant applications in the following areas: digital libraries, law enforcement, access control, credit card verification, criminal identification, public security, information security, and human-computer intelligent interaction. People in public places including homes, workplaces, airports, retail malls, and banks are typically recognized by it. By detecting motion that is managed by the embedded system, this technique allows for safe entry into the home. The most significant portion of a person's body is their face. As a result, it can convey a wide range of feelings. Long ago, smart cards, plastic cards, PINS, tokens, and keys were among the inanimate objects that people used for identification and entry to places that were restricted, such as ISRO, NASA, and DRDO. The nose, eyes, and mouth are the most crucial aspects of the face picture since they are linked to facial extraction. This research aims to investigate and compare different classifier types utilized in facial recognition security systems based on their accuracy. MagFace technique was used for face recognition in order to achieve fast discriminatory performance and good results, according to numerous researches.

2. Background

Smart home security is being revolutionized by face recognition technology, which provides a strong substitute for traditional entry techniques. This research paper compares various face recognition classifiers in smart door locks, highlighting their critical role in providing ease and security. We investigate different classifiers in an effort to determine which method works best for practical use. There are several benefits to integrating face recognition technology into smart home systems, both in terms of security and user experience. Our project aims to contribute to the advancement of smart home security measures by showcasing the usefulness and efficacy of this integration. This research emphasizes how crucial biometric authentication is to preventing unwanted access to smart homes. The application of facial recognition technology has enormous potential to improve. The integration of facial recognition technology presents significant promise for augmenting the general security stance of intelligent home settings. In conclusion, this paper clarifies how face recognition technology is revolutionizing accessibility and security for smart homes.

3. Related Work

In 1997, Belhumeur et al.[4] developed "Fisherface" which is a face recognition method that deals with changes in lighting and facial expressions. It uses a mathematical approach to group similar images of faces together, even when there are differences in lighting or expression. This method outperforms other techniques in recognizing faces accurately, even with minimal computational resources. In 2001, Jamil et al [5] tested a method for recognizing faces using eigenfaces and neural networks. Eigenfaces pick out key facial features, reducing images to simpler data. The neural network learns to identify faces based on these simplified images. The system was accurate 95.6% of the time on a database of 80 face images from eight people, especially when the faces were straight on. In 2003, D´eniz et al.[6] proposed a paper that combines two techniques, support vector machines (SVM) and independent component analysis (ICA), for face recognition. It finds that while both combinations, ICA/SVM and PCA/SVM, achieve high recognition rates, PCA/SVM is more practical due to shorter training times. In 2018, Fatihah et al[7] build a face recognition system using LBP and nearest neighbor algorithms. The system was tested on three datasets and achieved high accuracy, especially on simpler datasets like JAFFE. Also in the same year, Bhatia et al.[8] used IoT and facial recognition to boost home security. employing Local Binary Pattern Histograms to recognize family members. The system ensures security, real-time monitoring, and automation. Raspberry Pi 3, a webcam, a speaker, and a stepper motor were used to implement this system. In 2020,Pinjala et al.[9] proposed a smart lock system that lets controlling and monitoring door remotely with a smartphone app. It includes a camera activated by the doorbell, sending notifications to your phone. You can view and decide whether to allow or deny access by entering a password. Moreover, you can send audio messages to visitors.

4. Project Details

This project employs artificial intelligence to create a door access system that only allows entry when a recognized face is detected by the recognition algorithms. When a person approaches the door, the system verifies their identity based on facial recognition. If the person's face is recognized, the door will unlock; otherwise, it remains locked.

In order to implement facial recognition technology with high accuracy, it was necessary for us to utilize a classifier that provides high accuracy. We conducted research on projects similar to ours,. We compared their results, datasets and their classifiers to find the most effective one.

Method	LFW	AgeDB	CFP-FP	CALFW	CPLFW
Softmax	99.45	96.58	92.67	93.52	86.27
Center loss[10]	99.65	96.83	93.37	94.23	86.58
Triplet loss[11]	99.58	96.27	92.30	93.27	85.07
UniformFace[12]	99.70	96.90	94.34	94.40	87.45
SphereFace[13]	99.70	96.43	93.86	94.17	87.81
CosFace[14]	99.73	97.53	94.83	95.07	88.63
ArcFace[15]	99.75	97.68	94.27	95.12	88.53
AdaCos[16]	99.68	97.15	94.03	94.38	87.03
Ada-Softmax[17]	99.74	97.68	94.96	95.05	88.80
MV-softmax[18]	99.72	97.73	93.77	95.23	88.65
ArcNegFace[19]	99.73	97.37	93.64	95.15	87.87
CurricularFace[20]	99.72	97.43	93.73	94.98	87.62
CircleLoss[21]	99.73	-	96.02	-	-
NPCFace[22]	99.77	97.77	95.09	95.60	89.42
MagFace[23]	99.83	98.17	98.46	96.15	92.87
AdaFace[24]	99.80	97.90	99.17	96.05	94.63

Table 1: Verification accuracy (%) on easy benchmarks

Method	IJB-B 1e-4	IJB-B 1e-5	IJB-C 1e-4	IJB-C 1e-5
Softmax	85.66	73.63	86.62	96.48
Center loss[10]	86.43	74.16	86.87	76.64
Triplet loss[11]	73.21	40.37	78.12	48.07
UniformFace[12]	87.22	75.01	88.87	79.64
SphereFace[13]	86.67	74.75	87.92	78.77
CosFace[14]	90.60	82.28	91.72	86.68
ArcFace[15]	90.83	82.68	91.82	85.75
AdaCos[16]	86.04	73.34	87.53	78.91
AdaM-Softmax[17]	90.54	82.70	91.64	86.84
MV-softmax[18]	90.67	83.17	92.03	87.52
ArcNegFace[19]	90.62	81.59	90.91	85.64
CurricularFace[20]	90.04	81.15	90.95	84.63
NPCFace[22]	92.02	85.59	92.90	88.08
MagFace[23]	94.51	90.36	95.97	94.08
AdaFace[24]	96.03	-	97.39	-

Table 2: Veri_cation accuracy (%) on IJB-B and IJB-C.

Then we find that:

From Table 1 (Verification accuracy (%) on easy benchmarks):

- The highest accuracy values are:
  - LFW: MagFace (99.83%)
  - AgeDB: MagFace (98.17%)
  - CFP-FP: MagFace (98.46%)
  - CALFW: MagFace (96.15%)
  - CPLFW: MagFace (92.87%)

From Table 2 (Verification accuracy (%) on IJB-B and IJB-C):

- The highest accuracy values are:
  - IJB-B 1e-4: AdaFace (96.03%)
  - IJB-B 1e-5: MagFace (90.36%)
  - IJB-C 1e-4: MagFace (95.97%)
  - IJB-C 1e-5: MagFace (94.08%)

Overall, MagFace consistently achieves the highest accuracy across multiple benchmarks and configurations. Therefore, MagFace can be considered the classifier with the highest accuracy among those listed and this is the classifier that we use.

About MagFace:

A class of face recognition losses known as MagFace learns a universal feature embedding whose size can be used to gauge a face's quality. It is demonstrated that, with the new loss, the likelihood of the subject being recognized increases monotonically with the feature embedding magnitude. Furthermore, MagFace presents an adaptive method that draws easy samples into class centers and pushes hard samples away in order to learn a well-structured within-class feature distribution. By using an adaptive approach to learn well-structured within-class feature distributions, MagFace helps prevent model overfitting on noisy and low-quality examples for face recognition by attracting easy samples to the center of the class and pushing away hard sample[25].

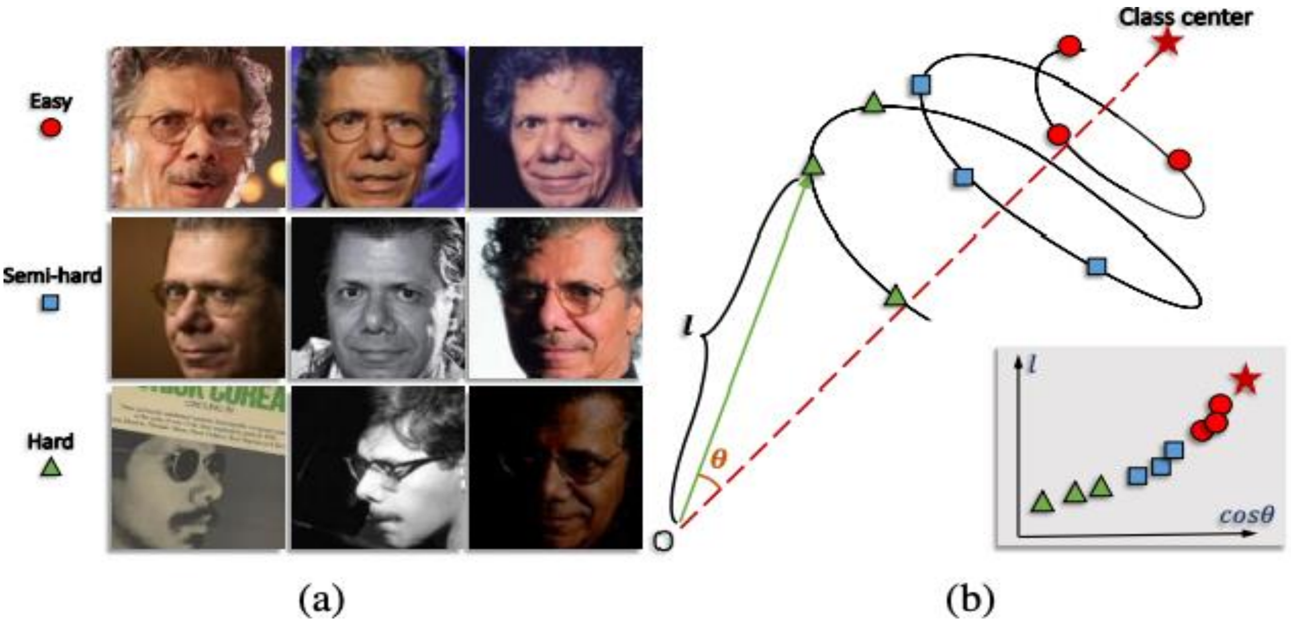


Figure (1)

Figure (1): MagFace learns for (a) in-the-wild faces (b) a universal embedding by pulling the easier samples closer to the class center and pushing them away from the origin o. As shown in this experiments and supported by mathematical proof, the magnitude I before normalization increases along with feature's cosine distance to its class center, and therefore reveals the quality for each face, The larger the l, the more likely the sample can be recognized.[25]

- **Key Features:[26]**
  - **Margin-Aware Loss**: MagFace incorporates a margin-aware loss function, which aims to increase the margin between intra-class and inter-class face representations. This helps in better separating face identities in feature space.
  - **Feature Enhancement**: The architecture and training strategies used in MagFace are designed to enhance the discriminative power of feature representations, making them more robust to variations in pose, expression, lighting, and other factors.

- **Applications:[27]**
  - **Biometric Security:** MagFace can be used in a number of biometric security applications, such as identity verification, access control, and surveillance systems. Because of its great precision and resilience, it can be used in situations where accurate identification of persons is essential.
  - **Smart Devices**: MagFace can be included for user authentication and customized user experiences into smart devices, such tablets and smartphones. It makes digital services and apps convenient and safe to use.
  - **Law Enforcement:** MagFace and other face recognition technology can help law enforcement find missing people, identify suspects, and improve public safety. They can be used to automate and speed up the identification process in conjunction with surveillance cameras and facial recognition databases.

3. Research Contributions:

MagFace has contributed to advancing the state-of-the-art in face recognition by achieving high accuracy on various benchmark datasets. Its performance has been evaluated and validated in research studies and competitions, demonstrating its effectiveness in real-world applications

4. Pros:[28]

- **High Accuracy:** MagFace is really good at recognizing faces accurately.
- **Robustness:** It can handle different lighting, facial expressions, and angles well.
- **Margin-Aware Loss:** The way it learns helps it tell faces apart better.
- **Versatility:** MagFace can be used in lots of different situations, like security and law enforcement.
- **Research Contribution:** It helps make face recognition technology better overall.

5. Cons:

- **Complexity:** It's hard to set up and needs a lot of computer power.
- **Data Dependency:** It needs a ton of good quality pictures to learn from.
- **Ethical Concerns:** Using it might raise big questions about privacy and fairness.
- **Vulnerability to Attacks:** It can be tricked by sneaky changes to pictures.

This was an introduction to what we researched and looked for before starting work on our project. Now, this is what we're working on:

The PEAS description for this system is as follows:

- **Performance Measure**: Rapid response, high security, cost-effective
- **Environment:** Main door entrance
- **Actuator**: Image capture
- **Sensors**: Camera In this setup, the environment is fully observable, meaning the camera sensor can perceive the complete state of the agent (person) at any given time.

Additionally, an infrared sensor is planned to be incorporated so that the camera activates when someone approaches the door's proximity, enhancing both convenience and security measures.

During the setup process, the camera captures an image of the user's face, which is then converted to gray scale to expedite processing. Subsequently, real-time face detection occurs using the camera at the door.

The detected face image is compared to stored images in the database. If a match is found, the door unlocks; otherwise, it remains locked. This integration of facial recognition technology not only enhances convenience but also strengthens the security of smart homes, ensuring that only authorized individuals gain access.

ARCHITECTURE

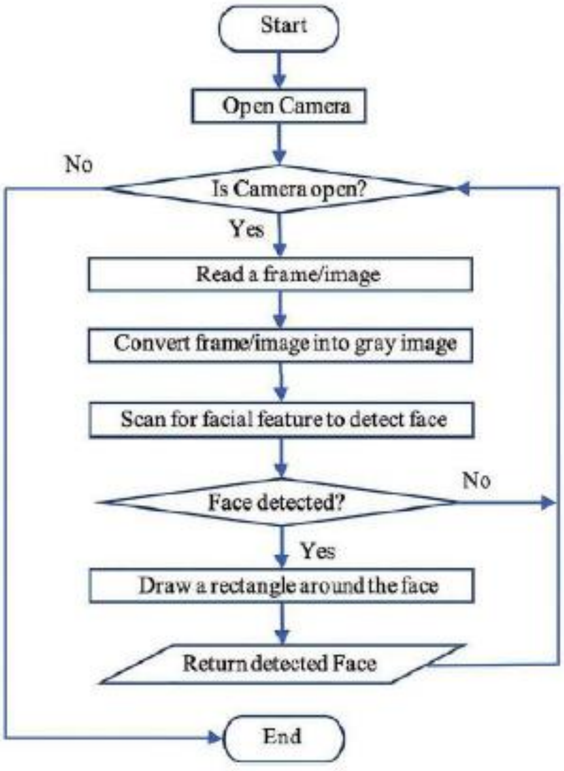

Start
Open Camera
No
Is Camera open?
Yes
Read a frame/image
Convert frame/image into gray image
Scan for facial feature to detect face
No
Face detected?
Yes
Draw a rectangle around the face
Return detected Face
End

Figure (2) - Architecture diagram

During the setup process, the camera captures an image of the user's face, which is subsequently converted to gray scale to expedite processing. The face detected by the camera in real-time serves as the input. This captured face image is then compared to stored images in the database. Depending on the match result, the door will either unlock or remain locked. This robust facial recognition process not only enhances convenience but also bolsters the security of smart homes, ensuring that only authorized individuals gain access.

The implementation:

- In order to make it easier to identify faces in grayscale, the first photographs of the subject are taken and converted from RGB to grayscale. Here's where OpenCV becomes useful. Following that, the picture manipulation, which includes cropping, resizing, blurring, and sharpening photos as necessary.
- The next stage is image segmentation, which divides an image into segments or uses contour detection to identify many items in a single image so that the classifier can identify faces and objects in the image fast. The method for Haar-Like features is now used. With the use of edge, line, and center detection, this algorithm locates the locations of the human faces inside a frame or image, identifying features like the mouth, nose, and eyes.
- The coordinates of x, y, w, and h are then entered, creating a rectangular box in the image that indicates where the face is located. Numerous more detecting methods are also employed in tandem for detection, such the detection of a grin, an eye, a blink, etc. A scale that is smaller than the selected image is chosen.

  The average of the pixel values in each part is then calculated once it has been put on the image.
- If the difference between two values pass a given threshold, it is considered a match. Face detection on

a human face is performed by matching a combination of different Haar-like-features.[29]

- The facial recognition process consists of three stages:
  1. Gathering photos, which we have already completed
  2. Extracting unique features, classifying them..
  3. Predicting identification by comparing an incoming image's attributes to those in stored pictures.
- Faces in an image can be clipped and transferred for recognition using a face detector.
- This is done using the same technique used for the image capture application.
- FaceRecognizer makes a prediction in order to detect faces.predict() verifies confidence by comparing each image in the dataset with the supplied image.

The steps:[30]

- Hardware setup: We have linked the door lock's servo motor to our Arduino board[31]. Moreover, instead of an external 2MP door cam, we are using the laptop’s webcam.
- The webcam on our laptop will capture the facial photographs, which will then undergo a series of cropping and editing steps. The Open CV package is going to take care of this. After that, they'll be kept in the database. The original image is altered, cropped, and changed from RGB to grayscale. It is for Multi user as well, Face will be matched with all of the stored faces and if it matches, then door will unlock or else not
- Dataset Training: After our algorithm has been trained using the samples, it will provide the training result.

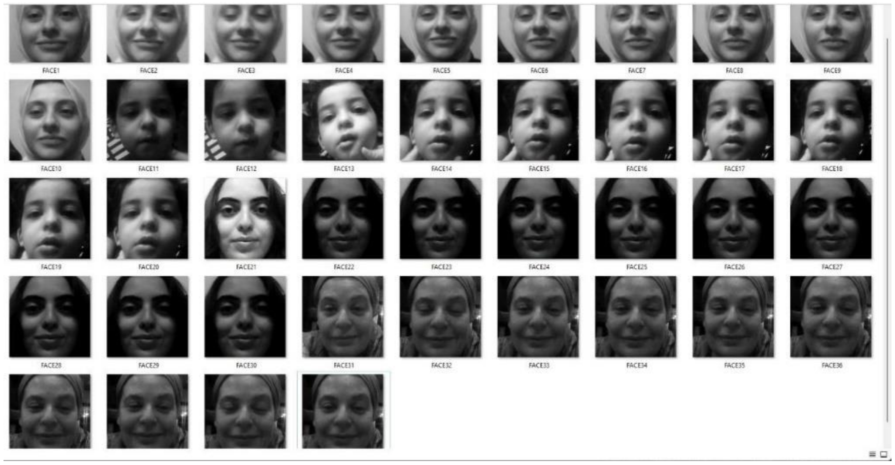
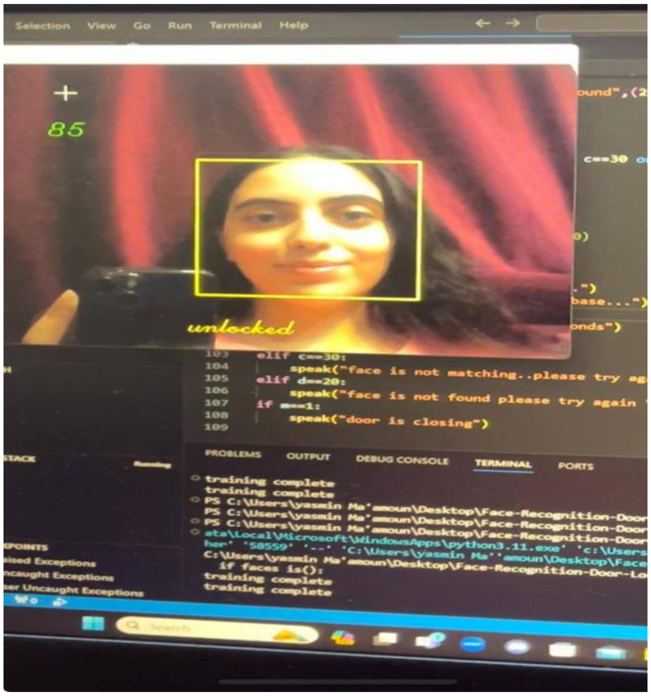


Figure (3) - Program is trained to recognize each face.

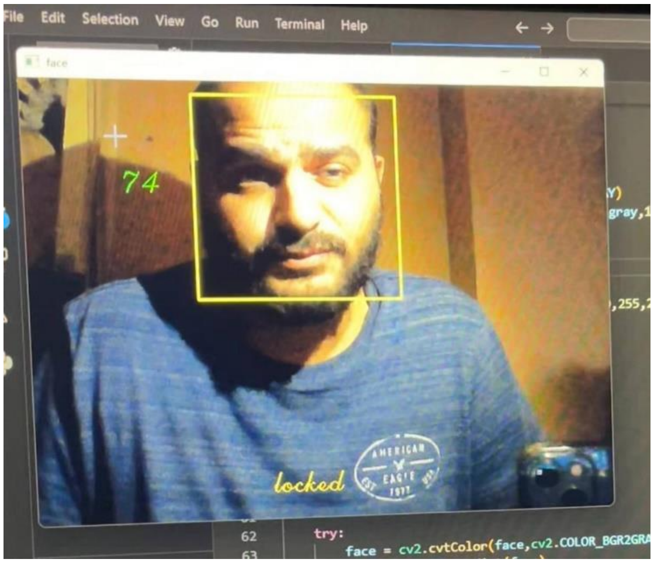
- Then when a face is detected at camera, program scans and authenticates it with the database. On successful recognition door will unlock and on failed recognition, relevant message will be said and displayed


Selection View Go Run Terminal Help
85
unlocked
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
    elif c==30:
        speak("face is not matching..please try ag
    elif d==20:
        speak("face is not found please try again
    if m==1:
        speak("door is closing")
```

```
training complete
training complete
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
ata\Local\Microsoft\WindowsApps\python3.11.exe' 'c:\Users
her' '58559' '--' 'C:\Users\yasmin Ma''amoun\Desktop\Face
C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lo
  if faces is():
training complete
training complete
```

Figure (4) - when the image is matched.



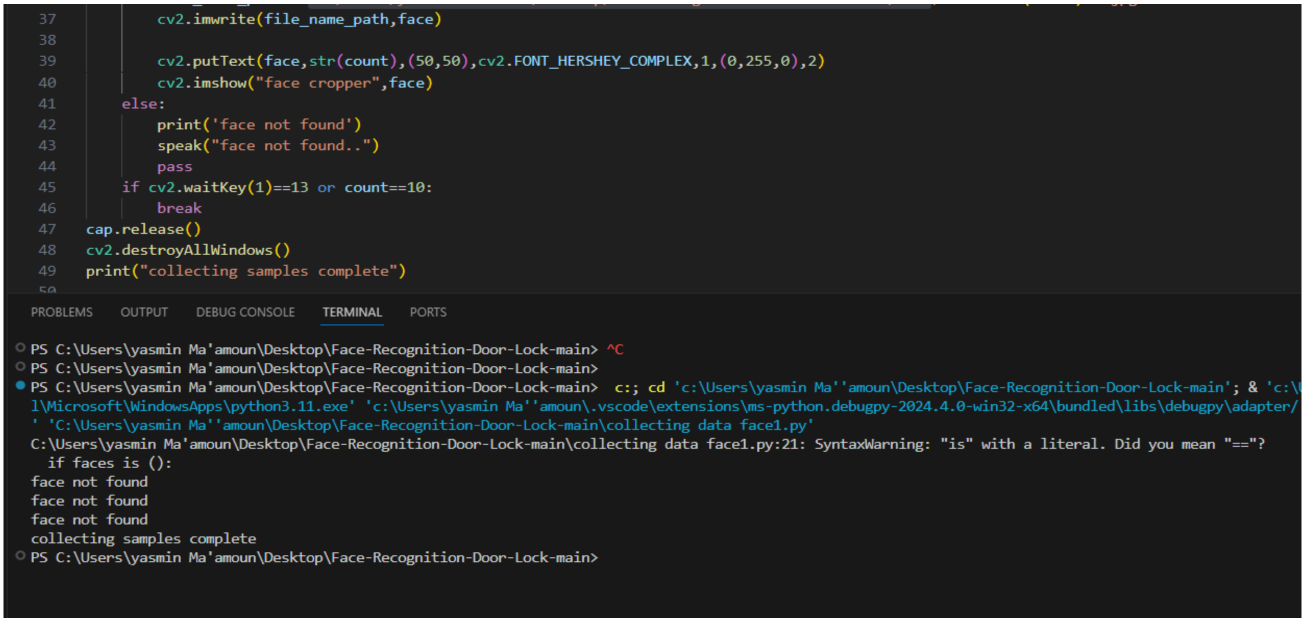
```
try:
    face = cv2.cvtColor(face,cv2.COLOR_BGR2GRA
```

Figure (5) - when the image not matched.

- Door Lock/Unlock Mechanism: Upon an individual's arrival, the camera will take their picture and cross-reference it with the database. The door will unlock and the servo motor will run for five seconds while a welcome voice is audible if the percentage matches. In the event that facial detection is unsuccessful or authentication fails, the door will remain locked and an alert voice will be audible.[32] [33]

5. Results

First : Collecting 10 face samples data for training.



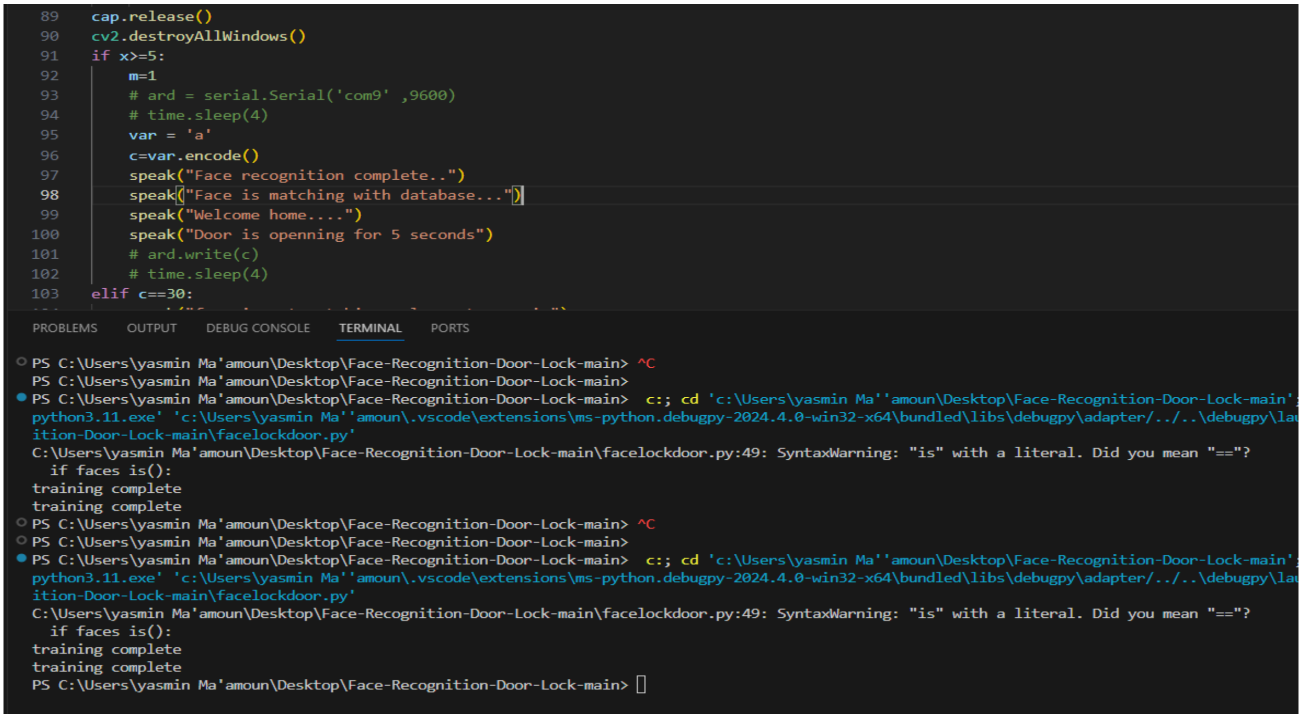
```
        cv2.imwrite(file_name_path,face)

        cv2.putText(face,str(count),(50,50),cv2.FONT_HERSHEY_COMPLEX,1,(0,255,0),2)
        cv2.imshow("face cropper",face)
    else:
        print('face not found')
        speak("face not found..")
        pass
    if cv2.waitKey(1)==13 or count==10:
        break
cap.release()
cv2.destroyAllWindows()
print("collecting samples complete")
```

```
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main> ^C
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>  c:; cd 'c:\Users\yasmin Ma''amoun\Desktop\Face-Recognition-Door-Lock-main'; & 'c:\
l\Microsoft\WindowsApps\python3.11.exe' 'c:\Users\yasmin Ma''amoun\.vscode\extensions\ms-python.debugpy-2024.4.0-win32-x64\bundled\libs\debugpy\adapter/
' 'C:\Users\yasmin Ma''amoun\Desktop\Face-Recognition-Door-Lock-main\collecting data face1.py'
C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main\collecting data face1.py:21: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if faces is ():
face not found
face not found
face not found
collecting samples complete
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>
```

Figure (6) - Collecting Face Data.

Second: Training the face samples inside our database for accurate results.

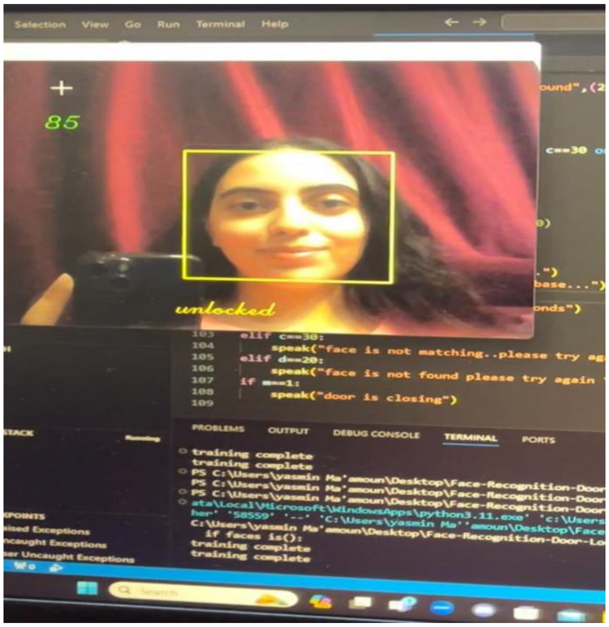


```
cap.release()
cv2.destroyAllWindows()
if x>=5:
    m=1
    # ard = serial.Serial('com9' ,9600)
    # time.sleep(4)
    var = 'a'
    c=var.encode()
    speak("Face recognition complete..")
    speak("Face is matching with database...")
    speak("Welcome home....")
    speak("Door is openning for 5 seconds")
    # ard.write(c)
    # time.sleep(4)
elif c==30:
```

```
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main> ^C
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>  c:; cd 'c:\Users\yasmin Ma''amoun\Desktop\Face-Recognition-Door-Lock-main';
python3.11.exe' 'c:\Users\yasmin Ma''amoun\.vscode\extensions\ms-python.debugpy-2024.4.0-win32-x64\bundled\libs\debugpy\adapter/../..\debugpy\la
ition-Door-Lock-main\facelockdoor.py'
C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main\facelockdoor.py:49: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if faces is():
training complete
training complete
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main> ^C
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>  c:; cd 'c:\Users\yasmin Ma''amoun\Desktop\Face-Recognition-Door-Lock-main';
python3.11.exe' 'c:\Users\yasmin Ma''amoun\.vscode\extensions\ms-python.debugpy-2024.4.0-win32-x64\bundled\libs\debugpy\adapter/../..\debugpy\la
ition-Door-Lock-main\facelockdoor.py'
C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main\facelockdoor.py:49: SyntaxWarning: "is" with a literal. Did you mean "=="?
  if faces is():
training complete
training complete
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lock-main>
```

Figure (7) - Training Samples.

Finally: face recognition by the camera to decide to open the door or not , if the face is recognized from previous samples the door will open automatically and stays open for 5 second , but if the camera didn't recognize the face the door won't open and try again.



```
elif c==30:
    speak("face is not matching..please try ag
elif d==20:
    speak("face is not found please try again
if m==1:
    speak("door is closing")
```

```
training complete
training complete
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
PS C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door
ata\Local\Microsoft\WindowsApps\python3.11.exe' 'c:\Users
her' '58559' '--' 'C:\Users\yasmin Ma''amoun\Desktop\Face
C:\Users\yasmin Ma'amoun\Desktop\Face-Recognition-Door-Lo
  if faces is():
training complete
training complete
```

Figure (8) - Face Recognition in Progress.

6. Conclusion

In conclusion, this study underscores the critical role of facial recognition technology in fortifying the security of smart homes. Through a meticulous review of literature, we evaluated the efficacy of various classifiers, culminating in the selection of MagFace for implementation in our system. Our integration of artificial intelligence and computer vision, facilitated by Python and OpenCV, empowered us to develop a robust face recognition door lock/unlock system using Arduino UNO. By seamlessly integrating servo motors with door locks, our prototype demonstrates the practical application of this technology, where the door's locking mechanism responds dynamically to recognized faces. This endeavor represents a significant stride towards enhancing home security through innovative engineering solutions.

7. future work

Looking ahead, there are several avenues for further research and development in the realm of facial recognition technology applied to security systems:

Expanding the Scope: We envision undertaking more extensive projects encompassing larger datasets and exploring the efficacy of diverse classifiers, including neural networks and other advanced machine learning algorithms. By incorporating larger datasets, we can enhance the accuracy and robustness of our system, thereby extending its applicability to a wider range of environments and scenarios.

Scaling Up: In addition to residential applications, we intend to extend the deployment of our facial recognition system to larger-scale installations. This could involve implementing the technology at compound gates, corporate facilities, or high-security areas such as bank vaults and government buildings. By adapting our solution to larger contexts, we aim to address the security needs of diverse settings with varying levels of complexity.

Integration with Mobile Applications: To further augment the functionality and user-friendliness of our system, we plan to develop a complementary mobile application. This application will serve as a centralized interface for homeowners or security personnel to monitor and manage access control remotely. In the event of an unrecognized face detection, the application will promptly notify the homeowner and provide them with the captured image for verification. Additionally, we envision integrating the system with other smart home devices, such as windows, curtains, and all entry points, to create a comprehensive and seamlessly integrated security ecosystem.

8. References:

[1] *Why smart home security systems are essential today*. A.F.I.T Pro Business Solutions Ltd. (n.d.). https://itpro.cy/why-smart-home-security-systems-are-essential-today-2/#:~:text=Benefits%20of%20Smart%20Home%20Security%20Systems&text=Real%2Dtime%20surveillance%20and%20alerts,and%20control%20the%20system%20remotely.

[2] Othman, N. A., & Aydin, I. (2018). A face recognition method in the internet of things for security applications in smart homes and cities. *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*. https://doi.org/10.1109/sgcf.2018.8408934.

[3] Kaspersky. (2024, March 14). *What is facial recognition – definition and explanation*. usa.kaspersky.com. https://usa.kaspersky.com/resource-center/definitions/what-is-facial-recognition.

[4] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, “Eigenfaces vs. fisherfaces: Recognition using class specific linear projection,” IEEE Transactions on pattern analysis and machine intelligence, vol. 19, no. 7, pp. 711–720, 1997.

[5] N. Jamil, S. Lqbal and N. Iqbal, "Face recognition using neural networks," Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century., Lahore, Pakistan, 2001, pp. 277-281, doi: 10.1109/INMIC.2001.995351.

[6] O. D´eniz, M. Castrillon, and M. Hern´andez, “Face recognition using independent component analysis and support vector machines,” Pattern recognition letters, vol. 24, no. 13, pp. 2153–2157, 2003.

[7] N. N. Fatihah, G. Ariyanto, A. J. Latipah and D. M. Pangestuty, "Face Recognition Using Local Binary Pattern and Nearest Neighbour Classification," 2018 International Symposium on Advanced Intelligent Informatics (SAIN), Yogyakarta, Indonesia, 2018, pp. 142-147, doi: 10.1109/SAIN.2018.8673375.

[8] P. Bhatia, S. Rajput, S. Pathak and S. Prasad, "IOT based facial recognition system for home Security using LBPH algorithm," 2018 3rd International Conference on InventiveComputation Technologies (ICICT), Coimbatore, India, 2018, pp. 191-193, doi:10.1109/ICICT43934.2018.9034420.

[9] Pinjala, S. R., & Gupta, S. (2020). 2020 International Conference on Wireless Communications, Signal Processingand Networking, WiSPNET 2020. 2020 International Conference on Wireless Communications, SignalProcessing and Networking, WiSPNET 2020, 44–47.

[10] Y.Wen, K. Zhang, Z. Li, and Y. Qiao, \A discriminative feature learning approach for deep face recognition,"in European conference on computer vision, pp. 499{515, Springer, 2016.

[11] F. Schro_, D. Kalenichenko, and J. Philbin, \Facenet: A uni_ed embedding for face recognition and clustering," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815{823,2015.

[12] Y. Duan, J. Lu, and J. Zhou, \Uniformface: Learning deep equidistributed representation for face recognition,"in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3415{3424, 2019.

[13] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, and L. Song, \Sphereface: Deep hypersphere embedding for face recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 212{220,2017.

[14] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, \Cosface: Large margin cosine loss for deep face recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5265{5274, 2018.

[15] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, \Arcface: Additive angular margin loss for deep face recognition," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 4690{4699, 2019.

[16] X. Zhang, R. Zhao, Y. Qiao, X. Wang, and H. Li, \Adacos: Adaptively scaling cosine logits for e_ectively learning deep face representations," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 10823{10832, 2019.

[17] H. Liu, X. Zhu, Z. Lei, and S. Z. Li, \Adaptiveface: Adaptive margin and sampling for face recognition," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 11947{11956,2019.

[18] X. Wang, S. Zhang, S. Wang, T. Fu, H. Shi, and T. Mei, \Mis-classi_ed vector guided softmax loss for face recognition," in Proceedings of the AAAI Conference on Arti_cial Intelligence, vol. 34, pp. 12241{12248,2020.

[19] Y. Liu et al., \Towards ops-constrained face recognition," in Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops, pp. 0{0, 2019

[20] Y. Huang, Y.Wang, Y. Tai, X. Liu, P. Shen, S. Li, J. Li, and F. Huang, \Curricularface: adaptive curriculum learning loss for deep face recognition," in proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 5901{5910, 2020.

[21] Y. Sun, C. Cheng, Y. Zhang, C. Zhang, L. Zheng, Z. Wang, and Y. Wei, \Circle loss: A uni_ed perspective of pair similarity optimization," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 6398{6407, 2020.

[22] D. Zeng, H. Shi, H. Du, J. Wang, Z. Lei, and T. Mei, \Npcface: A negative-positive cooperation supervision for training large-scale face recognition," arXiv preprint arXiv:2007.10172, 2020.

[23] Q. Meng, S. Zhao, Z. Huang, and F. Zhou, \Magface: A universal representation for face recognition and quality assessment," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 14225{14234, 2021.

[24] M. Kim, A. K. Jain, and X. Liu, \Adaface: Quality adaptive margin for face recognition," in Proceeding of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 18750{18759, 2022.

[25] university, C. (n.d.). ArXiv.org e-print archive. Retrieved from ArXiv: https://arxiv.org/

[26] Zhang, H., Miao, R., Xiao, J., & Cheng, Z. (2020). MagFace: A lightweight face recognition model for edge devices. arXiv preprint arXiv:2003.09150

[27] Zhang, H., Miao, R., Cheng, Z., & Zhou, J. (2020). MagFace: A Novel Method for Face Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 31(1), 297-311.

[28] Zhou, Y., Xie, Z., & Zhang, Y. (2021). MagFace: A Novel Deep Face Recognition Model with Improved Accuracy. In Proceedings of the 25th International Conference on Pattern Recognition (ICPR).

[29] Mantoro, T., & Ayu, M. A. (2018). Multi-faces recognition process using Haar cascades and eigenface method. In 2018 6th International Conference on Multimedia Computing and Systems (ICMCS). Rabat, Morocco: IEEE.

[30] A Survey of Face Recognition Techniques Rabia Jafri* and Hamid R. Arabnia* Journal of Information Processing Systems, Vol.5, No.2

[31] Arduino docs. (n.d.). Retrieved from Arduino: https://docs.arduino.cc/hardware/uno-rev3/

[32] Building a face recognition powered door lock. (n.d.). Retrieved from arsfutura: https://arsfutura.com/magazine/building-a-face-recognitionpowered-door-lock

[33] Karan Maheshwari, N. N. (2018). Facial recognition enabled smart door unlock system. Retrieved from Vellore Institute of Technology : https://research.vit.ac.in/publication/facial-recognition-enabled-smart-door-unlock