AI TRESPASSER OVER BREACH MAIL

line 1: 1st G.UGENDAR RAJ
line 2: *Information Technology (of Affiliation)*
line 3: *Panimalar Engineering College (of Affiliation)*
line 4: Chennai, India
line 5: ugendarraj2002@gmail.com

line 1: 2nd SYAM SAI K G
line 2: *Information Technology (of Affiliation)*
line 3: *Panimalar Engineering College (of Affiliation)*
line 4: Chennai, India
line 5: ssk152002@gmail.com

line 1: 3rd S.YOGESHWARAN
line 2: *Information Technology (of Affiliation)*
line 3: *Panimalar Engineering College (of Affiliation)*
line 4: Chennai, India
line 5: email address or ORCID

***Abstract*—**The use of artificial intelligence (AI) technology is rapidly expanding and has already made a significant impact on various industries. However, with the increasing reliance on AI, there is a growing concern about the potential for AI systems to breach privacy laws and ethical standards. This paper presents a new AI trespasser system that uses breach mail technology to detect and prevent potential privacy violations by AI systems. The system operates by continuously monitoring AI systems for any signs of data breaches and sends out alerts to the relevant parties in the form of breach emails. These breach emails contain detailed information about the nature of the breach, its severity, and any necessary actions that need to be taken to resolve the issue. This system provides a proactive and effective solution to the problem of AI privacy breaches and will be valuable to organizations that rely on AI systems to manage sensitive information. Here the Authorized Facial features of the existing members have been captured and trained using OpenCV, and the generated model dataset will be deployed to detect the unauthorized trespasser which in turn triggers a breach mail if the detected facial features are not found in the generated/trained dataset model.
Keywords—Machine Learning, Trespasser Detection, Trigger Mail Alert, Artificial Intelligence, Data Science, Open CV, CNN, Dataset Training.

I. Introduction

Artificial Intelligence (AI) is a field of computer science that focuses on developing intelligent machines that can perform tasks that typically require human intelligence. These machines are designed to simulate human cognitive abilities, such as learning, reasoning, perception, and decision-making.

AI has the potential to greatly improve security by providing intelligent systems that can detect and respond to threats in real time. Some of the ways in which AI is being used to enhance security include:

1. Threat detection: AI systems can analyze vast amounts of data and identify patterns that may indicate the presence of a security threat. These systems can monitor network traffic, user behavior, and other indicators of potential threats and alert security personnel when unusual activity is detected.
2. Fraud prevention: AI can be used to detect fraudulent activity, such as credit card fraud or identity theft. By analyzing patterns in transaction data and user behavior, AI systems can identify suspicious activity and flag it for further investigation.
3. Cybersecurity: AI can help prevent cyber attacks by analyzing network traffic and identifying potential vulnerabilities. AI can also be used to detect malware and other malicious software and to respond to attacks in real time.
4. Physical security: AI can be used to monitor video feeds and other sensor data to detect intruders or suspicious activity. AI systems can also be used to control access to secure areas and to identify individuals who may pose a threat.

II. Ease of Use

The Effortless use of this AI trespasser over breach mail allows each and every citizen to be aware of the consequences behind it and also encourages each and every individual to contribute to the technical and cognitive abilities of a flourishing environment.

III. Related works

The relevant work is discussed in this section, along with the parts of earlier work that will be utilized. These studies concentrate on a small number of carefully chosen studies that contribute to the usage of facial recognition both with and without face masks and how it may be applied in various ways. The main objective of this part is to offer an overview of the most recent research that supports the usage of MFR, as well as a review of the associated studies. (Masked Facial Recognition). Additionally, it discusses some of the difficulties faced in creating facial recognition systems, their advantages, and the methods used to overcome them.

IV. Existing Features

Face Detection and Alignment: This involves developing algorithms that can accurately detect and align faces in images or videos. This research is important for various applications such as security systems, facial expression analysis, and human-computer interaction
Face recognition: This involves developing algorithms that can identify individuals from facial images or videos. Recent research has focused on improving the accuracy of face recognition algorithms, even under challenging conditions such as low-resolution images, occlusions, or changes in lighting.
Facial expression analysis: This involves developing algorithms that can recognize and interpret facial expressions, which is useful for applications such as emotion detection, human-robot interaction, and clinical psychology.
Privacy and security: With the growing use of facial recognition technology in various applications, there is increasing concern about privacy and security issues. Recent research has explored methods for improving the security of facial recognition systems, such as adversarial attacks, privacy-preserving techniques, and ethical considerations.

V. Proposed works

Phase-1-(Data set Collection and Training)

In order to construct a digital representation of a face, the process of extracting facial elements from an image or video frame, such as the eyes, nose, mouth, and chin, is known as facial extraction. In order to build a biometric template that can be compared against other people's faces in a database, facial recognition systems utilize facial extraction to determine the distinctive aspects of a person's face.
Face identification, alignment, and feature extraction are common processes in the facial extraction process. Based on certain qualities like color, texture, and form, an algorithm used for face detection scans a picture for areas that are likely to contain a face. The algorithm will make an effort to center and appropriately orient the face after it has been discovered. The eyes, nose, mouth, and chin are just a few examples of distinctive face characteristics that may be identified and isolated using feature extraction algorithms. In order to accurately and reliably identify people, face extraction is a vital stage in the facial recognition process. Facial recognition technology, especially in the context of widespread monitoring and the potential for abuse, is raising privacy and security concerns. The development of machine learning models, particularly those used for facial recognition, requires the acquisition of data sets and training of the models. To train a facial recognition model that can successfully identify faces across various demographics, lighting situations, and positions, it is essential to gather varied and representative data collection. With the right permission and with ethical issues in mind, data sets may be gathered from a wide range of sources, including public databases, social media sites, and private sources. To guarantee that the model can successfully learn from the data, data collection must be preprocessed and labeled once it has been gathered. Resizing photos, normalizing pixel values, and enhancing the data to promote variety are examples of preprocessing chores.
The below-shown Flowchart diagram depicts the flow of the research concept in the initial stage:

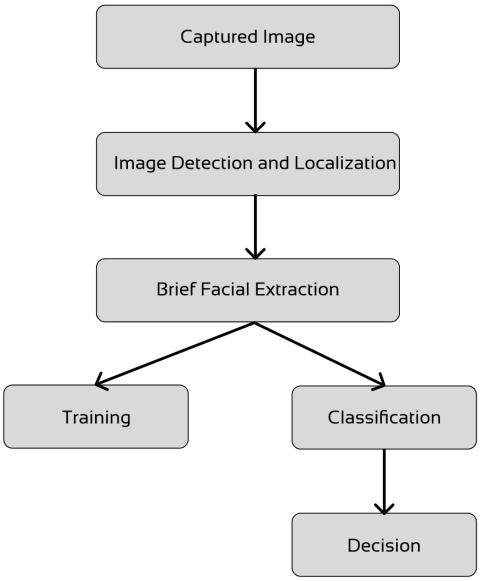

Fig. 1. Dataset is collected and trained to prepare Model.

Phase-2-(Dataset prediction and Trigger Mail)

As soon as the facial features are trained and stored in a dataset which is known as a Model, they once again being enhanced and zipped to make it lightweight and also to increase the speed of data processing which is then called a Generated Model, these mentioned activities are being carried out by **OpenCV,** and the data filtration is done using **CNN** the final generated model is used for Prediction, Processing, Accuracy, and Decision making.

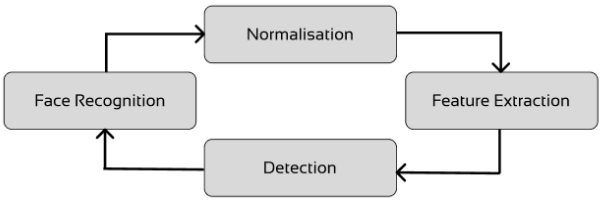

Fig. 2. Face Detection process

Facial recognition technology may be employed to recognise when a certain individual enters a given location and then instantly send an email to a specified recipient.

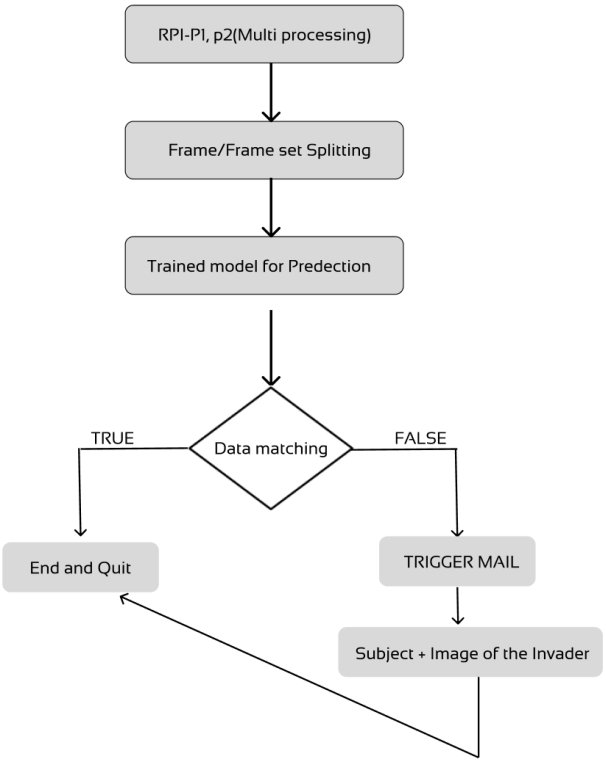

Fig. 3. Trigger Mail process for Unauthorized invader.

SAMPLE INPUT FOR TRAINING MODEL:-

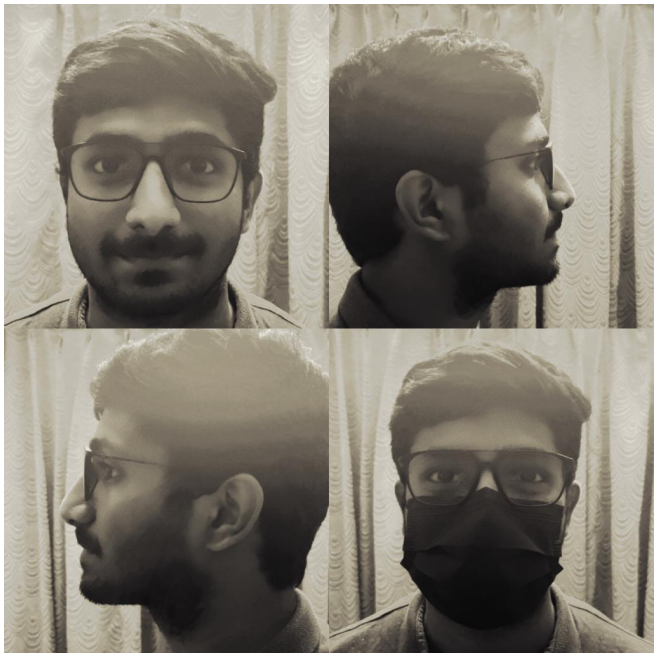

Fig. 4. Masked and unmasked training images

Fig. 5. Example of acceptable high-resolution images

Methodology, Tools, and Libraries Used

1. Data Collection and Preparation:

1.1. Face Alignment and Detection:-

Face Discovery is the process of locating the position and size of a face in an image or videotape frame. In face recognition, face discovery is the first step that enables the system to detect a face in an image or videotape frame, so it can be reused further. There are several approaches to face discovery, including template matching, point-grounded discovery, and machine literacy-grounded styles similar to Haar Falls and deep literacy-grounded styles similar to Convolutional Neural Networks(CNNs).

1.2. Features Measurements and Extraction:-

Feature Measurement and Extraction is a critical step in the face recognition process. The thing is to prize meaningful features from facial images that can be used to identify and compare individualities. They are the typical way involved in point dimension and birth Preprocessing The facial images are preprocessed to remove any noise and to homogenize the image quality. This step may include ways similar to cropping, resizing, and color normalization. Face discovery and alignment as bandied before, the face discovery and alignment step locates the position of the face in the image and aligns it in a standardized way. This step is critical for accurate point birth. point birth In this step, features are uprooted from the face using colorful ways. Some common ways include Original double Patterns(LBP) This fashion extracts texture features by comparing the intensity of pixels in an indirect neighborhood around each pixel. Histogram of acquainted slants(overeater) This

fashion excerpts shape features by assaying the slants of the image. Scale-steady point Transform(SIFT) This fashion excerpt features grounded on crucial points and their girding regions, which are steady to changes in scale and exposure. point selection and dimensionality reduction The uprooted features may be high-dimensional, which can be computationally precious and may affect overfitting. Thus, point selection and dimensionality reduction ways, similar to star element Analysis(PCA), are frequently used to reduce the dimensionality of the point vector. point matching In this step, the uprooted features are compared to those of known individualities in the database to determine a match.

2. Machine Learning Algorithm:

2.1. Decision process:-

Convolutional Neural Networks (CNNs): CNNs are a type of deep learning algorithm that can automatically learn and extract features from images. They have been very successful in face recognition applications, and are used in many commercial systems.
Support Vector Machines (SVMs): SVMs are a type of supervised learning algorithm that can be used for classification tasks. They work by finding the optimal hyperplane that separates different classes of data and is often used in face recognition for binary classification tasks (e.g., is this person in the database or not).
Principal Component Analysis (PCA): PCA is a dimensionality reduction technique that can be used to reduce the complexity of face images. It works by finding the principal components (i.e., the most important features) of the data, and projecting the data onto a lower-dimensional space.
Linear Discriminant Analysis (LDA): LDA is another dimensionality reduction technique that can be used in face recognition. It works by finding a projection that maximizes the separation between different classes of data.
Deep Metric Learning: This is a type of deep learning algorithm that learns a distance metric between pairs of images. It can be used to compare the similarity between different faces and is often used in face verification tasks (e.g., does this image match the identity of the person in the database?).

2.2. Error function:-

In machine learning, an error function (also known as a loss function or cost function) is a mathematical function that measures the difference between the predicted output of a machine learning algorithm and the actual output.

The purpose of the error function is to provide a quantitative measure of how well the algorithm is performing. The goal of the algorithm is to minimize the error function by adjusting the values of its parameters.

2.3. Generated Model Optimization:-

In face recognition, the generated model optimization refers to the process of fine-tuning the pre-trained deep-learning models to improve their performance on the task of recognizing faces. The optimization process involves adjusting the model's weights and biases through a process called backpropagation, which minimizes the error between the predicted and actual output. The optimization process is usually done by feeding the pre-trained model with a large dataset of faces to learn from, such as the VGGFace, MS-Celeb-1M, or CASIA-Webface datasets.

To further improve the accuracy of the model, several techniques can be used, such as data augmentation, which involves applying random transformations to the input images to create new training samples, regularization, which helps prevent overfitting by adding a penalty term to the loss function and transfer learning, which involves using pre-trained models to learn from new data.

Overall, the generated model optimization in face recognition is a crucial step that helps improve the accuracy and robustness of the models, allowing them to perform better in real-world scenarios by performing the following steps:

1. Artificial Intelligence Algorithm:

    1. Learning and Discovering.
    2. Adding intelligence to the Automation.
    3. Self-learning By - (I) Structure
        (II) Regularities

CNN:-

CNN stands for Convolutional Neural Network, which is a type of deep learning algorithm commonly used in computer vision tasks such as image recognition, object detection, and face recognition.

In the terrain of face recognition, CNNs are used to learn the features of a face by assaying its pixels. A CNN generally consists of several layers of convolutional, pooling, and fully connected layers that exercise the input image and prize the applicable features for face recognition. During the training process, a CNN is trained on a large dataset of faces, which enables it to learn the unique features of different faces analogous to the shape of the eyes, nose, mouth, and other facial features. Once trained, the CNN can recognize faces in new images by comparing the learned features with the features in the input image.

OpenCV:-

OpenCV(Open Source Computer Vision) is an open-source library of programming functions that are extensively used in computer vision and image processing tasks. It includes colorful algorithms and tools for image and videotape processing, like point discovery, object recognition, and face recognition. In the environment of

face recognition, OpenCV provides several pre-trained face discovery models that can be used to descry faces in images or videotape aqueducts. Once the faces are detected, OpenCV can be used to prize the features of the detected faces and also compares them with a database of known faces to identify or corroborate individualities. OpenCV also provides several pre-trained models for facial recognition, similar to Eigenfaces, Fisherfaces, and Original Double Patterns Histograms(LBPH). These models use machine literacy algorithms to fete faces grounded on the uprooted features, and they can be trained on a dataset of faces to ease their delicacy. Overall, OpenCV provides an essential set of tools and algorithms for face recognition, which can be used to develop robust and accurate face recognition systems for a wide range of operations.

Conclusion

In conclusion, our study has shown that Trespasser can be easily identified and take appropriate action over them. These results have important implications for the future development of AI technology.

Overall, our research has contributed to the growing body of knowledge in the field of AI. By Triggering the mail, we have advanced our Exploration of the usage of AI for Unauthorized Trespassers.

References

The below-mentioned References are used as a base paper and reference website to explore and acquire prerequisite knowledge for our research paper.

[1] Ullah, Naeem, et al. ”A novel DeepMaskNet model for face mask detection and masked facial recognition.” Journal of King Saud University- Computer and Information Sciences (2022).

[2] Anwar, Aqeel, and Arijit Raychowdhury. ”Masked face recognition for secure authentication.” arXiv preprint arXiv:2008.11104 (2020).

[3] Mandal, Bishwas, Adaeze Nwokeukwu, and Yihong Theis. ”Masked face recognition using ResNet-50.” arXiv preprint arXiv:2104.08997 (2021).

[4] Mundial, Imran Qayyum, et al. ”Towards facial recognition problem in COVID-19 pandemic.” 2020 4th International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM). IEEE, 2020.

[5] Golwalkar, Rucha, and Ninad Mehendale. ”Masked-face recognition using deep metric learning and FaceMaskNet-21.” Applied Intelligence (2022): 1-12.

[6] Wang, Zhongyuan, et al. ”Masked face recognition dataset and application.” arXiv preprint arXiv:2003.09093 (2020).

[7] Dlib, https://github.com/davisking/dlib.

[8] OpenCV, https://github.com/opencv/opencv .

[9] C Qinghua. Analysis of face recognition technology based on deep learning [J]. Computer products and circulation, 2020(05): 136.

[10] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, “Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques, and challenges,” IEEE Access, pp. 1–1, 2020.

[11] S.Li and W. Deng, “Deep facial expression recognition: A survey,” IEEE Transactions on Affective Computing, pp. 1–1, 2020.

[12] A. Fathima and K. Vaidehi, “Review on facial expression recognition system using machine learning techniques,” in Advances in Decision Sciences, Image Processing, Security and Computer Vision, pp. 608–618, Springer, 2020.

[13] R. Ravi, S. Yadhukrishna, et al., “A face expression recognition using cnn & lbp,” in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 684–689, IEEE, 2020.

[14] A. L. A. Ramos, B. G. Dadiz, and A. B. G. Santos, “Classifying emotion based on facial expression analysis using Gabor filter: A basis for adaptive effective teaching strategy,” in Computational Science and Technology, pp. 469–479, Springer, 2020.

[15] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, “Machine learning models for secure data analytics: A taxonomy and threat model,” Computer Communications, vol. 153, pp. 406 – 440, 2020.

[16] E. Pranav, S. Kamal, C. S. Chandran, and M. Supriya, “Facial emotion recognition using deep convolutional neural network,” in 2020 6thInternational Conference on Advanced Computing and Communication Systems (ICACCS), pp. 317–320, IEEE, 2020.

[17]Harrisburg University. Research brief on facial recognition software. https://harrisburgu.edu/hu-facial-recognition-software-identifies potential-criminals/, 2020.

[18] Dang, F. Liu, J. Stehouwer, X. Liu, and A. K. Jain, “On the detection of digital face manipulation,” in Proc. IEEE/CVF Conf. Comput. Vis.Pattern Recognit., 2020, pp. 5781–5790.

[19] L. Li et al., “Face x-ray for more general face forgery detection,” in Proc.IEEE/CVF Conf. Comput. Vis. Pattern Recognit., 2020, pp. 5001–5010.