# Framework for Face Recognition in CCTV Based on Internet of Things (IoT)

**SOURASIS CHATTOPADHYAY[1],MOSIUR RAHAMAN[1],CHAYADI OKTOMY NOTO SUSANTO[2],NIZIRWAN ANWAR[3],AUGUSTA AN-HAU CHEN[4]**

[1]Department of Computer Science and Information Engineering, Asia University, Taiwan
[2]Universitas Muhammadiyah Yogyakarta, Indonesia
[3]Esa Unggul University of Jakarta, Indonesia
[3]National Chung Hsing University, Taiwan.

**ABSTRACT** For public safety purposes, large networks of cameras are being utilized more regularly in public places like offices, residential complexes, college campuses, airports, train stations, and shopping malls. These systems are limited over time by factors like weariness and monitoring because they mainly rely on human observers on the other side the system needed for huge data storage and management device. To overcome this limitation, "intelligent" solutions are required, which may highlight the crucial information and exclude common circumstances that don't endanger safety. We can limit access to our facilities and protect our assets by using surveillance systems. There are face detection and recognition capable surveillance systems on the market now that can identify faces by comparing them to databases of known faces from video frames taken using IP cameras. However, the widespread use of those devices is being hampered by their greater costs and poor accuracy.

**KEYWORDS** Face Recognition; IoT; CCTV

## I. INTRODUCTION

Robberies are increasingly frequent in our daily lives. Commercially available security systems with CCD cameras can fend it off. These devices use a significant amount of electricity because they are always powered and continuously record video [1], [2]. Remote surveillance is required in the majority of places. These systems record video, send it via the internet to a server, and then send it from the server to a client. Our daily lives are becoming more and more regular with robberies. It can be repelled by commercially available security systems using CCD cameras [3], [4].Due to their constant power and ongoing video recording, these devices consume a lot of electricity. The majority of locations require remote observation. These systems record video, upload it to a server through the internet, and then distribute the server's content to clients. The video monitoring system and the access granting system are the two components of any smart security system that provide perfect security. ENVMT technology for video surveillance and face recognition for access control make up the suggested solution [5], [6]. In order to achieve the appropriate security, today's institutions need a number of individuals who have received specialized training. These employees make mistakes that could lower the security level because they are fallible human beings.

As a potential solution to the aforementioned problem, a face recognition security system has been proposed since it can capable to detect any unwanted intruders in highly secured areas and optimize human error as much as possible. This system is consisting of hardware and software part. The hardware part consists of a camera, while the software part consists of face-detection and face-recognition algorithms software [7], [8]. Once someone enters the restricted area, a sequence of pictures are taken by the camera and sent to the software system to be examined and cross-referenced with an existing database of reliable individuals to check the concerned person is allowed or not. And a notification will send of to the admin if the user is not recognized in the restricted zone. An intelligent surveillance system like the one in Figure 1 can aid in an inquiry.


FIGURE 1: Face detection through CCTV surveillance for home safety

The system can identify and classify visitors as members of the family, friends, or other close relatives, as well as service providers and Strangers, and it actively monitors visitor movement to spot any anomalies [9].

## II. LITERATURE REVIEW

One of the security technology markets with the quickest growth is CCTV-based video monitoring. However, the current video surveillance systems are still unable to be used to stop crime [10]–[12]. Large networks of cameras are being used more frequently in public locations for public safety objectives, such as offices, residential buildings, college campuses, airports, train stations, and retail centers. Since these systems rely heavily on human observers, they are constrained over extended periods of time by things like fatigue and monitoring [13]–[15].

The research addresses a number of issues with facial identification, including lighting changes, low-resolution cameras, occlusion from things like eyeglasses, hairstyles, and makeup [16]–[18].

This type of solution allows for discrete monitoring based on the system's correctness. The monitoring individual does not have to constantly watch the recorded video [19]–[21]. The system aims to improve security, adaptability, and efficiency while overcoming the shortcomings of previous surveillance systems. The primary goal of this study is to employ a PIR sensor located on the front door to automatically identify people and turn on the CCTV, which should be on the entire time guests are inside the home [22]–[24]. The system identifies and categorizes visitors as members of the family, friends, or other close relatives, as well as service providers and Unknown, and it continuously monitors visitor movement to spot any abnormalities [25].

We have observed a considerable and consistent increase in the usage of closed-circuit television (CCTV) surveillance cameras in recent years to deter crimes in public areas. Nearly whole cities can now be watched thanks to the expanding installation of sophisticated CCTV technology; however, the main benefit is simply evidentiary [26], [27]. An alarm or warning system for ongoing (or impending) accidents and crimes would be expected, as prompt action can mean the difference between life and death. Personnel watching live footage is supposed to monitor and spot such situations. But as the average number of CCTVs per unit keeps increasing, this strategy is becoming more and more unworkable. Both the automated smart CCTV monitoring systems and the current human-run CCTV monitoring system are only partially capable of making choices and initiating actions. The standard passive video surveillance system is inefficient because there are too many cameras for human operators to keep track of. The objective of visual surveillance is to carry out the surveillance task as automatically as feasible in addition to installing cameras in the two locations where humans have eyes [28], [29].

The automated smart CCTV monitoring systems that are now in place are not entirely capable of initiating actions. More on such kind of surveillance system is inefficient because there are too many complexities to operate and track of for human operators. Main objective of visual surveillance is to carry out the surveillance task as automatically as possible in addition to installing cameras in different locations. In addition to placing cameras in the 2 places of human eyes, the goal of visual surveillance is to accomplish, as automatically as possible, the surveillance task.

The proposed system takes into account the privacy concerns, cost-effectiveness, and effective alarm system that are part of the current security system trend. The goal of surveillance in dynamic situations is to identify, locate, and track specific items from image sequences as well as, more broadly, to comprehend the actions of objects. The goal is to create a sophisticated visual surveillance system to take the place of the current passive video surveillance system.

Physical security measures, such as hiring security personnel, setting up CCTV, and limiting public access, are already standard practice. Computer systems with archival storage media must be kept up to date, especially those that contain sensitive data that needs to be kept in a locked location. individuals can enter through other openings. When things are peaceful and the owner or security personnel are not around, theft and other crimes in the business commonly happen. The security system is still highly vulnerable as a result. The primary objective of this study is to assist industries in monitoring and controlling the security panel from their control panel and mobile. A user-friendly interface on mobile devices, such as smartphones, allows access to and control of the system at any time and from any location. The study of behavior, exercise, or information development and how it can be used to influence, monitor, regulate, or secure is known as supervision [30]–[32]. This system may be used to carry out tasks like alarm activation and door lock control in addition to monitoring and controlling. A warning tone is produced by the system in accordance with the command message. The panel will lock when the system receives a command from the user to lock the door [33]–[35].

## III. METHODOLOGY

As previously mentioned, this research span can be suitable for several disciplines. In this research, we established our proposed optimized security monitoring in the residential area. This proposed system consists of high-definition digital video recorder embedded with an infrared sensor for motion detection, a signal processing unit, a microcontroller, a data management come storage system, and a dynamic user interface to update the system and monitor the region of interest.

## IV. WORKING PROCESS OF THE PROPOSED SYSTEM

The working flow of the proposed methodology is shown in figure 2. At the very beginning state, the digital video recorder will be placed in a safe and secure position at the entrance of the residential building. This camera will be in a standby position until any motion is detected in the region of interest. If the motion is detected by the sensor features then,

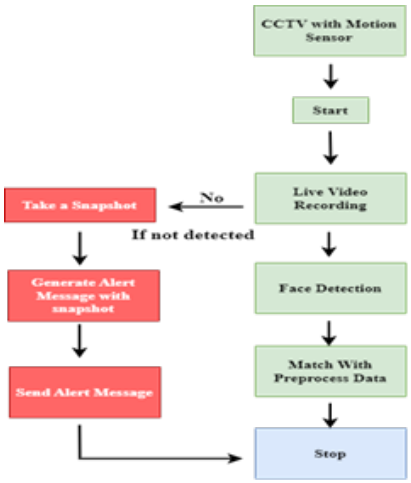


FIGURE 2: Working flow of the proposed methodology

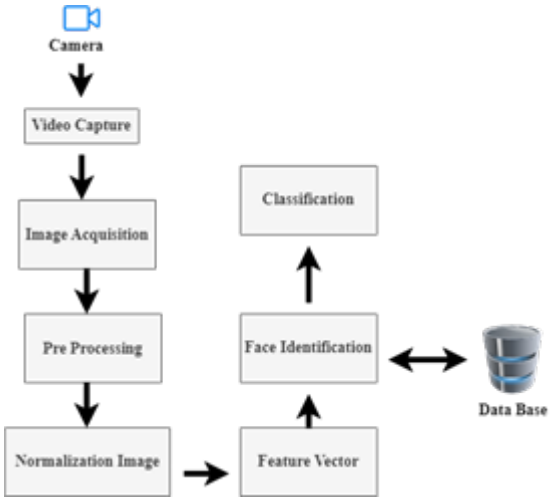


FIGURE 3: Facial recognition working flow

the video recording will be immodestly enabled. In the next step, the system will detect the face of the human. After that recognizing the detected face and similarity checked with the existing database. If the person's face is checked as similar to the database, then the camera will again go to a stand-by position until new motion is detected in the region of interest. On the other side, if the person's face is not matched with the database, then the system will take a snapshot of the concerned person's cropped face image and send this picture by generating a notification email to the user. As the advantage of our proposed system,

- Our system is not required for any kind of huge memory device.
- Not requiring extra security professionals to monitor the live footage of the recorded video.
- The chance of human error becomes less.
- Overall security cost is becoming more compressed

## V. FACE DETECTION, RECOGNITION, AND CLASSIFICATION

Facial recognition is a kind of pattern recognition technique, which used largely in image identification techniques. In our proposed possible scenario, it can be explained as categorizing or classifying a face as the user of the residential building, or Unknown after matching it with individuals who have been saved in a database as known people [36]. The main working flow is explained in figure 3.

## VI. IMAGE ACQUISITION

Image acquisition is the preliminary process of the facial recognition model. Within this module, the user configures the face image and inputs the facial data for the face recognition system. Most importantly the real-time input stream is used to capture the face image [37]. Which makes the entire system more robust.

## VII. IMAGE PRE-PROCESSING AND NORMALIZATION

In this module, the images are normalized to enhance machine recognition. For example, image size normalization, image contrast and brightness, nose pixel removal, background removal, translation and rotation normalization, and illumination normalization are all pre-processing procedures. In one sentence, this step is the most essential module for face detection and recognition.

## VIII. FACE IDENTIFICATION AND FEATURE VECTOR

According to our data demand, we only required the frontal faces as the input image. These images have been scaled and normalized. It is very crucial to identify and extract the particular facial region. Because we only require the frontal faces from the input images that have been scaled normally in our system. It is crucial to identify and extract the feature vector of the facial region from an image in order to minimize the computation required for feature extraction. For face identification, we are utilizing the Haar cascade algorithm [38].This harr cascade is specifically used for the image as well as face identification [39]. In figure 4 shows how Haar feature is utilized to identify that facial region.

## IX. CLASSIFICATION

Classification is the final step of face identification. In this step generally, data is classified by three Category as known, unknow and not recognized. To fulfill this criterion, here we implement local binary pattern histogram with Haar cascades algorithm [41]. This local binary pattern histogram is a most popular face recognition model [42]. With the help of this algorithm, we can recognized the side face and front face of the person. As the main fundamental feature of this algorithm is to extract the texture and labeling each image pixels by thresholding the neighborhood of each pixel and evaluate the result in binary number [41]. In figure 5 we shown the local binary pattern histogram in our proposed model.

FIGURE 4: Face Identification through HAAR cascade model [40]

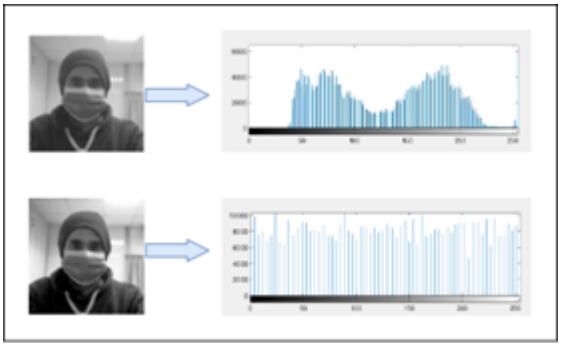

FIGURE 5: Local Binary Pattern Histogram in proposed model [43]

## X. PRE-TRAINED DATABASE

To train our machine we prepared 67 people's front face date set. And every individual people we create 26 different face images with different conditions such as low light and wearing a mask.

## XI. NOTIFICATION GENERATION

According to our model, we categorize a person as a known, or unknown after recognizing their face with our pre-trained database. If any unknown face is detected, then an alert notification will be transmitted to the user's mobile device as an email.

## XII. RESULTS

Our proposed model was simulated and implemented on MATLAB R2021b, and the system configuration is Intel i5 processor, 16 GB RAM, 8 GB graphics card. According to our requirement, we pre-trained our machine by using Multi-Task Cascaded Convolutional Neural Networks or MTCNN [44]. Our dataset is consisting of a total of 67 people and with the total number of front-face pictures are 1742. According to our training model, we are able to reach up to 73.41%

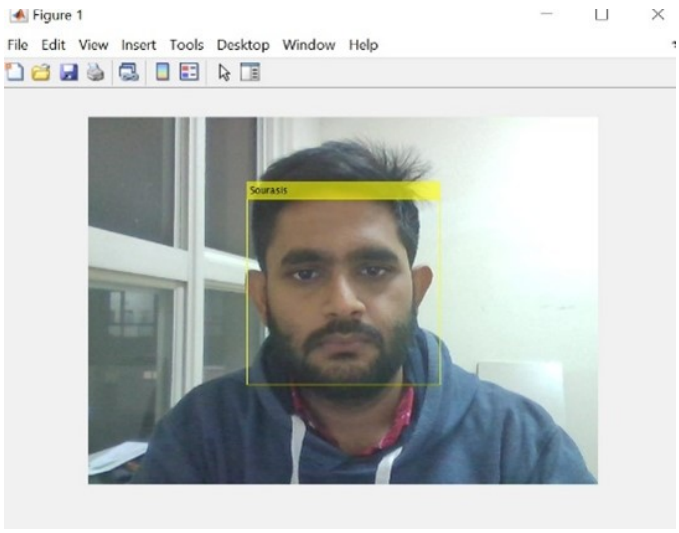


FIGURE 6: Real time identification of matching face

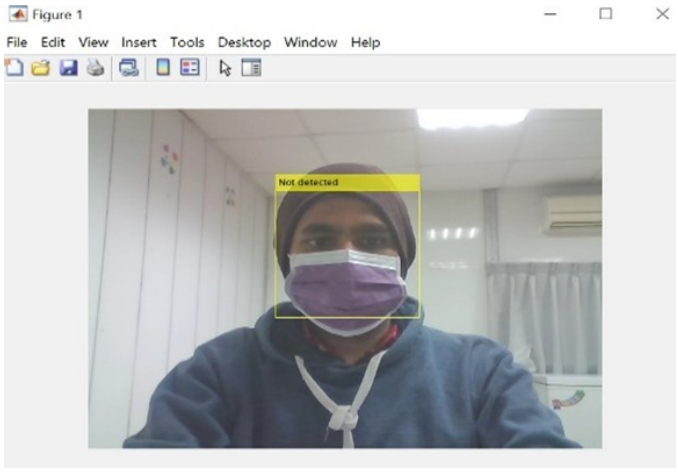


FIGURE 7: Real time identification of not matching face

accuracy. More on our proposed system took 309.14 second with 0.241 second for testing time. Most importantly our dataset is prepared with almost every kind of condition such as with facial cover, in low light, and so on. Real time implementation of our proposed model shown in figure 6. In this image shows that the concern person is known to the dataset. On the other side in figure 7 shows that the same person's face can't recognized due to facial obstruction. In figure 8 shows that the concerned person is unknown. At the same time, the same detected person snapshot is notified to the user of the system via email, which is shown in figure number 8.

## XIII. CONCLUSION

According to our proposed system we successfully overcome with our objective. As result of our proposed model, we optimized the huge video data storage problem. More on in this paper we discussed the advantages of the smart security system and solve the possible issues in conventional security

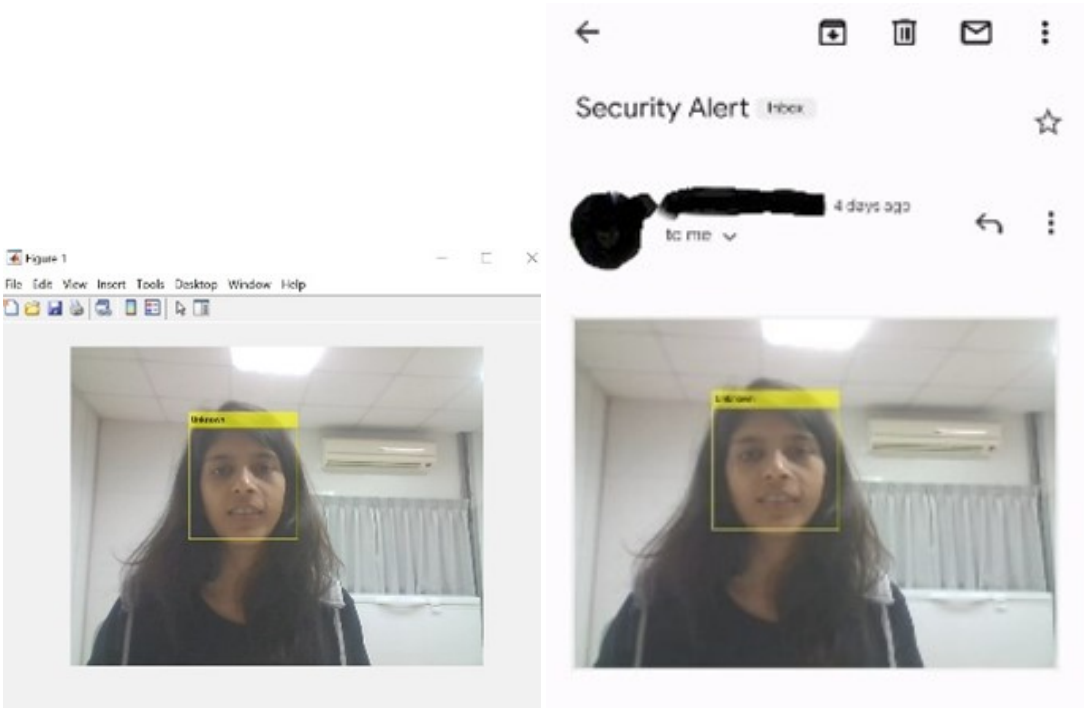


FIGURE 8: Real time identification of unknown face

system. From this study we conclude that our entire model is well performed with 73.41% of accuracy. As future scope, this proposed model's performance can be improved by considering all kind of physical factors such like video detection speed, more accuracy in data training model and so on.

## REFERENCES


[1] J. J. Lahoz-Monfort and M. J. Magrath, "A comprehensive overview of technologies for species and habitat monitoring and conservation," BioScience, vol. 71, no. 10, pp. 1038–1062, 2021.

[2] R. K. S. Rajput, D. Goyal, A. Pant, G. Sharma, V. Arya, and M. K. Rafsanjani, "Cloud data centre energy utilization estimation: Simulation and modelling with idr," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–16, 2022.

[3] S. R. Zeebaree and H. Rajab, "Design and implement a proposed multi-sources to multi-destinations broadcasting video-signals," in 2019 4th Scientific International Conference Najaf (SICN). IEEE, 2019, pp. 103–108.

[4] K. Pathoee, D. Rawat, A. Mishra, V. Arya, M. K. Rafsanjani, and A. K. Gupta, "A cloud-based predictive model for the detection of breast cancer," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–12, 2022.

[5] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," Sensors, vol. 20, no. 2, p. 342, 2020.

[6] M. Kaur and et al., "Secure and energy efficient-based e-health care framework for green internet of things," IEEE Transactions on Green Communications and Networking, vol. 5, no. 3, pp. 1223–1231, 2021.

[7] M. Owayjan, A. Dergham, G. Haber, N. Fakih, A. Hamoush, and E. Abdo, "Face recognition security system," in New trends in networking, computing, E-learning, systems sciences, and engineering. Springer, 2015, pp. 343–348.

[8] L. Zou and et al., "A novel coverless information hiding method based on the average pixel value of the sub-images," Multimedia tools and applications, vol. 78, no. 7, pp. 7965–7980, 2019.

[9] R. Vijaya Saraswathi, D. Vasundhara, R. Vasavi, G. Laxmi Deepthi, and K. Jaya Jones, "Face detection and comparison using deep learning," in Proceedings of Second International Conference on Advances in Computer Engineering and Communication Systems. Springer, 2022, pp. 499–512.

[10] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," IEEE Communications Surveys & Tutorials, 2022.

[11] A. Singh and et al., "Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 18, no. 1, pp. 1–43, 2022.

[12] A. Tewari and et al., "A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices," International Journal of Advanced Intelligence Paradigms, vol. 9, no. 2-3, pp. 111–121, 2017.

[13] S. H. Al Zaabi and R. Zamri, "Managing security threats through touchless security technologies: An overview of the integration of facial recognition technology in the uae oil and gas industry," Sustainability, vol. 14, no. 22, p. 14915, 2022.

[14] A. Gaurav, V. Arya, and D. Santaniello, "Analysis of machine learning based ddos attack detection techniques in software defined network," Cyber Security Insights Magazine (CSIM), vol. 1, no. 1, pp. 1–6, 2022.

[15] A. Tewari and et al., "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20–34, 2020.

[16] V. Fegade, A. Chodankar, A. Bhingle, and S. Mhatre, "Residential security system based on facial recognition," in 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2022, pp. 01–09.

[17] N. Kumar and et al., "A novel framework for risk assessment and resilience of critical infrastructure towards climate change," Technological Forecasting and Social Change, vol. 165, p. 120532, 2021.

[18] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," Multimedia Tools and Applications, vol. 77, no. 7, pp. 9203–9208, 2018.

[19] D. Mitra, S. Gupta, and A. Goyal, "Security system using open cv based facial recognition," in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). IEEE, 2022, pp. 371–374.

[20] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.

[21] M. Hammad and et al., "Myocardial infarction detection based on deep neural network on imbalanced data," Multimedia Systems, vol. 28, no. 4, pp. 1373–1385, 2022.

[22] M. R. Dhobale, R. Y. Biradar, R. R. Pawar, and S. A. Awatade, "Smart home security system using iot, face recognition and raspberry pi," International Journal of Computer Applications, vol. 975, p. 8887, 2020.

[23] M. Casillo and et al., "Context aware recommender systems: A novel approach based on matrix factorization and contextual bias," Electronics, vol. 11, no. 7, p. 1003, 2022.

[24] A. Dahiya and et al., "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," Future Generation Computer Systems, vol. 117, pp. 193–204, 2021.

[25] R. K. Verma, P. Singh, C. R. Panigrahi, and B. Pati, "Iss: intelligent security system using facial recognition," in Progress in Advanced Computing and Intelligent Engineering. Springer, 2021, pp. 96–101.

[26] A. J. Majumder and J. A. Izaguirre, "A smart iot security system for smart-home using motion detection and facial recognition," in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE, 2020, pp. 1065–1071.

[27] P. Do and et al., "Building a knowledge graph by using cross-lingual transfer method and distributed minie algorithm on apache spark," Neural Computing and Applications, pp. 1–17, 2020.

[28] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," Ai & Society, vol. 37, no. 1, pp. 167–175, 2022.

[29] B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed denial of service attack in iot networks using supervised learning classifiers," Computers & Electrical Engineering, vol. 98, p. 107726, 2022.

[30] S. Shri Bharathi, T. Aadithya Kiran, N. Dileep Kanth, B. Raghu Ram Reddy, and A. Geetha, "A hybrid approach to facial recognition for online shopping using pca and haar cascade," in International Conference on Image Processing and Capsule Networks. Springer, 2022, pp. 284–295.

[31] R. Jiao and et al., "Adaptive feature selection and construction for day-ahead load forecasting use deep learning method," IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4019–4029, 2021.

[32] B. B. Gupta, S. Gupta, and P. Chaudhary, "Enhancing the browser-side context-aware sanitization of suspicious html5 code for halting the dom-based xss vulnerabilities in cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 1, pp. 1–31, 2017.

[33] Y. Sundari, G. Laxminarayana, and G. V. Laxmi, "Anti-theft mechanism through face recognition using fpga," International Journal of Advancements in Research & Technology, vol. 1, no. 6, pp. 46–49, 2012.

[34] B. B. Gupta, A. Gaurav, P. K. Panigrahi, and V. Arya, "Analysis of artificial intelligence-based technologies and approaches on sustainable entrepreneurship," Technological Forecasting and Social Change, vol. 186, p. 122152, 2023.

[35] S. Kumar, S. Kumar, N. Ranjan, S. Tiwari, T. R. Kumar, D. Goyal, G. Sharma, V. Arya, and M. K. Rafsanjani, "Digital watermarking-based cryptosystem for cloud resource provisioning," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–20, 2022.

[36] D. Yang, A. Alsadoon, P. C. Prasad, A. K. Singh, and A. Elchouemi, "An emotion recognition model based on facial recognition in virtual learning environment," Procedia Computer Science, vol. 125, pp. 2–10, 2018.

[37] S. Khan, M. H. Javed, E. Ahmed, S. A. Shah, and S. U. Ali, "Facial recognition using convolutional neural networks and implementation on smart glasses," in 2019 International Conference on Information Science and Communication Technology (ICISCT). IEEE, 2019, pp. 1–6.

[38] M. H. Robin, M. M. U. Rahman, A. M. Taief, and Q. N. Eity, "Improvement of face and eye detection performance by using multi-task cascaded convolutional networks," in 2020 IEEE Region 10 Symposium (TENSYMP). IEEE, 2020, pp. 977–980.

[39] P. Kumar, N. Manzoor, and C. Dhiman, "A deep cascaded multi-task face recognition framework," in 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, 2021, pp. 569–573.

[40] J. W. D'Souza, S. Jothi, and A. Chandrasekar, "Automated attendance marking and management system by facial recognition using histogram," in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE, 2019, pp. 66–69.

[41] G. S. Nagpal, G. Singh, J. Singh, and N. Yadav, "Facial detection and recognition using opencv on raspberry pi zero," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). IEEE, 2018, pp. 945–950.

[42] P. Bhatia, S. Rajput, S. Pathak, and S. Prasad, "Iot based facial recognition system for home security using lbph algorithm," in 2018 3rd International Conference on Inventive Computation Technologies (ICICT). IEEE, 2018, pp. 191–193.

[43] G. Srivastav and R. Singh, "Facial recognition based workplace security system using lbph algorithm," in AIP Conference Proceedings, vol. 2555, no. 1. AIP Publishing LLC, 2022, p. 040008.

[44] N. C. Basjaruddin, E. Rakhman, Y. Sudarsa, M. B. Z. Asyikin, and S. Permana, "Attendance system with face recognition, body temperature, and use of mask using multi-task cascaded convolutional neural network (mtcnn) method," Green Intelligent Systems and Applications, vol. 2, no. 2, pp. 71–83, 2022.