Quest Journals
Journal of Software Engineering and Simulation
Volume 12 ~ Issue 5 (May 2026) pp: 01-09
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Airport Security Monitoring at Boarding Gate Using Smart FaceSurveillance Camera

Abstract
The level of airport security has been questioned in recent years as there have been various incidents of unexpected events occurred, such as a hijacking and the use of fake passports and documents. This has raised concerns about the efficacy of the airport security systems in place. It has also highlighted the need for more advanced biometric systems, such as facial recognition, to be employed in order to prevent such incidents from occurring. The purpose of this project is to develop smart IOT based surveillance systems that can be implemented at Airport. For this study, the Smart Face Surveillance Camera (SFSC) system has been designed and developed to identify the identity of passengers and cabin crew in real time, as well as the vaccination status of the passengers before boarding. A total of 20 volunteers were randomly selected for this study. The process began with the volunteer taking a picture using the Pi camera. The picture was then saved in the data. Upon obtaining the data, it will be transferred to the Raspberry Pi for the purpose of interpreting it by code. Data will be read according to an algorithm developed on a Raspberry Pi. If the data match with the algorithm that has been set, the output will be displayed directly on the Liquid Crystal Display (LCD) screen. The obtained data was then validated using confusion matrix and it shows 93% accuracy. This result demonstrates the efficacy of the algorithm and the programming of the Raspberry Pi in correctly interpreting the data, confirming the viability of the project.

Keywords: *Facial recognition; machine learning; confusion matrix; raspberry Pi; biometric*

*Received 02 May., 2026; **R**evised 10 May., 2026; **A**ccepted 12 May., 2026 © The author(s) 2026.*
P**ublished with open access at **www.questjournals.org

I. Introduction

In the aviation industry, hijacking refers to the illegal seizure of an aircraft by a passenger or a group of passengers. While hijackings have occurred in the past, authorities often struggle to identify suspected individuals due to limitations in airport infrastructure and resources. Outdated security systems, the lack of facial recognition software, and insufficient staffing contribute to inaccurate identification of potential hijackers (Kar et al., 2012; Bhowmik et al., 2011). The current reliance on closed-circuit television (CCTV) monitoring for verification purposes is time-consuming and may not provide clear images for identification (Bhowmik et al., 2011).

The ease with which suspected passengers can change their appearance at the boarding gate in a short period of time poses a significant challenge for authorities, as they can evade detection and board the aircraft without observation (Kar et al., 2012). This situation creates a serious security threat to the flight and its passengers. The Malaysia Airlines Flight MH370 incident in 2014 serves as an example where two passengers boarded the aircraft using fake passports and documents, potentially indicating a hijacking attempt. However, due to the unclear images captured by the camera, determining the identity of the suspected passengers was impossible, increasing the risk of hijacking and endangering the lives of the three hundred people on board (Kar et al., 2012).

To enhance airport security, the implementation of face recognition technology at the boarding gate is crucial. This technology enables quick and accurate identification of passengers, reducing the need for manual document checks and expediting the boarding process (Bhowmik et al., 2011). Face recognition technology, which combines computer vision, pattern recognition, and machine learning, allows for the mapping of facial features and the comparison of captured data with a database of known faces (Almudhahka et al., 2016). Its application has attracted the attention of researchers in various fields, including defense, automated surveillance, forensic applications, and multimedia applications (Almudhahka et al., 2016; Deepa & Chamundeeswari, 2016; Hassaballah & Aly, 2015; Sajid et al., 2014; Wu & Radke, 2011). By utilizing face recognition technology, potential terrorists can be identified at airports and border control points, providing a more efficient and secure means of identifying individuals (Uiboupin et al., 2016).

Face recognition technology evaluates features such as contours and facial expressions by comparing the captured face image with known faces in a database (Bhowmik et al., 2011). It looks for similarities in facial features, including the shape of the eyes, nose, and mouth, as well as facial expressions like smiles or frowns. Compared to other forms of verification such as biometrics and physiology-based systems, face recognition is non-invasive and user-friendly (Bhowmik et al., 2011). Real-time face recognition technology is accessible from various locations through wireless internet and smartphones, providing convenience and accessibility (Bhowmik et al., 2011). Additionally, face recognition enables users to access services and resources remotely, making it highly convenient. The technology allows for long-distance data collection without the need for verbal communication, which is particularly advantageous for security and monitoring purposes. Furthermore, face recognition technology provides quick and accurate authentication, facilitating more efficient access to secured sites and services (Bhowmik et al., 2011).

In conclusion, the integration of face recognition technology at the boarding gate is essential for enhancing airport security in the aviation industry. By addressing the limitations of existing systems, airports can strengthen their security protocols, minimize the risk of hijacking incidents, and ensure the safety of passengers.

II. Literature review

The history of face recognition dates back to the 1960s when semi-automated systems were developed to relocate facial features such as eyes, ears, noses, and mouths (Kar et al., 2012). Marks were placed on photographs, and reference points were computed by measuring distances and ratios between these marks, which were then compared with reference data. In the early 1970s, Goldstein, Harmon, and Lesk introduced a system that utilized more than 20 subjective markers, including hair color and lip thickness (Goldstein et al., 1971). However, this system faced challenges in proving accuracy due to the subjective nature of the measurements taken manually.

Fischler and Elschlager took a different approach in 1973 by measuring different facial components and mapping them onto a global template. However, they found that these features alone were insufficient to represent an adult face accurately (Fischler & Elschlager, 1973; Kar et al., 2012).

One of the primary challenges faced by face detection and recognition systems is dealing with uncontrollable conditions such as pose variation, occlusion, and facial expressions (Bah & Ming, 2020; Bhowmik et al., 2011; Olszewska, 2016).

Pose variation refers to the changes in the appearance of a face caused by movements of the head, including rotation angles such as roll, pitch, and yaw, as well as different camera viewpoints (Kar et al., 2012). To address this challenge, researchers have proposed various techniques. For example, Bhangale et al. (2018) introduced a robust pose-invariant face recognition method using Dual Cross Pattern (DCP) and Support Vector Machine (SVM) to handle pose variations. Hussien (2016) simplified the issues of shift and rotation using complex wavelet transform (CWT) and Fisherface.

By overcoming these challenges, face recognition systems can achieve more accurate and reliable results, even in the presence of pose variations and other uncontrollable factors. These advancements in pose-invariant recognition techniques contribute to the overall improvement of face recognition technology's effectiveness in enhancing airport security and identifying potential threats

Figure. 1 : Example of Pose Variation

Occlusion - The diversity in the intra-subject face's images could also be due the presence of components such as cap (Figure. 2a) and spectacles (Figure. 2b) (Du & Ward, 2006).

Figure. 2 : Example of Occlusion by wearing (a) cap and (b)spectacles

Facial expression – Facial expression changes are based on the person's emotional states (Prikler, 2016) which are displayed in Figure. 3 such as anger, happiness and sad.

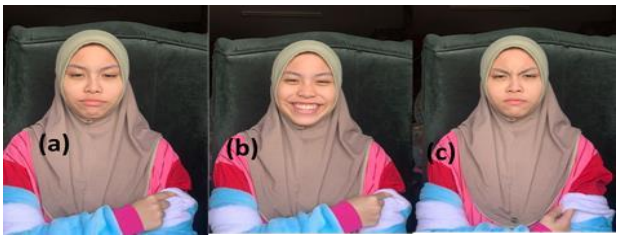

Figure. 3 : Example of different facial expression such as (a) Sad (b) Happy and (c)Angry

Previous method of face recognition

In the past decade, significant progress has been made in developing reliable face recognition algorithms for various industries. Several classical methods have been introduced, including principal component analysis (PCA) (Turk & Pentland, 1991), independent component analysis (ICA) (Bartlett et al., 2002), and linear discriminant analysis (LDA) (Belhumeur et al., 1996). However, these methods face challenges when it comes to adequately representing faces due to large variations in facial expression and illumination conditions. This is because the patterns of faces lie on a complex nonlinear and non-convex manifold in high-dimensional space.

Artificial Neural Networks (ANN) have also been utilized for face recognition, offering solutions for nonlinear problems (Li et al., 2006). For instance, a radial basis function neural network integrated with non-negative matrix factorization has been presented to recognize faces (Zhou et al., 2006). Additionally, backpropagation neural networks have been used for face and speech verification (Park et al., 2006). ANN's advantage lies in the integration of the radial basis function with non-negative matrix factorization, making it suitable for recognizing face images with partial distortion and occlusion. However, a drawback of this approach is the requirement for a larger number of training samples, which may not be feasible in some scenarios. It is also less accurate compared to statistically based methods.

3D-based face recognition has shown high recognition accuracy compared to 2D methods, as it is less affected by variations in pose and illumination (Kemelmacher-Shlizerman & Basri, 2011). Depth information in 3D data remains consistent regardless of pose or illumination changes, enhancing the robustness of the system. However, this method requires precise calibration and synchronization of all elements with existing 3D data, making it computationally expensive and less suitable for practical applications.

Video-based face recognition (VFR) has gained attention, especially in analyzing video streams of face images (Marin-Jimenez et al., 2014). One advantage of this approach is the possibility of leveraging redundancy present in the video sequence to improve recognition accuracy, particularly in freeze image systems (O'Toole et al., 2005). In the first stage of VFR, re-identification is performed to cross-match a collection of videos and locate all occurrences of the person of interest (Poh et al., 2010). However, challenges arise when measuring similarity between multiple images, which can affect the performance of this method.

Despite the advancements made in these previous methods, face recognition technology continues to evolve, and researchers are constantly exploring new techniques and approaches to overcome the limitations and enhance the accuracy and efficiency of face recognition systems.

Experimental

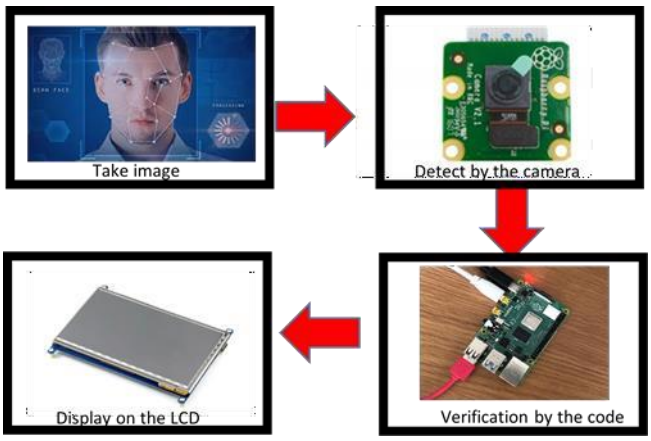

Figure. 4: The Raspberry Pi 4 Model B

The methodology for the design of this product is presented in Figure 4, illustrating the sequential flow from the initial stage to the final process of displaying the output on the screen. The design aims to demonstrate the overall process of the device, starting with the passenger capturing a picture using the camera at the departure gate. The Pi camera saves the captured image as data, which is then transferred to the Raspberry Pi for further processing.

The data is interpreted using the code implemented on the Raspberry Pi, utilizing the predetermined algorithm. The algorithm enables the Raspberry Pi to analyze and compare the received data with the stored reference data. If a match is found, the corresponding output is generated. The output is displayed directly on the Liquid Crystal Display (LCD) screen, providing immediate feedback.

The monitoring system consists of two main components: software and hardware. The software component encompasses the algorithm implemented on the Raspberry Pi, which enables data interpretation and matching. On the other hand, the hardware component includes the camera, Pi camera, Raspberry Pi, and LCD screen. A comprehensive list of all the components used in this product can be found in Table 1.

This conceptual design serves as a framework for understanding the workflow and components involved in the development of the face recognition system. It provides a clear overview of the process and sets the foundation for further implementation and testing of the product

Table 1 : Components of Smart Face Surveillance Camera

No.	Components
1	Raspberry Pi 4 Model B
2	Raspberry Pi Camera 8MP
3	Raspberry Pi power supply type C 5V 3A
4	Micro SD card adapter
5	LCD display
6	Micro USB type B
7	Logitech Keyboard

Hardware implementation

The Raspberry Pi 4 Model B is the latest product in the Raspberry Pi series, offering a cost-effective solution with significantly improved performance and capabilities compared to its predecessors. This model is equipped with several ports, including four USB ports, two micro HDMI 2.0 ports, and a USB Type-C power jack. The power jack serves as both a power input and an analog audio/video output port. Additionally, the inclusion of Gigabit

Ethernet enables reliable wired networking and the potential for control through Power over Ethernet.
To modulate the light and display the Raspberry Pi's output, such as captured images or videos during the emotion detection stages, an LCD is utilized. This LCD allows for effective visualization of the system's results and enhances the user experience.
In terms of imaging capabilities, the Raspberry Pi Camera is employed, featuring an 8MP image sensor and the option to attach a focus lens. This camera is capable of capturing high-resolution static images at 3280 x 2464 pixels and recording videos at resolutions of 1080p, 720p, and 640x480p. Its versatility makes it well-suited for the face recognition system.
Once all the necessary components listed in Table 1 are assembled, a proper prototype product is created. The data collection phase follows, where various passenger faces are captured and recorded to ensure the system functions correctly. This testing process is crucial to validate the system's performance and ensure its reliability and accuracy in real-world scenarios.

Software implementation

Before that, the LCD screen needs to be connected to the Raspberry Pi using the cable. Once connected, the terminal is opened on the Raspberry Pi and edited to the CONFIG.TXT file located in the /boot folder. Following that, a file is saved while the LCD display continues to function normally. After that, a 7-inch LCD touchscreen driver is mounted to allow touchscreen functionality. The fileneeds to be downloaded and extracted the .zip file to the raspberry pi using this link http://www.waveshare.com/w/upload/3/3d/LCD-show-160811.tar.gz. Once the file has been fully extracted, the following command is run to enable the touchscreen feature by adding add"./LCD7-800480-show" to the end of the line as seen in Figure. 5. Touch screen function is now enabled to the system.

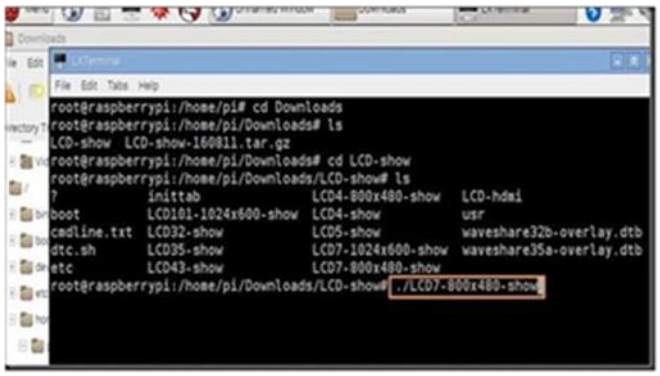

Figure. 5: To integrate the LCD screen with the Raspberry Pi

III. Results and Discussion

In this study, the Smart Face Surveillance system was subjected to data collection and rigorous testing to evaluate its performance. The data collection process involved utilizing a Raspberry Pi along with a camera. The system was integrated with Python, a programming language, which was utilized as the software framework on the Raspberry Pi. Specifically, Python software with IDLE 3.9 was employed, and a code file was opened and executed to ensure the accuracy and correctness of the coding implementation.

Upon running the program, the main window of the system was displayed, as depicted in Figure 6. To simulate real-world scenarios, passenger details were inputted into the system, capturing relevant information for analysis and verification. The passenger details were structured and organized as presented in Table 2, enabling the system to process and evaluate the captured data effectively. This comprehensive testing process allowed for a thorough assessment of the Smart Face Surveillance system's performance and functionality. By systematically inputting passenger details and assessing the system's response, the system's reliability and accuracy could be measured and analyzed. Such rigorous testing procedures were crucial to ensure the system's effectiveness and its ability to accurately identify and verify individuals in real-time scenarios.

The combination of Raspberry Pi, Python software, and the integrated camera formed a robust and capable framework for data collection, processing, and analysis within the Smart Face Surveillance system. These components worked in harmony to create a functioning system capable of accurately capturing and analyzing passenger data, contributing to enhanced airport security and a safer travel experience for all individuals involved

Figure. 6: The main window that display on the LCD

Table 2 : Information display on the LCD

No	Information
1	Flight number
2	Passport number
3	Passenger name

Upon completion of the passenger data input, the Smart Face Surveillance system proceeds to the face image capture stage. The system requires the face image to be taken before proceeding with the face recognition process. A prompt is displayed, ensuring that all necessary passenger information has been provided before capturing the image. Once the face image is ready for capture, the user can save it within the system by clicking on the "Train Image" button. This action saves the image in the system's database for further processing and comparison during the face recognition phase.

Following the data collection and image training, the system is prepared to operate in real-time surveillance mode. By clicking on the "Track Image" option within the main window, the system automatically initiates its monitoring function, actively detecting and analyzing the faces of passengers passing by the camera. The system incorporates the vaccination status of each individual, as illustrated in Figure 7. Upon detecting a passenger, the system promptly retrieves and displays the relevant information from Table 2 on the screen. This information includes passenger details such as name, passport number, and vaccination status. Simultaneously, an alert is sent to the authorities, notifying them of the detected passenger and displaying their corresponding details.

Through this process, the Smart Face Surveillance system demonstrates its ability to accurately identify and monitor individuals in real-time, providing crucial information to the authorities while maintaining a high level of security and passenger safety. The combination of automated detection, vaccination status integration, and real-time notifications enhances the system's efficacy in ensuring the safety and security of airports, while streamlining the process of identifying individuals and mitigating potential risks.

Figure. 7: Taking face image using the camera after key in all the data

If the passenger did not check in, the system will be detected as UNKNOWN with the RED colourof frame on the face as seen in Figure. 8.

Figure. 8 : The system will detect the check in passenger as name shown on the screen in greencolour and the red colour shown as unknown person

All the data, train image, track image of the passenger will be saved to the Cloud as seen in Figure. 9which is directly to be documented for authority purpose

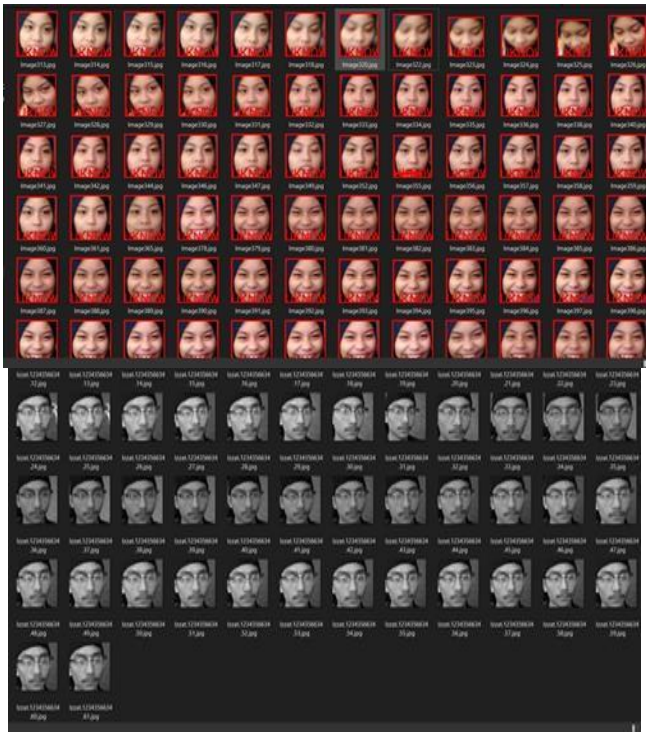

Figure. 9 : Example of taking a face image using the camera and the image will be sent to the Cloudfor the monitoring purpose.

Table 3 : Condition of system monitoring

Status check in	Screen Display Status	Font colour
Check in	Name will be shown on screen	Green
Not check in	Unknown	Red

The accuracy of this system is measured based on the total student in Table 4. The calculation is listedbelow

Table 4 : The total student that has been tested this product is 20 students

	Check in	**Unknown**	**Total**
Check in	**18**	**2**	**20**
Unknown	**1**	**19**	**20**
Total	**19**	**21**	**40**

The equation to calculate the precision is based on equation 1 and equation 2.

$$Precision = \frac{Correctly\ predicted}{Total\ predicted} \quad \textbf{(Equation 1)}$$

$$Precision\ (check\ in) = \frac{18}{19} = 0.95$$

$$Precision\ (unknown) = \frac{1}{\frac{2}{1}} = 0.9$$

$$Recall = \frac{Correctly\ classified}{Total\ Actual} \quad \textbf{(Equation 2)}$$

$$Recall\ (check\ in) = \frac{18}{20} = 0.9$$

$$Recall\ (unknown) = \frac{1}{2} = 0.05$$

$$Accuracy = \frac{Total\ correctly\ classified}{Total\ Actual} = \frac{37}{40} = 0.93 = 93\%$$

IV. Conclusions

In this study, a face recognition system integrated with a camera has been developed and tested, aiming to provide real-time access to crucial airport security information at the boarding gate. The system's functionality includes verifying whether a passenger's face matches the photo on their passport, alerting security staff in case of any discrepancies. The Smart Face Surveillance Camera, as developed in this study, can provide accurate data for authentication purposes before passengers board the aircraft. Additionally, the system is capable of detecting any suspicious or unusual behavior, significantly enhancing overall airport security and ensuring a safer flying experience for all passengers.

Furthermore, this product offers an additional advantage by providing vaccination status, which greatly facilitates the travel experience for airport users. This can be likened to a lock and key mechanism, where the security system acts as the lock and the vaccination status serves as the key. Having both the lock (security system) and the key (vaccination status) is essential for establishing a secure and safe environment, as well as ensuring a seamless and hassle-free travel experience. With data stored in the Cloud system and real-time monitoring

capabilities, authorities can promptly apprehend any suspicious passengers, ultimately bolstering national airport security. The system achieves an impressive accuracy rate of 93%, further highlighting its effectiveness and reliability in ensuring the safety of all travelers.

By successfully implementing this technology, airports can benefit from an efficient and dependable solution that addresses key security challenges. The integration of face recognition, coupled with real-time monitoring and verification capabilities, significantly strengthens airport security protocols, ultimately fostering a safer and more secure environment for passengers and staff alike.

References

[1]. Almudhahka, N., Nixon, M., & Hare, J. (2016). Human face identification via comparative soft biometrics. *ISBA 2016 - IEEE International Conference on Identity, Security and Behavior Analysis*. https://doi.org/10.1109/ISBA.2016.7477246

[2]. Bah, S. M., & Ming, F. (2020). An improved face recognition algorithm and its application in the attendancemanagement system. *Array*, *5*, 100014. https://doi.org/10.1016/j.array.2019.100014

[3]. Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2002). Face Recognition by Independent Component Analysis.

[4]. *Transactions on Neural Networks*, *16*(6), 1450–1464. https://doi.org/10.1109/TNN.2002.804287

[5]. Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1996). Eigenfaces vs. Fisherfaces: Recognition using classspecific linear projection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1064*(7), 45–58. https://doi.org/10.1007/bfb0015522

[6]. Bhangale, K. B., Jadhav, K. M., & Shirke, Y. R. (2018). Robust pose invariant face recognition using DCP and LBP. *International Journal of Management, Technology and Engineering*, *8*(9), 1026–1034.

[7]. Bhowmik, M. K., Saha, K., Majumder, S., Majumder, G., Saha, A., Nath Sarma, A., Bhattacharjee, D., Basu, D. K., & Nasipuri, M. (2011). Thermal Infrared Face Recognition – A Biometric Identification Technique for Robust Security systems. *Reviews, Refinements and New Ideas in Face Recognition*. https://doi.org/10.5772/18986

[8]. Deepa, S., & Chamundeeswari, V. V. (2016). A novel approach for genetic face recognition. *Proceedings - IEEEInternational Conference on Information Processing, ICIP 2015*, 767–771.https://doi.org/10.1109/INFOP.2015.7489485

[9]. Du, S., & Ward, R. (2006). Face recognition under pose variations. *Journal of the Franklin Institute*, *343*(6 SPEC. ISS.), 596–613. https://doi.org/10.1016/j.jfranklin.2006.08.006

[10]. Fischler, M. A., & Elschlager, R. A. (1973). The Representation and Matching of Pictorial Structures Representation. *IEEE Transactions on Computers*, *C–22*(1), 67–92. https://doi.org/10.1109/T-C.1973.223602

[11]. Goldstein, A. J., Harmon, L. D., & Lesk, A. B. (1971). Identification of human faces. *Proceedings of the IEEE*, *59*(5), 748–760. https://doi.org/10.1109/PROC.1971.8254

[12]. Hassaballah, M., & Aly, S. (2015). Face recognition: Challenges, achievements and future directions. *IET Computer Vision*, *9*(4), 614–626. https://doi.org/10.1049/iet-cvi.2014.0084

[13]. Hussien, A. (2016). CWT and Fisherface for Human Face Recognition. *International Journal of Computer Applications*, *142*(6), 27–30. https://doi.org/10.5120/ijca2016909837

[14]. Kar, N., Debbarma, M. K., Saha, A., & Pal, D. R. (2012). Study of Implementing Automated Attendance System Using Face Recognition Technique. *International Journal of Computer and Communication Engineering*, *1*(2), 100–103.http://www.ijcce.org/papers/28-N010.pdf

[15]. Kemelmacher-Shlizerman, I., & Basri, R. (2011). 3D face reconstruction from a single image using a single reference face shape. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *33*(2), 394–405. https://doi.org/10.1109/TPAMI.2010.63

[16]. Li, G., Zhang, J., Wang, Y., & Freeman, W. J. (2006). Face recognition using a neural network simulating olfactory systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3972 LNCS*, 93–97. https://doi.org/10.1007/11760023_14

[17]. Marin-Jimenez, M. J., Zisserman, A., Eichner, M., & Ferrari, V. (2014). Detecting people looking at each other in videos. *International Journal of Computer Vision*, *106*(3), 282–296. https://doi.org/10.1007/s11263-013-0655-7

[18]. O'Toole, A. J., Harms, J., Snow, S. L., Hurst, D. R., Pappas, M. R., Ayyad, J. H., & Abdi, H. (2005). A videodatabase of moving faces and people. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *27*(5), 812–816.https://doi.org/10.1109/TPAMI.2005.90

[19]. Olszewska, J. I. (2016). Automated Face Recognition: Challenges and Solutions. *Pattern Recognition - Analysis and Applications*. https://doi.org/10.5772/66013

[20]. Olszewska, J. I., Vleeschouwer, C. De, & Macq, B. (2008). MULTI-FEATURE VECTOR FLOW FOR ACTIVECONTOUR TRACKING. *IEEE ICASSP 2008 - 2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, *4*, 721–724. https://doi.org/10.1109/icassp.2008.4517711

[21]. Park, C., Ki, M., Namkung, J., & Paik, J. (2006). Multimodal priority verification of face and speech using momentum back-propagation neural network. *Lecture Notes in Computer Science (Including Subseries Lecture Notes inArtificial Intelligence and Lecture Notes in Bioinformatics)*, *3972 LNCS*, 140–149. https://doi.org/10.1007/11760023_22

[22]. Poh, N., Chan, C. H., Kittler, J., Marcel, S., Mc Cool, C., Rúa, E. A., Alba Castro, J. L., Villegas, M., Paredes, R.,Štruc, V., Pavešić, N., Salah, A. A., Fang, H., & Costen, N. (2010). An evaluation of video-to-video face verification. *IEEE Transactions on Information Forensics and Security*, *5*(4), 781–801. https://doi.org/10.1109/TIFS.2010.2077627

[23]. Prikler, F. (2016). Evaluation of emotional state of a person based on facial expression. *Perspective Technologies and Methods in MEMS Design, MEMSTECH 2016 - Proceedings of 12th International Conference*, 161–163. https://doi.org/10.1109/MEMSTECH.2016.7507537

[24]. Sajid, M., Hussain, R., & Usman, M. (2014). A conceptual model for automated attendance marking system using facial recognition. *2014 9th International Conference on Digital Information Management, ICDIM 2014*, 7–10. https://doi.org/10.1109/ICDIM.2014.6991407

[25]. Turk, M. A., & Pentland, A. P. (1991). *Face recognition using eigenfaces* (pp. 586–591). https://doi.org/10.5120/20740-3119

[26]. Uiboupin, T., Rasti, P., & Anbarjafari, G. (2016). Facial Image Super Resolution Using Sparse Representation for Improving Face Recognition in Surveillance Monitoring. *Signal Processing and Communication Application Conference*, *24*, 437–440. https://doi.org/10.1109/SIU.2016.7495771

[27]. Wu, Z., & Radke, R. J. (2011). Real-time airport security checkpoint surveillance using a camera network. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 25–32. https://doi.org/10.1109/CVPRW.2011.5981718

[28]. Zhou, W., Pu, X., & Zheng, Z. (2006). Parts-based holistic face recognition with RBF neural networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3972 LNCS*, 110–115. https://doi.org/10.1007/11760023_17