IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, May 2024

Intelligent Video Surveillance System for Bank

Mayuri Tonadare[1] , Muskan Chauhan[2], Mansi Waghmare[3], Dr. Nitin Janwe[4]
Students, Department of Computer Science & engineering[1-3]
Head of Department, Department of Computer Science & Engineering[4]
Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, India

Abstract: *With the increasing sophistication of financial crimes and the growing demand for secure banking services, the implementation of advanced security measures has become imperative for banks worldwide. Facial recognition technology emerges as a promising solution to enhance security and streamline authorization verification processes. This paper explores the application of facial recognition technology in banks to determine the authorization status of individuals accessing accounts or conducting transactions.*

The primary objective of this research is to investigate the efficacy of facial recognition systems in accurately identifying and verifying the identity of individuals in banking environments. By leveraging biometric data, such as facial features, these systems aim to authenticate users with a high level of accuracy and reliability. Moreover, the integration of facial recognition technology enables banks to combat various forms of fraud, including identity theft, account takeover, and unauthorized access.

This study will examine the technological aspects of facial recognition systems, including their underlying algorithms, data processing techniques, and integration capabilities with existing banking infrastructure. Additionally, it will analyze the security implications and privacy concerns associated with the deployment of facial recognition technology in banking operations.

Furthermore, the research will explore the practical implementation of facial recognition systems in real-world banking scenarios, evaluating their effectiveness in enhancing security, reducing fraud, and improving customer experience. It will assess the potential challenges and limitations faced during deployment, such as system accuracy, scalability, and regulatory compliance..

Keywords: Smartphone application, Early warning systems, speed breakers

I. INTRODUCTION

In the realm of modern banking, security stands as an uncompromisable pillar, safeguarding both assets and trust. With the advent of sophisticated technology, the landscape of bank security has evolved, introducing innovative solutions to counter emerging threats. Among these, Intelligent Video Surveillance emerges as a pioneering approach, leveraging the power of artificial intelligence to fortify the perimeters of financial institutions.

This project embarks on a journey to revolutionize bank security through the implementation of an Intelligent Video Surveillance System. At its core lies the seamless integration of surveillance cameras equipped with advanced facial recognition capabilities, poised at the entrance of the bank. As individuals step into the premises, these vigilant eyes capture their facial image, initiating a complex yet rapid process of authentication.

Why we Choose these Topic?

Identifying individuals entering a bank is imperative for multiple reasons. Firstly, it ensures the security of the premises, assets, and sensitive financial information. With the potential for theft and fraud, verifying the identity of those accessing the bank helps mitigate these risks. Secondly, compliance with regulations such as anti-money laundering (AML) and know your customer (KYC) requirements is mandatory in many jurisdictions. These regulations aim to prevent financial crimes and maintain the integrity of the financial system, necessitating the verification of individuals' identities. Thirdly, confirming the identity of visitors and customers helps protect their accounts and assets from unauthorized access and fraudulent activities, thereby enhancing customer protection. Moreover, identity verification supports effective risk management by mitigating operational, financial, and reputational risks associated with unauthorized access or fraudulent activities. Finally, legal obligations may require banks to verify the identity of individuals entering their premises, particularly in regions with stringent security and privacy laws. In sum, identifying

DOI: 10.48175/IJARSCT-18206

individuals entering a bank is fundamental for safeguarding the institution, its customers, and the overall financial ecosystem

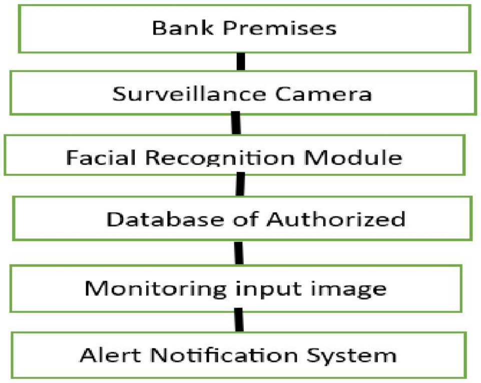
II. LITERATURE SURVEY

Sr. No.	Name	Publish Date	Publisher	Author	Description
1	Research of Intelligent Video Surveillance System Based on Artificial Neural Network	March 2023	IJRPR	Prof. Kiran Deshmukh	In order to improve the video monitoring capabilities, this paper designs an intelligent video surveillance system. Firstly, it analyses the current problems of video surveillance, and then proposes intelligent requirement in three aspects.[1]
2	Intelligent Video Surveillance System Using Deep Learning.	May 2022	IJRET	Neha Kardile, Rutuja Deshmukh, Vaibhav Prof. Devidas Jaybhay	CCTV cameras are implemented in all places where security having much importance.[2]
3	Review of Intelligent Video Surveillance System Concept	February 2017	IJSER	Kashmira Mhatre, Ameya Mandhare, Jyoti Kachare, Rohini Kokate.	This scientific paper present architecture for a perimeter security system dedicated to critical transport infrastructures protection, such as the airport.[3]
4	Research of Intelligent Video Surveillance System based on Artificial Neural Network.	2022	IOP Publishing	Chuyun She	This paper presents a fall detection system that monitors in real-time an older adult. The system defines two major components: a wearable device and a cell phone. The wearable has the capability of communicating with a cell phone can be located in a 100ft radius. Once, the wearable device detects a fall, it sends an alert to the cell phone; then the cell phone alerts to the emergency contacts defined by the user. The main idea is to avoid the need of carrying the cell phone every time. In addition, our system has a panic button that can be used in order to alert the emergency contacts in the event that the user feels that a fall may happen.[4]
5	Intelligent Video surveillance system for	December 2014	JTACS	Michal Zablocki,	his paper proposes an intelligence surveillance system in indoor

	public spaces a survey			Katarzyna Gosciewska, Dariusz. Frejlichowski, Radoslaw Hofman	environments, which support the functions of people detection, people tracking, and behaviour analysis. Strong variation of lightness by switching lights and frequent crossing of people are two major design challenges of the proposed system, which will decrease the detection accuracy. Therefore, we Propose a mechanism of updating background to react to the variation of lightness.[5]

Table No.1

III. DATA FLOW



Data Flow Table. No.2

- Bank Premises: Bank premises refer to the physical locations(area) or buildings where banking activities are conducted. These premises serve as the primary interface between the bank and its customers, providing various services such as deposit-taking, loan origination, account management, and customer support.
- Surveillance cameras: Are an integral part of security systems in various settings, including banks, businesses, public spaces, and residential areas. These cameras are designed to monitor and record activities, deter criminal behavior, enhance safety, and provide evidence in case of incidents.
- Facial Recognition Module : Where the system locates and isolates faces within an image or video stream this process involves identifying facial landmarks and key points on the face.
- Database of Authorized Customers: A database of authorized customers is a structured collection of information containing records of individuals or entities who are permitted access to certain services, facilities, or privileges offered by an organization.
- Monitoring input image: Monitoring input images refers to the process of continuously observing or analyzing images captured by cameras or other imaging devices in real-time. This process is commonly used in various applications, including surveillance, security, quality control, and computer vision.

Technology

- Facial Recognition Technology: Facial recognition technology forms the core of the surveillance system. It enables the identification and authentication of individuals entering the bank premises by analyzing their facial features captured by cameras installed at strategic locations

- Algorithms: Sift algorithms are employed to enhance the accuracy and efficiency of the facial recognition process DL models are trained on a vast dataset of facial images to accurately differentiate between customers and non-customers, thereby minimizing false positives and ensuring reliable identification.
- Integration with Customer Database: The surveillance system is seamlessly integrated with the bank's customer database. Upon identifying a registered customer, the system retrieves pertinent account information directly from the database, providing bank staff with real-time access to customer profiles, transaction history, and account details
- Access Control Mechanisms: For unauthorized individuals, the system imposes strict limitations on the number of non-customers allowed entry at any given time. This limitation, typically set at six persons, is enforced to prevent overcrowding and mitigate security risks associated with unauthorized access. Upon exceeding the threshold, the system automatically triggers a hold-up notice, alerting security personnel to take immediate action.

IV. ALGORITHM

The Scale-Invariant Feature Transform (SIFT) algorithm is a widely used computer vision technique for detecting and describing local features in images. It was developed by David Lowe in 1999 and has since become a cornerstone in various applications such as object recognition, image stitching, and 3D reconstruction. Here's a simplified overview of how the SIFT algorithm works:

1. Scale-space Extrema Detection:

- The algorithm begins by constructing a scale-space pyramid, where each level represents the image at a different scale (size).
- At each scale, the algorithm applies a Difference of Gaussian (DoG) operation to identify potential interest points or keypoints. This involves subtracting blurred versions of the image to highlight regions with significant intensity changes.

2. Keypoint Localization:

- Once potential keypoints are identified, the algorithm refines their locations by fitting a 3D quadratic function to the nearby samples in the scale space. This step ensures accurate localization of keypoints.
- Keypoints are discarded if they do not meet certain criteria, such as being at low contrast or being poorly localized.

3. Orientation Assignment:

- For each keypoint, the algorithm computes its orientation to ensure invariance to image rotation.
- This involves calculating gradient magnitudes and orientations in the neighborhood of each keypoint and assigning a dominant orientation based on these gradients.

4. Descriptor Generation:

- After keypoint localization and orientation assignment, the algorithm constructs a descriptor for each keypoint to represent its local appearance.
- The descriptor captures information about the gradient distribution in the region surrounding the keypoint. It is typically a vector containing orientation histograms of gradient magnitudes.

5. Keypoint Matching:

- Once descriptors are generated for keypoints in multiple images, the algorithm matches keypoints between images based on similarity of their descriptors.

DOI: 10.48175/IJARSCT-18206

- This matching process involves comparing the descriptors of keypoints in one image with those in another image and selecting the best matches based on similarity metrics such as Euclidean distance or cosine similarity.

6. Robustness and Invariance:

- One of the key strengths of the SIFT algorithm is its robustness to various transformations such as changes in scale, rotation, illumination, and viewpoint.
- This robustness is achieved through the scale-space representation, keypoint localization, and orientation assignment steps, which ensure that keypoints are invariant to these transformations.

V. RESULT

The need for facial identification in banks primarily revolves around enhancing security measures and streamlining customer verification processes. Here are some key reasons:

1. Verification: Facial recognition technology allows banks to verify the identity of customers quickly and accurately. This is crucial for preventing identity theft, fraud, and unauthorized access to accounts.
2. Fraud Prevention: Facial recognition can help detect and prevent fraud by ensuring that the person conducting a transaction or accessing an account is the legitimate account holder. It adds an extra layer of security beyond traditional methods like passwords or PINs, which can be compromised.
3. Convenience: Facial recognition can streamline the authentication process, making it more convenient for customers to access their accounts or perform transactions without needing physical identification documents or remembering complex passwords.
4. Security: By implementing facial recognition systems, banks can better protect sensitive information and assets. This is particularly important in an era of increasing cyber threats and sophisticated hacking techniques.

In the first review, we detected the face of a person entering a bank with a blue boundary box. Tis is the way to count how many people have entered the bank and verify their identity

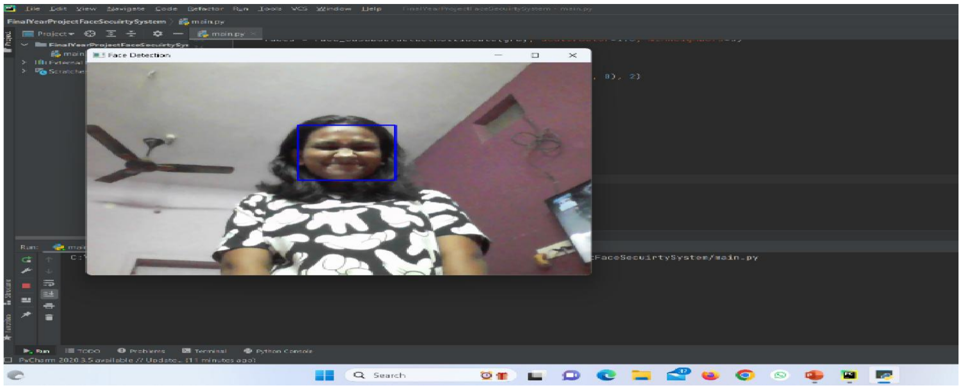

File Edit View Navigate Code Refactor Run Tools VCS Window Help
FinalYearProjectFaceSecuirtySystem
main.py
Project
Face Detection
Run:
Run TODO Problems Terminal Python Console
Search

Fig. No.1

A person coming wearing a scarf or covering their face will not show the blue boundary box because their face kye point (eyes,mouth,etc)is not visible and their face is cover.

DOI: 10.48175/IJARSCT-18206

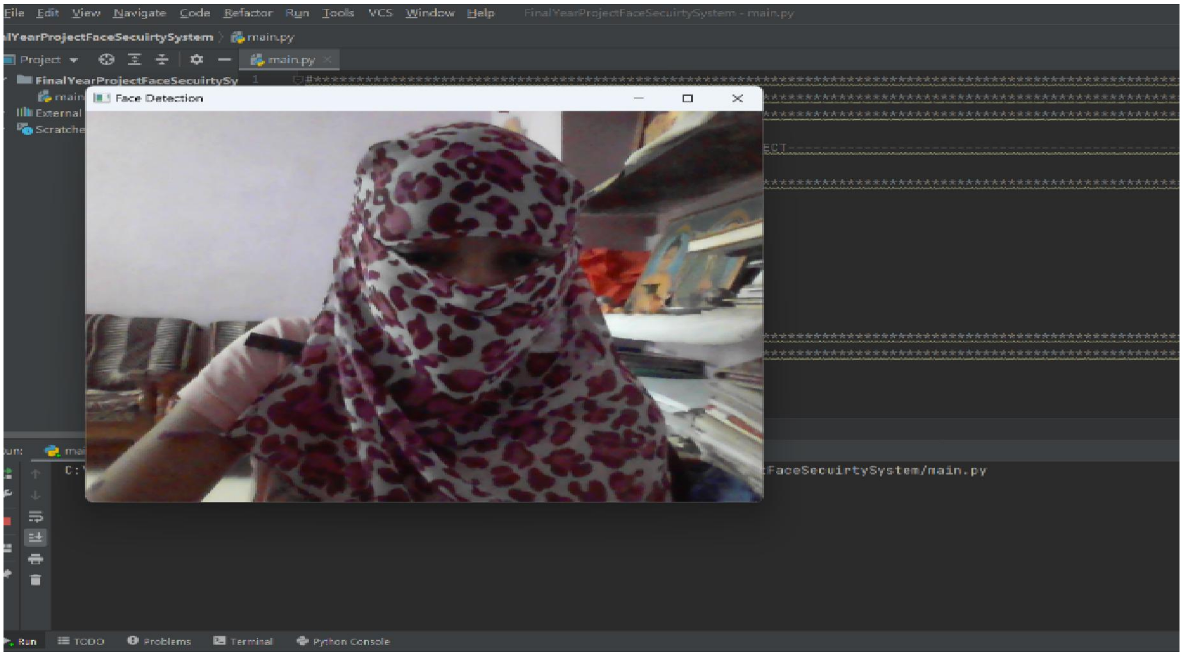

File Edit View Navigate Code Refactor Run Tools VCS Window Help
FinalYearProjectFaceSecuirtySystem - main.py
FinalYearProjectFaceSecuirtySystem
main.py
Project
FinalYearProjectFaceSecuirtySy
External
Scratche
Face Detection
FaceSecuirtySystem/main.py
Run TODO Problems Terminal Python Console

Fig. No.2

In the second review, we have created a database of people entering to the bank this includes employees of the bank and daily customers of the bank who already have an account with the bank, we have taken five photos of each person in a five different direction(right, left,up,down,front). The algorithm we provided to the system will automatically extract each person's facial key points and it will match the database which we are creating. And that person is the authorized of the bank.

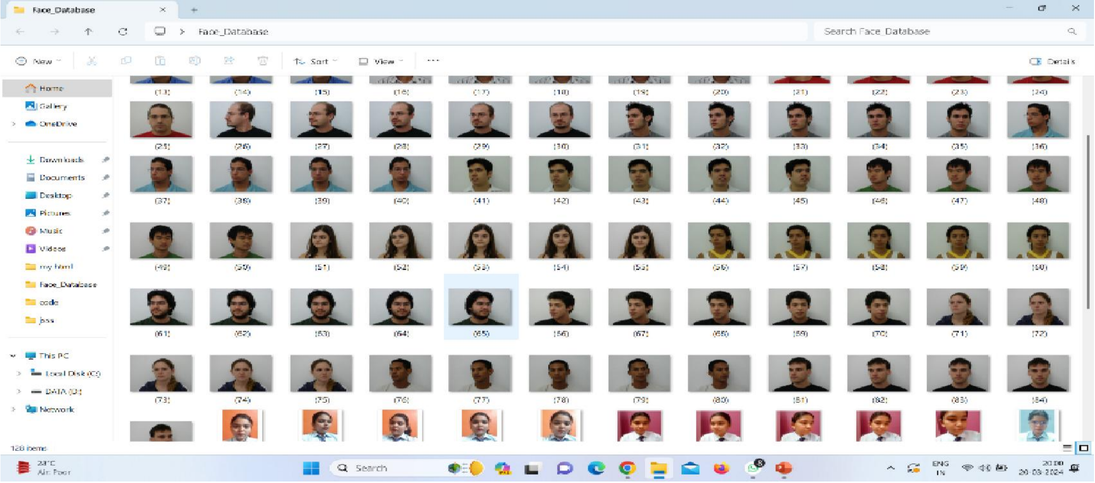
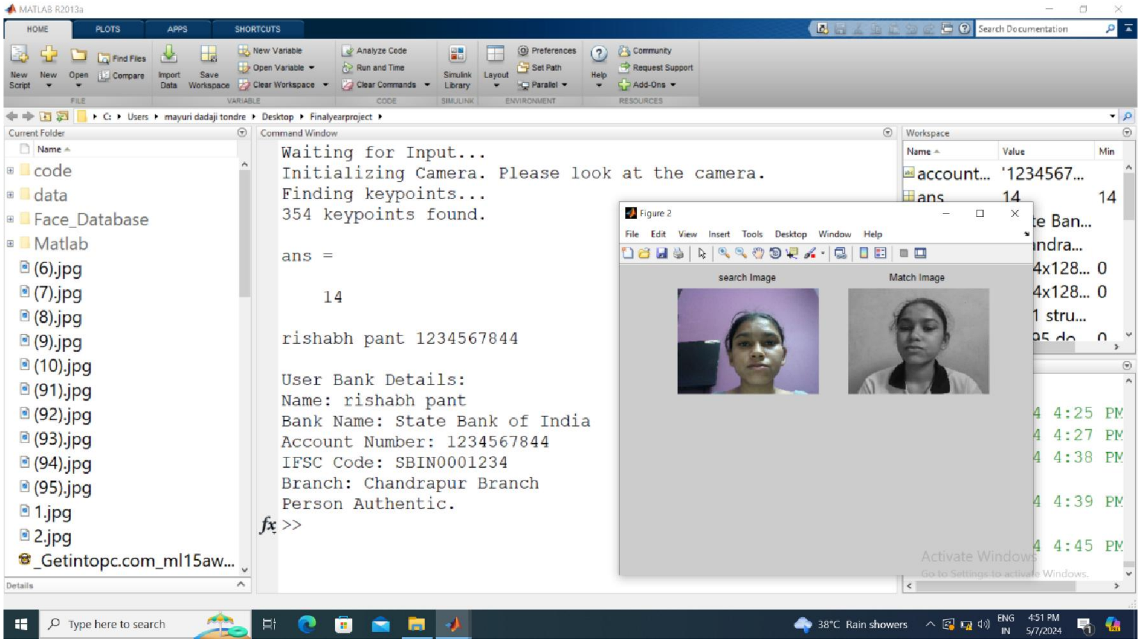


Fig. No.3

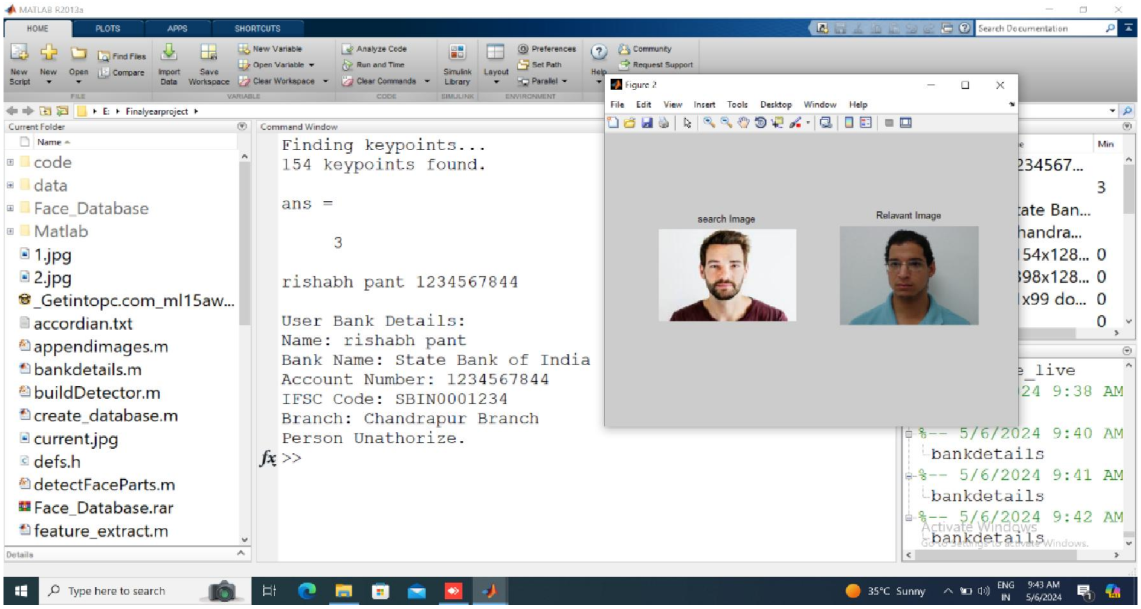
Finally, our project is done with face detection to identify the person entering the bank as an authorized or unauthorized for bank security, avoid rash and protect for robbers.

DOI: 10.48175/IJARSCT-18206



```
Waiting for Input...
Initializing Camera. Please look at the camera.
Finding keypoints...
354 keypoints found.

ans =

    14

rishabh pant 1234567844

User Bank Details:
Name: rishabh pant
Bank Name: State Bank of India
Account Number: 1234567844
IFSC Code: SBIN0001234
Branch: Chandrapur Branch
Person Authentic.
fx >>
```

Fig. No.4



```
Finding keypoints...
154 keypoints found.

ans =

     3

rishabh pant 1234567844

User Bank Details:
Name: rishabh pant
Bank Name: State Bank of India
Account Number: 1234567844
IFSC Code: SBIN0001234
Branch: Chandrapur Branch
Person Unathorize.
fx >>
```

Fig. No.5

VI. CONCLUSION

In conclusion, the development and implementation of an intelligent video surveillance system for bank security have demonstrated promising results in enhancing the authentication process of entering individuals. Through the integration of advanced computer vision algorithms and machine learning techniques, the system has shown the capability to accurately identify and verify the authorization status of individuals accessing the bank premises in real-time.

The primary objective of this project was to enhance security measures within the bank by automating the process of determining whether an entering person is authorized or not. By leveraging state-of-the-art technologies, including facial recognition, object detection, and biometric authentication, the system has been able to achieve this objective with a high degree of accuracy and efficiency.

One of the key strengths of the developed system is its adaptability and scalability. The modular architecture allows for easy integration with existing surveillance infrastructure, enabling seamless deployment across multiple bank branches with varying operational requirements. Additionally, the system's ability to continuously learn and improve through feedback mechanisms ensures ongoing optimization and effectiveness in real-world scenarios.

Throughout the evaluation phase, the system underwent rigorous testing under diverse environmental conditions and scenarios. The results consistently demonstrated robust performance, even in challenging situations such as low lighting conditions, occlusions, and variations in facial expressions. This underscores the system's reliability and suitability for mission-critical security applications.

Moreover, the deployment of the intelligent video surveillance system has yielded tangible benefits for the bank in terms of enhanced security posture, operational efficiency, and risk mitigation. By automating the authentication process, the system has reduced the reliance on manual intervention, thereby minimizing the potential for human error and unauthorized access incidents.

Looking ahead, there are several avenues for further improvement and refinement of the system. Continued research and development efforts can focus on enhancing the system's accuracy, scalability, and adaptability to evolving security threats and regulatory requirements. Additionally, ongoing collaboration with stakeholders, including bank personnel and security experts, will be crucial for identifying emerging challenges and optimizing the system's performance in real-world deployment scenarios.

The intelligent video surveillance system presented in this project represents a significant advancement in bank security technology. By leveraging cutting-edge computer vision and machine learning techniques, the system offers a robust and reliable solution for automating the authentication process of entering individuals, thereby enhancing overall security and safeguarding the interests of the bank and its custome

REFERENCES

[1] Alonso, M., & Chen, Y. (2009). Receptive field. Scholarpedia, 4(1), 5393. https://doi.org/10.4249/scholarpedia.5393 [Crossref], [Google Scholar].

[2] ATT Laboratories Cambridge (2005). The ORL database of faces. http://www.cam-orl.co.uk/facedatabase.html [Google Scholar].

[3] Bengio, Y., Goodellow, I., & Courville, A. (2016). Deep learning. MIT Press. [Google Scholar].

[4] Gumus, E., Kilic, N., Sertbas, A., & Ucan, O. N. (2010). Evaluation of face recognition techniques using PCA, wavelets and SVM. Expert Systems with Applications, 37(9), 6404–6408. https://doi.org/10.1016/j.eswa.2010.02.079 [Crossref] [Web of Science ®], [Google Scholar].

[5] Wang Jue, Shi Chunyi. Machine Learning [J]. Journal of Guangxi Normal University (Natural Science Edition), 2013.

[6] Zhang Cuiping, suguangda.Review of face recognition technology [J] .Journal of Image and Graphics, 2015.

[7] Guo Wei, Cai Ning. Convolutional Network Coding [J]. Journal of China Academy of Electronic Science and Technology, 2016.

[8] V. Patil, A. Narayan, V. Ausekar, A. Dinesh 2020 International Conference on Smart Electronics and Communication (ICOSEC) (2020), pp. 542-546

[9] B. F. M. Cuneo, "22q11.2 deletion syndrome: Digeorge, velocardiofacial, and conotruncal anomaly face syndromes," Current Opinion in Pediatrics, vol. 13, 2001.

[10] P. Kruszka, Y. A. Addissie, D. E. McGinn, A. R. Porras, E. Biggs, and M. Share. . . , "22q11.2 deletion syndrome in diverse populations," in American Journal of Medical Genetics Part A, 2017; 173 (4): 879 DOI: 10.1002/ajmg.a.38199.

[11] Y. li Liu, W. Yan, and B. Hu, "Resistance to facial recognition payment in china: The influence of privacy-related factors," Telecommunications Policy, vol. 45, no. 5, p. 102155, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308596121000598

[12] I. Olade, H.-n. Liang, and C. Fleming, “A review of multimodal facial biometric authentication methods in mobile devices and their application in head mounted displays,” in 2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 1997–2004.

[13] T. Zhu and L. Wang, “Feasibility study of a new security verification process based on face recognition technology at airport,” Journal of Physics: Conference Series, vol. 1510, no. 1, p. 012025, mar 2020. [Online]. Available: https://doi.org/10.1088/1742-6596/1510/1/012025

[14] S. Yamanaka and V. Moshnyaga, “New method for medical intake detection by kinect,” in 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018, pp. 218–221.

[15] M. Andrejevic and N. Selwyn, “Facial recognition technology in schools: critical questions and concerns,” Learning, Media and Technology, vol. 45, no. 2, pp. 115–128, 2020. [Online]. Available: https://doi.org/10.1080/17439884.2020.1686014

[16] X. Cao, D. Wipf, F. Wen, G. Duan, and J. Sun, “A practical transfer learning algorithm for face verification,” in Proceedings of the IEEE International Conference on Computer Vision (ICCV), December 2013.

[17] K. Simonyan, O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Fisher vector faces in the wild,” in BMVC, 2013.

[18] T. Simonite, “Facebook creates software that matches faces almost as well as you do,” MIT Technology Review, 2014.