**Asian Journal of Science, Engineering and Technology (AJSET)**
eISSN: 3006-6980 (online)
https://www.ideapublishers.org/index.php/ajset
Vol. 2, No. 1 (January-December), 2023, pp. 33-49
https://doi.org/10.47264/idea.ajset/2.1.4

Research Article

# Innovative security solutions: context-aware facial recognition system using VB.NET

Ammad Hussain*[1] | Muhammad Azam[1] | Shehr Bano[1] | Ahmad Nasir[1] |
Malik Abdul Manan[2]

1. Department of Computer Science, Institute of Southern Punjab, Multan, Pakistan.
2. Department of Computer Science, Beijing University of Technology, Beijing, China.

*Corresponding Author Email: ammadhussain709@gmail.com

Published: December 31, 2023

## Abstract:

A sophisticated VB.NET intelligent security system is presented in this paper to meet the needs of comprehensive security surveillance in varied contexts. The system's context-aware architecture lets it adapt to environmental changes and assess user activity for better security. The system uses real-time data to reduce false alarms and ensure fast security measures using reactive alerts and reaction processes. The system's novel security features, built on VB.NET, provide flexibility and quick reactions to emerging threats. This research shows that intelligent security monitoring technologies have achieved a peak, with excellent performance, and are ready for implementation in controlled-access public spaces. The system reacts to the surroundings and detects the subject behaviour. The system may now access new conceptual words for security issues that demand more focused solutions. A system with capabilities encourages security protocol innovation and maintains secure public spaces. This innovative technique increases security, scalability, and future flexibility for security systems. In the hunt for creative, secure areas with intelligent monitoring and danger detection, the example of an intelligent security system is impressive.

**Keywords:** Smart security, Facial recognition, Real-time monitoring, Threat detection, Image processing, Context awareness, Automation security system, Intelligent security.

**How to Cite:**
Hussain, A., Azam, M., Bano, S., Nasir, A., & Manan, M. A. (2023). Innovative security solutions: context-aware facial recognition system using VB.NET. *Asian Journal of Science, Engineering and Technology (AJSET), 2*(1), 33-49. https://doi.org/10.47264/idea.ajset/2.1.4

## 1. Introduction

The technological improvement of intelligent security systems has grown to a massive enrolment. Their installation will promote safety measures and operate across all types of environments, be it in a smart home, reference to smart homes, government premises, or even financial institutions. Such architectures are based on the latest technologies like face detection algorithms, image processing, and complexities of machine learning, as well as context awareness for ensuring proper security monitoring while detecting threats. In light of this digital epoch, facial analytics has become an indispensable benchmark in developing contemporary intelligent security mechanisms through which elements detailing all people accessing a secure premise will be duly issued. It includes papers comprising the research carried out by (Malla *et al.*, 2022). This also involves design concepts of prototypes along with the detailed components of the relationship between facial recognition coupled with artificial intelligence for lockers in smart lockers developed by (Ashraful, 2022) (conceptual model, prototype design concepts, and Such systems are programmed in VB.NET enable the development of facial recognition holotypes that confirm the identification of authorized people coming into the site and preventing illegal pursuits made by anyone else who aims at entering as an immediate neighbouring wine storage facility whereby the relevant responsible authorities do not legitimize him or her.

Apart from government activity recognition systems, context awareness forms an essential bridge in intelligent security systems as it considers the environment and user behaviour patterns concerning improving secure services. The team of (Malla *et al.*, 2022) provides a context-aware intelligent security system where the responses and alerting adjust with real-time data, which minimizes inaccurate alarms and optimizes the monitoring of actions over various settings. This system uses VB.NET to develop algorithms for context awareness, making adaptive and intelligent security measures possible because of the suitability of this technology in smart buildings and places possessing sensitive material or are security sensitive. In addition, the successful integration of facial recognition and other security tools with automation creates synergy further to amplify the efficiency and efficacy of smart security systems. These systems use VB.NET to create an automation algorithm that makes decisive and reaction actions possible in real-time, thus minimising problems quickly as security dangers thin off.

In this paper, we endeavour to contribute to the field of smart security systems by summarising the development and implementation of a VB.NET-based application, a context-aware smart system designed to ensure heightened human protection levels at present and in the future. Depending on the achievements presented above, as well as the current level of development of facial recognition, image processing algorithms, machine learning technologies, and context awareness, our system uses such a platform of integration that makes it possible to create a comprehensive, adaptive security solution intended for deployment in various environments. By applying VB.NET, we prove the usability and efficiency of our solution towards improving capability in increasing security surveillance and threat identification.

## 2. Literature review

Hossain *et al.* (2021) proposed that real-time facial recognition in intelligent surveillance systems often faces a dilemma: Speed for efficiency or accuracy reliability for accurate identification of identity. To solve this problem, the authors devised an intelligent idea—a two-stage deep learning framework instead of a single layer where Artificial Intelligence (AI) nets information to create AI for purposes such as categorizing images or finding specific patterns in the pictures without human requests. To enhance the speed of face detection, this framework uses a fast, weightless CNN, which reduces processing load compared to real-time. Detected faces emerge towards the more elaborate CNN for precise recognition. This mighty method provides not only spectacular performance but also unrivalled accuracy, which proves its viability for applications based on real-time surveillance. Authors think of improving the presented framework for resource-limited devices and aiming for better precision with difficult-to-approximate cases in mind; the emerging possibility is that it can and should be used more comprehensively.

Bagchi *et al.* (2022) designed smart home security systems with facial recognition based on cloudy technology. However, there are some limitations, such as the system's inability to differentiate between twins originating from the same womb, etc. It detects people who are not authorized to be at the door, informing average homeowners of smartphone devices in real-time. In this way, the system relies on cloud-based processing as it operates fast and with high accuracy to perform identification with almost no false alarms allowed among more than 98% match rate of the identified persons. The futuristic vision incorporates the intelligent links to the home automation devices responsible for achieving the automatic responses, thereby enabling the environmental monitoring. The staff are using this cloud approach less and the facial recognition more.

Pawar *et al.* (2018) proposed a study to simulate an intelligent security system that combines facial recognition and the Internet of Things IoT features. It is not limited to detecting intruders; it uses sensors and real-time analysis to achieve sustainable security through environmental monitoring. Their system can identify the individuals quite precisely and even work with several IoT devices whereby you could issue a command like calling an Uber when there is a triggered action.

Sivachandiran *et al.* (2022) addressed deep learning-based person detection and tracking in real-time for intelligent surveillance, making the task of great importance. Under camera footage, their system is to know individuals and distinguish legal people from unauthorized persons. This difference caused automated responses that alerted maintenance for a dark area because, on such an attempt, the alarm sounded off unauthorized entrants and provided overall security. The system runs in real-time, meaning it would detect, gather, and change over quickly, making it suitable for applications used in stealth surveillance.

Ghafoor *et al.* (2020) developed a face recognition-based home automation system built on VB.NET technology to respond to the requirements. It greets people into the room as they enter, allowing them to enter while simultaneously controlling various devices, such as lights and appliances, based on their identity. Tying real-time monitoring to your system offers yet another level of security and personalization; indeed, this could lead the home to automatically change based on who is there. This VB.NET method of the home system using facial recognition could open some exciting opportunities.

Ashraful *et al.* (2022) introduced a face recognition system based on the hybrid real-time implementation model for intelligent security. The technology offers improved security power in a super quick and precise identification process involving objects and people surviving in intelligent surveillance environments. In this way, this study can provide an alternative approach to real-time facial recognition that is more effective and has a lower consumption of resources than the project.

Gami *et al.* (2023) presented a comprehensive review of AI-based blockchain solutions for intelligent healthcare, focusing on privacy-preserving techniques. The problem addressed is the need for secure and private healthcare data management. The study discusses various AI and blockchain integration approaches to address this challenge, highlighting their effectiveness in preserving patient privacy while facilitating efficient healthcare data sharing. Algorithms reviewed include privacy-preserving data-sharing mechanisms and AI-enhanced blockchain consensus algorithms. Future work could explore the implementation and scalability of these solutions in real-world healthcare systems.

Telo (2023) investigated intelligent city security threats and countermeasures in the context of emerging technologies. The problem statement addresses the vulnerabilities introduced by adopting advanced technologies in urban environments. The study presents a range of security threats faced by smart cities and proposes countermeasures to mitigate these risks. Algorithms discussed may include intrusion detection systems, encryption techniques, and anomaly detection algorithms. Future research directions could involve enhancing the resilience of smart city infrastructures against evolving cyber threats and integrating novel security measures into urban planning frameworks.

Farooq *et al.* (2022) put forward a private blockchain network model for intrusion detection in a smart home environment. The model is equipped with a hybrid model, namely the Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system. The approach facilitates the use of data fusion and decision-level fusion procedures for this aim. The RTS-DELM methodology is a core element of the study that allows the detection of malicious acts recorded within the smart home environment using blockchain technology. The achieved performance is high, considering the low error percentage. Simulation results show behavioural intelligence algorithms implementing the most effective mechanisms for monitoring and identifying shenanigans with a smart home network.

Hall *et al.* (2020) deal with the IoT, which is a novel area whose primary application is smart homes. They trace the advancement of IoT in smart homes for a decade. These lines illustrate essential technologies as well as appliances that would be present in a smart home. At the same time, they underscore the imperative issues concerning security and privacy. The paper presents a solution to the problem, inviting the reader into a new world that is safeguarded outside the risk of the IoT with the rising adoption rates.

Anupriya and Muthumanikandan (2023) surveyed to explore the effectiveness of IoT-based home security systems. The problem addressed is the need for reliable and efficient home security solutions leveraging IoT technologies. The study reviews existing IoT-based home security systems, evaluates their performance, and identifies challenges and opportunities for improvement. Algorithms discussed may include sensor data fusion techniques, machine learning algorithms for anomaly detection, and encryption methods for data security. The future work could enhance the scalability, interoperability, and usability of the IoT-based home security systems.

Khan *et al.* (2022) introduced an intelligent control system for user confirmation based on IoT, focusing on enhancing user authentication and access control mechanisms. The problem statement addresses the vulnerabilities of traditional authentication methods in IoT environments. The study proposes a system that leverages IoT devices for user confirmation, enhancing security and usability. Algorithms discussed may include IoT data encryption techniques, authentication protocols, and access control mechanisms. Future research directions could involve enhancing the resilience of the system against cyber threats and integrating additional security features, such as multi-factor authentication.

Chakraborty and Sultana (2021) introduced an IoT-based smart home security and automation system aiming to enhance the security and convenience of residential premises. The problem statement involves addressing the vulnerabilities of traditional home security systems and improving the overall living experience through automation. The research suggests an IoT system that utilizes associated gadgets for constant checking, remote controls, and protection cautions. Some algorithms mentioned involve IoT data encryption methods, sensor data fusion algorithms, and machine learning algorithms for anomaly detection. Future research directions in the implementation of the proposed system should be directed towards making it increasingly scalable and interoperable, as well as integrating it with upcoming technologies for more advanced home automation and security features.

Varma *et al.* (2021) proposed a smart wireless black box with a cognitive facial recognition system to avoid vehicular accidents and vehicle theft by assisting Raspberry Pi with IoT sensors. The problem to be solved is centralized vehicle tracking and surveillance using mobile robotics technology. A prototype system that has been developed and described here captures and analyses facial images for user authentication as well as detection of illegal access to vehicles is provided in this study. Facial recognition algorithms and IoT data processing techniques are the algorithms employed. Potential future directions could be focused on optimizing the consistency of facial recognition algorithms in various environmental settings and implementing other security elements in the system.

Rizki *et al.* (2020) proposed a smart home security image processing technique using Principal Component Analysis (PCA) methods is presented in this paper. We have considered the development of image processing techniques for building effective and non–fail home security systems. The study envisages a structure that uses PCA for feature extraction and classification, thereby permitting real-time detection of security threats. The studied algorithms may comprise PCA-based feature extraction algorithms until recursive erosion architecture is used with machine learning classifiers till the transformation ratio is involved. Further research may focus on enhancing the accuracy and the speed of the suggested system and may be integrating it with other IoT based security applications for the complete protection of a house.

Bhowate *et al.* (2020) proposed a system to address the need to improve the security of houses and offices. This paper initiates an intelligent theft prevention system based on face recognition. Focused on the growing cases of theft and unlawful access to premises, the problem statement is formulated to represent the above incidence. The research posits a face recognition-based access control and intrusion detection system, which is more secure than traditional means. Discussed algorithms include face recognition, motion detection, alarm systems, etc. Research prospects could extend to improving presented system's precision and scalability and involvement with other IoT-based safety methods for safety against theft.

Malla *et al.* (2022) described a new Access Control Security system developed in VB.NET for sensitive institutions like government buildings or financial houses having an operator's barcode embedded form of user identification. It mentioned ensuring all forms of logins are through the process of using VB.NET. They show how the authors make a refined security solution that will arrest and tame any intruders' attempt to blaze on buildings with hitherto high risk, thereby promoting the prospects for operators and customers.

Kiran *et al.* (2020) presented a PCA-based facial recognition system for an attendance system to automate attendance tracking in educational and organizational settings. The problem addressed is the inefficiency of traditional attendance tracking methods, such as manual attendance registers. The study proposes a system that utilizes PCA for feature extraction and classification, enabling accurate and efficient attendance recording. The algorithms discussed include PCA-based feature extraction, face recognition, and attendance management algorithms. Future work could involve optimizing the performance of the proposed system and integrating it with existing attendance management systems for seamless deployment in educational and organizational settings.

## 3. Proposed model

The smart security system that we introduced includes a constellation of inter-dependent technologies developed using VB.NET, and the latter undertakes real-time crime monitoring and identification of threats in an environment and, if needed, takes some intelligent actions on behalf of humans against potential attacks. The system's architecture is designed to fulfil the stringent requirements imposed by smart security applications consisting of real-time image scanning, PCA-style face detection mechanisms with a facial recognition subsidiary capable of object identification, and an alert generator module.

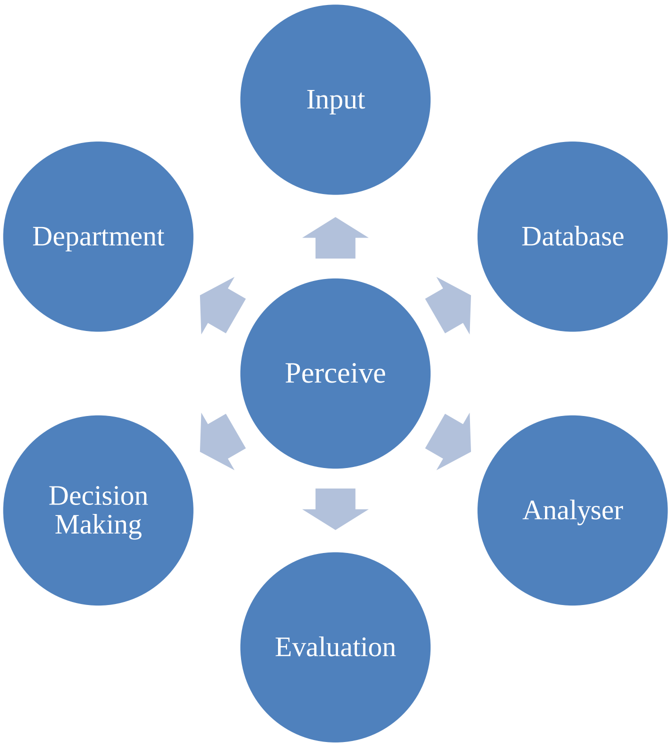
- Real-time image scanning: The system is based on VB.NET that continuously catches and processes the data dynamically captured by surveillance cameras. The system eliminates the need to create predefined rules that indicate events and anomalies to be monitored in real-time as they develop on the secured premises.
- PCA-based face detection: Using the benefits of the PCA algorithm that is leveraged by the system, this successfully detects faces on each incoming video stream. PCA facial patterns and comparison studies allow the built-in system to identify individuals within the surveillance region, guaranteeing optimal face recognition performance.
- Object recognition: Besides face detection, this system uses object recognition features that detect and classify objects of interest through video feeds. This feature allows the system to identify and follow security-related objects, including an object or unauthorized item, e.g., a cigarette or a suspicious package.
- Database integration: After the detection of security events and by matching them with facial records, this information is saved not only on a local database but also on a server that will be accessible online to conduct further analysis or search operations. This dual-storage method provides more efficient storage to secure critical security information, and it ensures the preservation of data that allows tracking it when doing forensic research or trend analysis.
- Alert generation and response: After comparing the incident reports of detected events against records in the database, the system e generates alerts and activates response protocols where necessary. Our systems in the areas of safety or security risks are raised

and promptly passed on to the relevant departments that may take appropriate measures before things go out of control.

- Decision-making mechanism: The system uses decision computing that calculates the matched records and historical data to estimate proper reaction approaches based on parameter settings. The decision-making process promotes intelligent decisions applied to the system, effectively minimizing security threats while avoiding false alarms and needless interventions.

In summary, our model uses real-time image scanning schemes, PCA-based facial detection technology, object recognition, database integration into alert-generating mechanisms, and minor decision-making to create a flexible and intelligent security apparatus. Our proposed model, written in the VB.NET platform and applied to a real-life environment, illustrates the applicability of advanced technologies for the protection of assets and the successful accomplishment of saving lives within intelligent security environments.

Figure 1: Proposed model framework



In our proposed model, the PCA algorithm is one of the most integral parts, undermining its role in improving the efficiency and accuracy of face detection used in an intelligent security system. PCA is also employed as a dimensionality reduction technique, which is very common in facial recognition-related applications. This extracts and uses the most relevant features from high-dimensional data, such as Facial images, while retaining much of the original information needed.

- Dimensionality reduction: By transforming them to a lower subspace, PCA reduces the dimensionality of facial images. This simplifies the number of computations needed for face detection by algorithms that make them more efficient and applicable to streams from cameras used in security systems.

- Feature extraction: The most discriminating features are captured from facial images through PCA, including eyes, nose, and mouth, which are essential for accurate representation of the faces. PCA is targeted to name only the features that have more information and help it solve the problem. This refined data helps the system quickly identify persons within the monitor area of concern.
- Noise reduction: Because of noise and variability in facial images that result from lighting fade, changes in radiation direction, conditions plethora face models altering and deprival of part feature PCA can reduce these effectors, contributing to face identification strength. This ensures that the system has high reliability in identifying faces under different environmental scenarios.
- Improved matching performance: With the application of PCA-based feature extraction, the performance of facial matching can be enhanced with respect to dividing redundant information within a specific feature process. This, in turn, helps improve the efficiency and accuracy with which faces detected are then matched to corresponding records in the databases.
- Scalability: Diversion from very high dimensional feature vectors to the reduced need for computations by PCA guarantees a fortified capacity of large-scale facial data processing that is fast due to the enhanced computational power. This scalability is fundamental for the real-time processing of millions of mass surveillance video streams coming from various security cameras in large deployments of secure video streaming systems.

However, in general, the central component that brings our proposal up to par with respect to addressing detection accuracy while reducing facial differences and enabling the applicability of a large-scale operation intelligent security system. Our work of applying the PCA as a solution to reduce dimensionality and extract features to enhance system performance helps us promote reliability in such individual identification tasks, positively contributing to intelligent security solutions face recognition.

One of the newly implemented aspects that we include in our intelligent security system model, to be discussed ahead, is a face detection module or meant by PCA algorithm that gets incorporated into the previous sub-module to achieve progress and improved accuracy with the means of proper identification of persons within the monitored area.

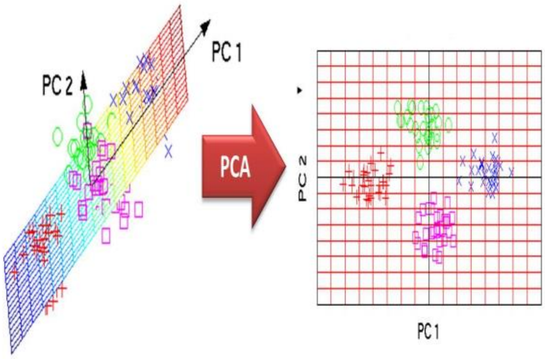
- Face detection module: This unit is used to determine and capture the information from real-time video records, given by surveillance cameras, on whether any faces are present. In this module, the PCA is applied to transform into lower dimensional arrays, and it infers eyes, nose, and mouth to characterize all of the piece's facial images under its framework.
- Preprocessing: Before and after PCA implementation, the preprocessing step for facial images provides high-quality data reliability. Processing these types of work before it can be worked upon implies activities such as converting in grayscale and image reshaping, among others, and all the input images should have a standard to suit this.
- Feature extraction: To serve this purpose, this PCA introduces the pre-processed facial images in a feature extraction model. PCA utilizes the covariance matrix calculated from the input image data as the basis for finding main components that represent significant changes to major characteristics within facial features.

- Dimensionality reduction: The first vital skip-building factors that are PCA-dependent capture a large volume of original variation and reduce the dimensions by eliminating while summarising essential univariate representation. This dimensionality reduction tool allows for fast-facing as well as reporting performance.
- Matching and recognition: Recognition and detection are carried out by matching with PCA-derived reduced-dimension feature vectors to retrieve the database records used comparatively. Such mechanisms, based on recognition systems performing identification and possessing in memory which one can recognize faces of people and possess electronic models – facial templates with the help of this procedure after extraction of anticipated features from detected human faces through identification results are exact point about identifying the person.
- Alert generation and response: Upon the detection and identification of a facial image, by comparing it against those stored in a database inside the computer's proper system of the police officer responsible for this operation, warning alarms are raised, which causes appropriate protocol responses. These trigger response alerts are supposed to notify of hacking breaches and resolve devices just in time before an impending threat transpires.

Last but not least, face detection and recognition become priority means of optimizing our intelligent security system's model performances through improved accuracy. PCA does it via contrastive features and reduces the dimensionality of façade data; PCA increases the system accuracy for identifying individuals in the monitored area, and therein, its effectiveness is ensured: The intensity \( S_i \) int Φ increases along with the decrease of the d value.

Figure 2 illustrates PCA's essence in compressing facial image data. It begins with data centralization, subtracting the mean image to isolate facial characteristics. The covariance matrix captures pixel intensity relationships, revealing key facial patterns. Eigenvalue decomposition extracts eigenvectors, representing significant image variations. Higher eigenvalues denote more crucial directions. PCA selects top eigenvectors, forming principal components that define a new coordinate system. Reconstruction combines these components with the mean image, yielding compressed, informative facial representations. This process demonstrates PCA's efficacy in dimensionality reduction while retaining essential features, making it a potent tool in facial image analysis.

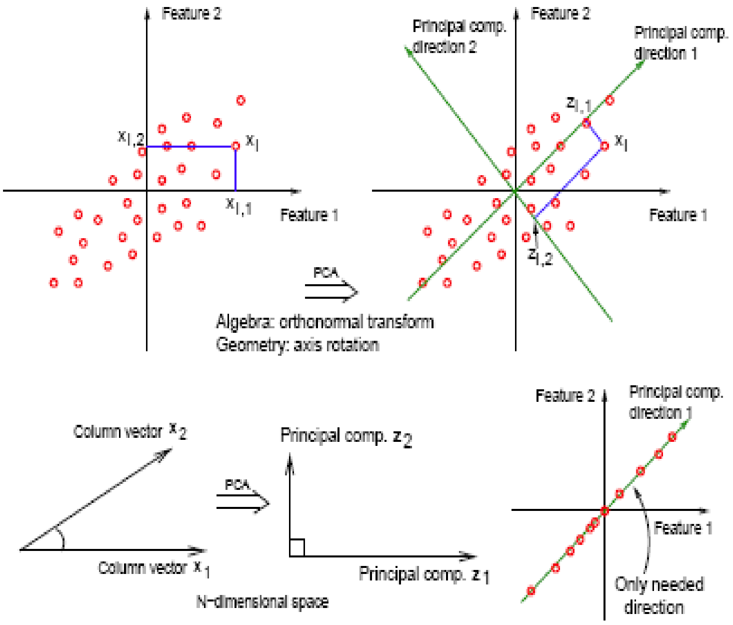
Figure 2: Dimension reduction and PCA



Source: Tripathi (2019)

Figure 3 illustrates PCA's role in extracting vital facial image details while compressing data. Initially, centralization removes brightness bias by subtracting the mean image. The covariance matrix reveals pixel relationships crucial for pattern extraction. Eigenvalue decomposition uncovers eigenvectors pointing towards directions of the highest variance, representing vital facial features. Larger eigenvalues signify more significant directions. PCA selects top eigenvectors as principal components, defining a new coordinate system. Reconstruction combines these components with the mean image, compressing data while preserving essential facial features. This visual representation underscores PCA's efficacy in dimensionality reduction and feature preservation, aligning with the given data.

Figure 3: PCA's role in extracting vital facial image



Source: https://online.stat.psu.edu/stat508/book/export/html/639/

### 3.1. Centralising the data

$$u = \left(\frac{1}{N}\right) * \sum (x\_i)$$

$$z_i = x_i - \mu$$

- µ: This is a column vector that has as many elements numbering as would be the same features on our images of faces. The elements are merely mean values of that property for every image (e.g., average pixel tone for each pixel).
- $x_i$: This is a vector representing a single facial image, with each element corresponding to a pixel intensity.
- $z_i$: This is the "centred" image, where the mean intensity has been subtracted from each pixel value. This removes the overall brightness bias and focuses on the variations in individual images.

### 3.2. Calculating the covariance matrix

$$\Sigma = \left(\frac{1}{N-1}\right) * \Sigma(z_i * z\_i{}^\wedge\mathrm{T})$$

- $\Sigma$: This is a square matrix with dimensions (number of features) x (number of features). It captures the relationships between different features (pixel intensities) across all images. Each element represents how much two specific pixel intensities co-vary (change together) across all images.

## 3.3. Eigenvalue decomposition

$$\Sigma * \mathrm{v_i} = \lambda_\mathrm{i} * \mathrm{v_i}$$

- $v_i$: This is a column vector with the same number of elements as the number of features, representing an eigenvector. Eigenvectors are directions in the data with the highest variance (spread). In face images, they might correspond to directions capturing prominent features like eyes, noses, and mouths.
- $\lambda_\mathrm{i}$ This is a scalar value representing the eigenvalue associated with the eigenvector v_i. It indicates the amount of variance captured by that direction. Larger eigenvalues correspond to more important directions.

## 3.4. Choosing principal components

- Select the eigenvectors corresponding to the largest eigenvalues. These represent the directions of maximum variance in the image data, capturing the most significant information about facial features. These chosen eigenvectors are our principal components.

## 3.5. Projecting data onto principal components

$$y_i = z_i * V$$

- V: This is a matrix with dimensions (number of features) x (number of chosen principal components). It contains the chosen principal components as columns.
- $y_i$ This is a column vector with the same number of elements as the number of chosen principal components. It represents the projected image in the lower-dimensional space spanned by the principal components. This compressed representation retains the most essential information while discarding less relevant details.

PCA is a widely used technique in data analysis and dimensionality reduction. The process begins by centralizing the data, where the mean vector is computed to remove overall brightness bias and focus on individual pixel intensity variations. Next, the covariance matrix is calculated to understand the relationships between pixel intensities across images and how they co-vary. Eigenvalue decomposition follows, identifying eigenvectors and eigenvalues that represent directions of maximum variance in the data. These eigenvectors, along with their corresponding eigenvalues, are pivotal in choosing principal components that capture the most significant information about the data. Finally, data is projected onto these principal components, creating a lower-dimensional representation that retains essential information while reducing dimensionality. This stepwise approach ensures that PCA effectively compresses data while preserving critical features, making it invaluable in various applications such as facial recognition and image compression.

- Dimensionality reduction: Through projecting images onto the principal components, you establish a dimensionality reduction, which ends up reducing up to such an extent that from each image, only one feature needs to be represented. As a result, computational complexity is reduced significantly, and algorithm face detection is accelerated.
- Feature extraction: The variations in features of the human face are, therefore, caught by these principal elements. From this point of view, it is not very dissimilar to utilizing a "template" that would allow highlighting just some basic features, such as eyes, noses, and mouths, bringing ease in recognizing different faces.
- Noise reduction: The samples obtained also form principal components that indicate directions of high variance and are highly resistant to noise even after averaging pixel intensities. It can tolerate changes in the illumination, poses, and facial occlusions.
- Improved matching performance: Using a lower-dimensional representation model reduces efficiency for matching detected faces with database entries and works faster and more accurately. This stems from the fact that it only highlights features/information that can offer discrimination while eliminating essential differences.
- Scalability: Through dimensionality reduction, PCA allows your system to work well with large amounts of facial images without problems in real-time processing systems, for this case, where the number of populations served is enormous.

## 4. Discussion

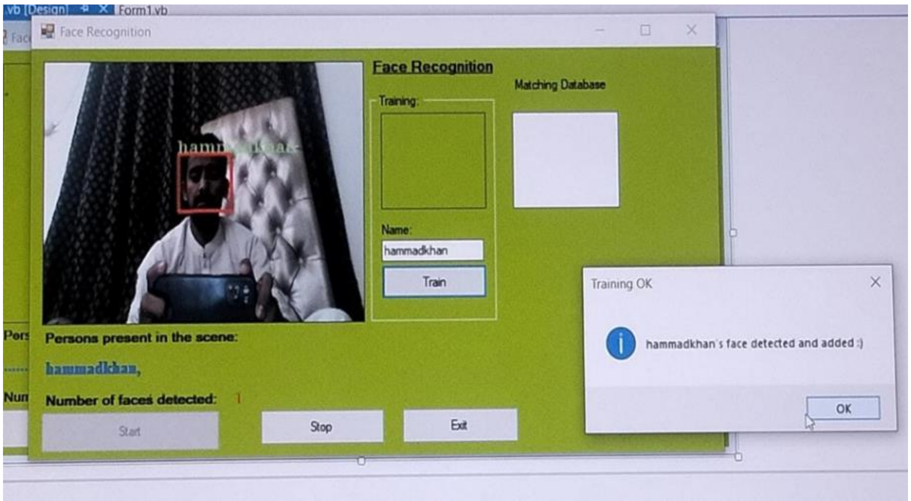
The VB.NET application provides image quoting techniques support that allows striking in real-time mode and implements measures to improve safety parameters available through any area of operation by processing video sources in VB. NET, the system can sense mining of security-relevant realms by detecting and analysing such events near 'real-time.' By incorporating face, field of view, and object detection along with the PCA algorithm, it is possible to accurately determine a person or specific objects present in each surveillance area.

The approach also guarantees both availability and availability of any critical security data, such as detection of all events in a quick manner saved on a local database server, as well as an online server. It avails the two-storage that improves information replication and affordability, making online selectors from data security records on request, either forensic investigations or trend analysis, in a limited time. Secondly, to ensure that violation is reported early, the system must be eligible to generate alerts accordingly as it detects matching events and records in the database. Through the same process, it can deliver immediate alerts to departments or stakeholders, who will be able to take appropriate actions based on such a response, which will help them minimize, if not reduce, security threats.

The decision-making capability of this system is mainly driven by the coupling of records and its history analyses through coupled weights algorithm, which is used for the identification of patterns of every record. By applying its powers, the system sets upper-bound actions over matches' records according to criteria associated with security-level contexts by evaluating the criticality of related events. An intelligent decision mechanism of this type increases the efficiency of this system for risk mitigation purposes while producing only a minimum number of false alarms and other disturbances.

In Figure 4, the face is detected with the help of PCA and eigen recognition. It will later generate a message alert as the name is saved in the system and added for later processing.

Figure 4: Face detection with PCA and eigen recognition



Name: hammadkhan

Persons present in the scene: hammadkhan,

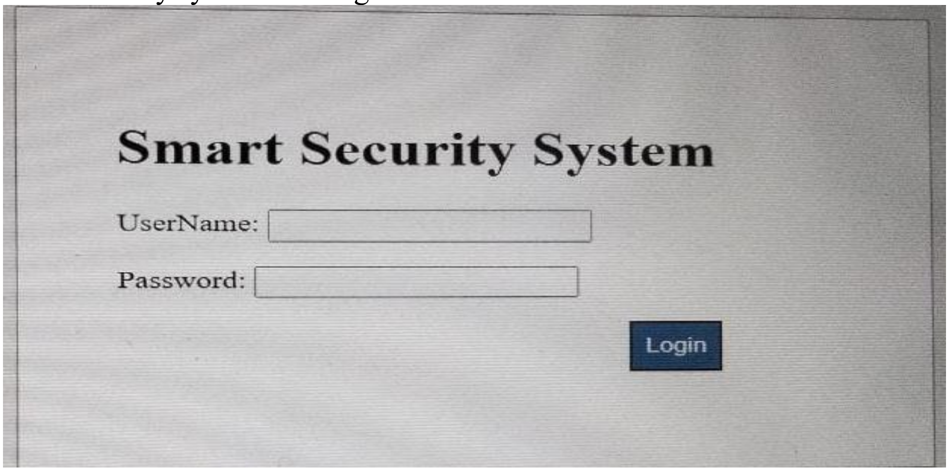
Number of faces detected: 1

Training OK

hammadkhan's face detected and added :)

Figure 5 provides a smart security system interface with real-time information via face recognition and a secure login system. Only the authorized person who has login credentials can access the smart security system status.

Figure 5: Smart security system user login


Smart Security System

UserName:

Password:

In Figure 6, the detected faces are kept in the central system repository as well as in the local repository captured during the facial recognition system, which is shown in Figure 4. It aids in recording the track of the detected person for future utilization.

Figure 6: Greyscale

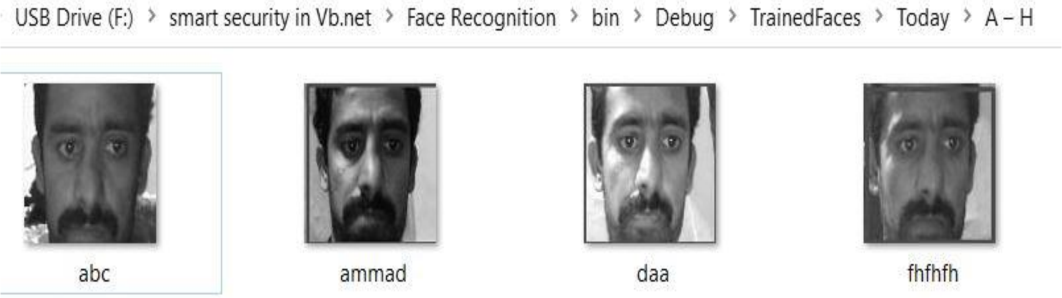
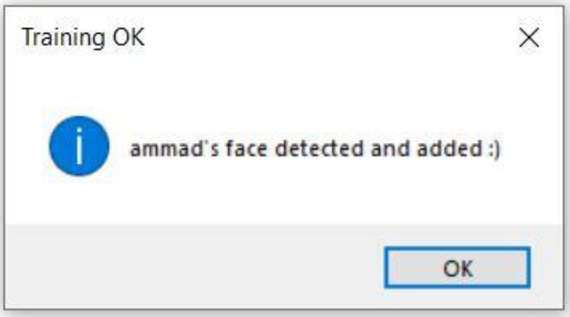

USB Drive (F:) › smart security in Vb.net › Face Recognition › bin › Debug › TrainedFaces › Today › A – H

Figure 4 captures the image of a person in real time and makes the check match the image of a person. The detected person's name is shown in Figure 7 as it was detected and saved in the local repository and centralized system.

Figure 7: Message of image saved in the local repository and centralized system

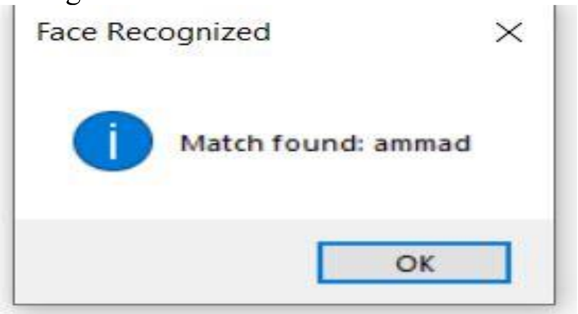


Training OK

ammad's face detected and added :)

In Figure 8, the person identified found an alert generated because in Figure 4, when a person comes under the system, the system captures the picture of the person in real-time to make the alerts and send it to the relevant department as soon as possible in our case it is an intelligent security system as shown in Figure 5 from which only the authorized person can reach it for the purpose of tracking the person already saved in the system.

Figure 8: Massage of face recognition



Face Recognized

Match found: ammad

## 5. Conclusion

In conclusion, we have delved deep into the realm of security technology, focusing on the creation and effectiveness of a real-time monitoring system. By using intelligent threat detection with VB.NET and PCA algorithms, we have showcased how our system can effectively tackle security challenges in smart environments, bridging the gap between old methods and modern needs. Through rigorous analysis and experimentation, we have proven the prowess of our system in adapting to evolving threats. However, it is not just about the tech—it is about collaboration and integration. Our system's ability to seamlessly work with others highlights the importance of partnerships in fortifying security across the board. Looking forward, there is still plenty of work to be done. We are aiming to fine-tune our algorithms, make our system even more precise and scalable, and explore opportunities for nationwide deployment. We are also keen on diving into the complexities of security resource management and finding innovative ways to tackle emerging threats head-on. Ultimately, our research is not just about advancing technology—it is about safeguarding our interconnected world. By continually innovating and collaborating, we are committed to addressing the multifaceted challenges of cybersecurity and ensuring the safety of critical infrastructures. This research lays a strong foundation for future endeavours, guiding the evolution of security solutions to meet the ever-changing needs of our society.

## Declaration of conflict of interest

The author(s) declared no potential conflicts of interest(s) with respect to the research, authorship, and/or publication of this article.

## Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

## Publisher's Note

IDEA PUBLISHERS (IDEA Publishers Group) stands neutral with regard to the jurisdictional claims in the published maps and the institutional affiliations.

## References

Anupriya, S. R., & Muthumanikandan, V. (2023, January). A survey on exploring the effectiveness of IoT based home security systems. In *2023 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–10). IEEE. https://doi.org/10.1109/ICCCI56745.2023.10128178

Ashraful, M., Hossain, M. S., Hannan, M. A., & Islam, M. T. (2022). Real-time person re-identification for smart surveillance systems using Deep Learning and VB.NET. In *2022 International Conference on Computer Communications and Network*s (ICCCN). IEEE.

Bagchi, T., Mahapatra, A., Yadav, D., Mishra, D., Pandey, A., Chandrasekhar, P., & Kumar, A. (2022). Intelligent security system based on face recognition and IoT. *Materials Today: Proceedings*, *62*,21332137.https://www.sciencedirect.com/science/article/pii/S2214785322016984

Bhowate, S., Bashine, K., Gajbhiye, P., Paidlewar, S., Dharpure, N., & Langde, P. (2020). Smart security system for theft protection using face recognition. https://doi.org/10.32628/IJSRSET

Chakraborty, P., & Sultana, S. (2021, September). IoT-based smart home security and automation system. In *International Conference on Micro-Electronics and Telecommunication Engineering* (pp. 497–505).

Farooq, M. S., Khan, S., Rehman, A., Abbas, S., Khan, M. A., & Hwang, S. O. (2022). Blockchain-based smart home networks security empowered with fused machine learning. *Sensors*, *22*(12), 4522. https://doi.org/10.3390/s22124522

Gami, B., Agrawal, M., Mishra, D. K., Quasim, D., & Mehra, P. S. (2023). Artificial intelligence-based blockchain solutions for intelligent healthcare: A comprehensive review on privacy-preserving techniques. *Transactions on Emerging Telecommunications Technologies*, *34*(9), e4824. https://doi.org/10.1002/ett.4824

Ghafoor, S., Khan, K. B., Tahir, M. R., & Mustafa, M. (2020). Home automation security system based on face detection and recognition using IoT. In *Intelligent Technologies and Applications: Second International Conference, INTAP 2019, Bahawalpur, Pakistan, November 6–8, 2019, Revised Selected Papers 2* (pp. 67–78). https://www.researchgate.net/publication/341261991_Home_Automation_Security_System_Based_on_Face_Detection_and_Recognition_Using_IoT

Hall, F., Maglaras, L., Aivaliotis, T., Xagoraris, L., & Kantzavelou, I. (2020). Smart homes: security challenges and privacy concerns. *arXiv preprint arXiv:2010.15394*. https://doi.org/10.48550/arXiv.2010.15394

Hossain, S., Umer, S., Asari, V., & Rout, R. K. (2021). A unified framework of deep learning-based facial expression recognition system for diversified applications. *Applied Sciences, 11*(19), 9174. https://www.mdpi.com/2076-3417/11/19/9174

Khan, A., Ahmad, M., Bangash, J. I., Khan, A., & Ishaq, M. (2022, April). Smart Control System for User Confirmation Based on IoT. In *Proceedings of International Conference on Information Technology and Applications (ICITA)* (pp. 397–416).

Kiran, T. A., Reddy, N. D. K., Ninan, A. I., Krishnan, P., Aravindhar, D. J., & Geetha, A. (2020, September). PCA based facial recognition for attendance system. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 248–252). IEEE. https://doi.org/10.1109/ICOSEC49089.2020.9215326

Malla, A. M., Silva, A. A. A. S., Silva, T. M. L. G., Santos, L. C. P., Ferreira, A. S. C., & de O. Guerra, R. M. C. (2022). Secure access control system with facial recognition and VB.NET for sensitive facilities. *Procedia Computer Science, 206*, 31–36. https://www.sciencedirect.com/science/article/pii/S2214785322016984: https://www.sciencedirect.com/science/article/pii/S2214785322016984

Pawar, S., Kithani, V., Ahuja, S., & Sahu, S. (2018, August). Smart home security using IoT and face recognition. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1–6). IEEE. https://ieeexplore.ieee.org/document/8697695

Rizki, R. P., Hamidi, E. A. Z., Kamelia, L., & Sururie, R. W. (2020, September). Image processing technique for smart home security based on the principal component analysis (PCA) Methods. In *2020 6th International Conference on Wireless and Telematics (ICWT)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICWT50448.2020.9243667

Sivachandiran, S., Mohan, K. J., & Nazer, G. M. (2022). Deep Learning driven automated person detection and tracking model on surveillance videos. *Measurement: Sensors*, *24*, 100422. https://www.sciencedirect.com/science/article/pii/S2665917422000563

Telo, J. (2023). Smart city security threats and countermeasures in the context of emerging technologies. *International Journal of Intelligent Automation and Computing, 6*(1), 31–45. https://orcid.org/0009-0004-5101-8064

Tripathi. A. (2019, July 11). A complete guide to principal component analysis – PCA in machine learning. https://ashutoshtripathi.com/2019/07/11/a-complete-guide-to-principal-component-analysis-pca-in-machine-learning/

Varma, V. B., Kiranmayee, B. V., Reddy, L. A., Kumar, S. S., & Varma, P. S. (2021). Smart wireless black box with intelligent facial recognition system for prevention of accidents and theft of vehicles using Raspberry Pi along with sensors based on IoT. In *Proceedings of International Conference on Advances in Computer Engineering and Communication Systems* (ICACECS) (pp. 381–392).