ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 April 2024

SMART SECURITY SYSTEM FOR SUSPICIOUS ACTIVITY DETECTION IN VOLATILE AREAS

Chilukuri Soujanya [1], Simantika Majumder [2], Sunku Hamsini [3], Pambala Harsha [4], Mrs.A. Padma Priya[5]
[1,2,3,4] UG Student, Department of ECE, CMR Institute of Technology, Hyderabad
[5]Assistant Professor, Department of ECE, CMR Institute of Technology, Hyderabad

Abstract

In recent years, the demand for image analysis applications of video surveillance has grown rapidly. The latest advances in video surveillance have aimed at automating the monitoring itself, so that it is a computer (not the security personnel) what observes the images and detects suspicious behavior or events. In this context, we present system for the automatic detection of suspicious behavior in public buildings, that obtains high resolution image of the individual or individuals who have activated the alarm in the system.

Introduction

Most current video surveillance systems share one characteristic: they need human operator to constantly watch monitors that show the images captured by the cameras [1]. The effectiveness of these systems is not determined by their technological characteristics but by the person who is monitoring the system [2]. Today, thanks to advances in many fields of computer vision, these systems are evolving to become virtually automatic. It is not human observer who detects suspicious situations, but algorithms that process the captured images and detect suspicious behavior or events [3]. The purpose of this article is to describe semiautomatic video surveillance system that is able to detect suspicious situations using artificial vision, as well as to facilitate the operator's work by generating visual and audible alerts. Most surveillance cameras installed today have static location and capture low quality images (we all have once seen on television news the images of an assault at shop where the action and the individual appears in small area of the image). Despite the high quality of the available tools for image processing, typical captured images are not very useful for crime investigation. The increasing need for security in public spaces makes real-time

detection of suspicious behavior essential, rather than simply recording them [4]. This system aims to control the camera movement and zoom in order to obtain higher quality pictures for further investigations. The system relies on two physical components: security camera to get pictures of the monitorized environment and motorized Pan-Tilt. The motorized Pan-Tilt allows the use of patrol mode. This patrol mode is sequence in which the camera remains static during configured time monitorizing defined area/position. When this time is over, the system changes the position of the camera and re-starts the monitorization (of the new area). Figure 1 represents the patrol mode described.

Literature survey

M. Shah, O. Javed, and K. Shaque. Automated visual surveillance in realistic scenarios. IEEE Computer Society, 14:30-39, Jan.-March 2007.

Using video cameras for monitoring and surveillance is common in both federal agencies and private firms. Most current video surveillance systems share one feature: they need a human operator to constantly monitor them. Their effectiveness and response is largely determined not by the technological capabilities but by the vigilance of the person monitoring the camera system. Furthermore, the number of cameras and the area under surveillance are limited by the personnel available. To overcome these limitations of traditional surveillance methods, a major effort is under way in the computer vision and artificial intelligence community to develop automated systems for the real-time monitoring of people, vehicles, and other objects.1-3 For a breakdown of the tasks and problems involved, see the sidebar "Surveillance System Tasks and Related Technical Challenges." These systems can create a description of the events happening within their area and generate warnings if they detect a suspicious person or unusual activity. In this article, we introduce the key logical components of a general automated surveillancesystem, noting important technical challenges in the real-world deployment of such a system.

A. Hampapur, L. Brown, J. Connell, S. Pankanti, A. Senior, and Y. Tian. Smart video surveillance: Applications,

technologies and implications. In IEEE Pacic-Rim Conference On Multimedia, Singapore, December, 2:1133-1138, 2003.

S ituation awareness is the key to security. Awareness requires information that spans multiple scales of space and time. A security analyst needs to keep track of “who are the people and vehicles in a space?” (identity tracking), “where are the people in a space?” (location tracking), and “what are the people/vehicles/objects in a space doing?” (activity tracking). The analyst also needs to use historical context to interpret this data. For example, the fact that the paper delivery truck showed up at 6 a.m. instead of the usual 8 a.m. would alert a security analyst. Smart video surveillance systems are capable of enhancing situational awareness across multiple scales of space and time. However, at the present time, the component technologies are evolving in isolation; for example, face recognition technology addresses the identity tracking challenge while constraining the subject to be in front of the camera, and intelligent video surveillance technologies provide activity detection capabilities on video streams while ignoring the identity tracking challenge.

V. Gouaillier and A. Fleurant. Intelligent video surveillance: Promises and challenges. Technological and Commercial Intelligence Report, March 2009.

In modern society, the development of a territory is increasingly tied to the capability to ensure an adequate level of security to persons and infrastructures. Criminal acts, including terrorist attacks; accidents; and adverse natural events can pose a threat to homeland security (HS). In recent years, in all developed countries, the awareness about the high vulnerability of the infrastructures has increased considerably. In fact, the welfare, the quality of life, and all the vital functions of a country increasingly depend on the continuous and coordinated operation of several infrastructures, which for their importance are de!ned as critical infrastructures (CI). Critical infrastructure protection (CIP) has become a crucial and delicate activity, which requires the development of innovative approaches for identi!cation, detection, and mitigation of threats, vulnerabilities, and risks. • e events of September 11, 2001, brought about a rapid expansion of CIP e□orts, in particular to prevent terrorist attacks, minimize the

damage, and recover from disruptive events. In all the activities concerning the speci!c context of the HS, information technology (IT) plays an important role, since it enables new and e□ective means to mitigate risks, providing early warning of threats and improving the response to disasters of various severity.

Anthony R.Dickand and Michael J.Brooks. Issues in automated visual surveillance. School of Computer Science, University of Adelaide, 2003.

In recent years, the demand for image analysis applications of video surveillance has grown rapidly. The latest advances in video surveillance have aimed at automating the monitoring itself, so that it is a computer (not the security personnel) what observes the images and detects suspicious behavior or events. In this context, we present system for the automatic detection of suspicious behavior in public buildings, that obtains high resolution image of the individual or individuals who have activated the alarm in the system. Most current video surveillance systems share one characteristic: they need human operator to constantly watch monitors that show the images captured by the cameras [1]. The effectiveness of these systems is not determined by their technological characteristics but by the person who is monitoring the system [2]. Today, thanks to advances in many fields of computer vision, these systems are evolving to become virtually automatic.

Existing system

The Smart Door Unlocking System with Face Recognition introduces a highly secure and convenient access control mechanism to the existing security infrastructure. In the current system, traditional methods such as keys or keycards are replaced with a sophisticated face recognition system. This system typically comprises a camera or a set of cameras integrated with facial recognition algorithms. When an individual approaches the door, the camera captures their facial features and processes the data using advanced machine learning algorithms to verify their identity.

The face recognition technology employed in this system is designed to be robust and accurate, allowing for quick and reliable identification of authorized individuals. The system can be programmed to recognize specific faces based on a pre-existing database of authorized users, ensuring that only approved individuals gain access. This technology adds an extra layer of security, as facial features are unique to each person, reducing the risk of unauthorized entry.

The Smart Door Unlocking System is often integrated with a central control unit, which manages the authentication process and controls the unlocking mechanism. Upon successful face recognition, the system triggers the unlocking of the door, granting access to the individual. Additionally, some systems may incorporate supplementary authentication methods, such as PIN codes or card-based systems, for added security.

One of the key advantages of this technology lies in its user-friendly and contactless nature. Authorized users can gain access without the need for physical keys or cards, enhancing convenience and minimizing the risk of lost or stolen credentials. Moreover, the system can log entry and exit times, providing a comprehensive access history that can be useful for security monitoring and auditing purposes.

In conclusion, the Smart Door Unlocking System with Face Recognition represents a modern and secure solution for access control. By leveraging advanced facial recognition technology, this system enhances both the convenience and security of door access, making it suitable for a variety of applications, including residential, commercial, and institutional settings.

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 April 2024

Proposed system

The proposed Smart Security System for Suspicious Activity Detection in Volatile Areas aims to enhance the safety and security of high-risk environments by employing advanced technologies for proactive threat identification. This system integrates a combination of sensors, cameras, and machine learning algorithms to monitor and analyze activities in real-time. Deployed in volatile areas such as critical infrastructure sites or public spaces, the system is designed to detect unusual or suspicious behavior that may indicate potential security threats.

The core components of this system include a network of strategically placed surveillance cameras equipped with high-resolution imaging capabilities and motion sensors. These cameras continuously capture video feeds, which are then processed by machine learning algorithms trained to recognize patterns associated with normal behavior and identify anomalies that may indicate potential security risks. The use of machine learning allows the system to adapt and improve its detection capabilities over time, enhancing its accuracy in identifying suspicious activities.

The smart security system is capable of recognizing a range of behaviors, such as unauthorized access, loitering, sudden crowd dispersal, or the presence of unattended objects. Upon detecting such anomalies, the system triggers real-time alerts to security personnel or law enforcement, enabling swift response to potential threats. Additionally, the system can integrate with existing security infrastructure, such as access control systems or alarms, to enhance its overall effectiveness.

To minimize false alarms and optimize system performance, the proposed system can also incorporate contextual information, such as time of day, weather conditions, or historical data. This contextual awareness enables the system to differentiate between normal activities and potentially threatening behavior, improving the accuracy of threat detection.

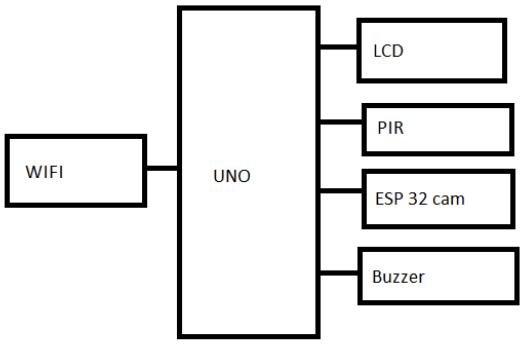
In conclusion, the Smart Security System for Suspicious Activity Detection in Volatile Areas represents a comprehensive solution for enhancing security in high-risk environments. By combining advanced surveillance technology with machine learning algorithms, the system provides a proactive approach to threat identification, allowing for timely responses and mitigating potential security risks in volatile areas.

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 April 2024

Block diagram



HARDWARE COMPONENTS

LCD (Liquid Cristal Display)

Introduction:

A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other.

A program must interact with the outside world using input and output devices that communicate directly with a human being. One of the most common devices attached to an controller is an LCD display. Some of the most common LCDs connected to the contollers are 16X1, 16x2 and 20x2 displays. This means 16 characters per line by 1 line 16 characters per line by 2 lines and 20 characters per line by 2 lines, respectively.

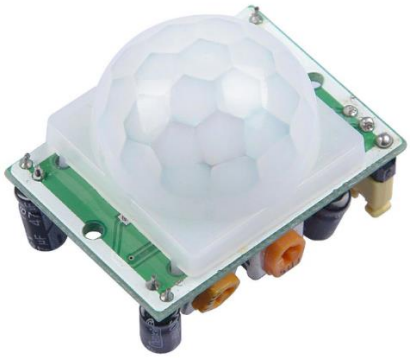
PIR SENSOR

- PIR Sensor is short for passive infrared sensor, which applies for projects that need to detect human or particle movement in a certain range, and it can also be referred as PIR(motion) sensor, or IR sensor. Since its powerful function and low-cost advantages, it has been adopted in tons of projects and widely accepted by the open-source hardware community for projects related to Arduino and raspberry pi. All this can help the beginners learn about PIR sensor more easily.

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 April 2024



- Image: PIR Motion Sensor – Large Lens version
- In this article, I will introduce PIR Sensor with the following 7 sections and compare different PIR sensors that you can find at our online store. Hope it can help you understand PIRs better and pick the suitable PIR sensor for your projects.

Applications

The ESP32-CAM suit for IOT applications such as:

- Smart home devices image upload
- Wireless monitoring
- Intelligent agriculture
- QR wireless identification
- facial recognition

BUZZERS

In common parlance a Buzzer is a signaling device that is not a loudspeaker. It can be mechanical, electromechanical, or electronic (a piezo transducer). BeStar produces Buzzers in every available configuration for a wide variety of applications. A Piezo transducer can produce the sound for panel mount buzzers, household goods, medical devices and even very loud sirens. When a lower frequency is required an electromagnetic buzzer can fill the need. These are very common in automotive chimes and higher end clinical diagnostic devices. The BeStar buzzer range includes self drive units with their own drive circuitry (indicators), or external drive units, which allow the designer the flexibility to create their own sound patterns.

ESP8266

The ESP8266 is a low-cost Wi-Fi microchip, with a full TCP/IP stack and microcontroller capability, produced by EspressifSystems[1] in Shanghai, China. The chip first came to the attention of Western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small

module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted.[2] The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, the chip, and the software on it, as well as to translate the Chinese documentation.[3] The ESP8285 is an ESP8266 with 1 MiB of built-in flash, allowing the building of single-chip devices capable of connecting to Wi-Fi.[4] The successors to these microcontroller chips is the ESP32 family of chips, including the pin-compatible ESP32-C3.

Conclusion

We built a prototype of video surveillance hardware-software system to detect potentially dangerous events in real time and alert the human operator. In addition, we have successfully fullled the goal of obtaining a view with more detail of the area or individual that has generated an alarm thanks to the pan-tilt-zoom mechanism. The system deployment is very simple, since it enables realtime threshold setting that allow to modify the degree of detections made by the system during its execution, thus adapting the system to the conditions of the dierent surveillance areas.

References

[1] M. Shah, O. Javed, and K. Shaque. Automated visual surveillance in realistic scenarios. IEEE Computer Society, 14:30-39, Jan.-March 2007.

[2] A. Hampapur, L. Brown, J. Connell, S. Pankanti, A. Se nior, and Y. Tian. Smart video surveillance: Applications, technologies and implications. In IEEE Pacic-Rim Conference On Multimedia, Singapore, December, 2:1133-1138, 2003.

[3] V. Gouaillier and A. Fleurant. Intelligent video surveillance: Promises and challenges. Technological and Commercial Intelligence Report, March 2009.

[4] Anthony R.Dickand and Michael J.Brooks. Issues in automated visual surveillance. School of Computer Science, University of Adelaide, 2003.

[5] Nathan Johnson. Background subtraction: Various methods for dierent inputs. CiteSeerX Scientic Literature Digital

Library and Search Engine [http://citeseerx.ist.psu. edu/oai2] (United States), 2008.

[6] Reddy, Kallem Niranjan, and Pappu Venkata Yasoda Jayasree. "Low Power Strain and Dimension Aware SRAM Cell Design Using a New Tunnel FET and Domino Independent Logic." International Journal of Intelligent Engineering & Systems 11, no. 4 (2018).

[7] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Design of a Dual Doping Less Double Gate Tfet and Its Material Optimization Analysis on a 6t Sram Cells."

[8] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Low power process, voltage, and temperature (PVT) variations aware improved tunnel FET on 6T SRAM cells." Sustainable Computing: Informatics and Systems 21 (2019): 143-153.

[9] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Survey on improvement of PVT aware variations in tunnel FET on SRAM cells." In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), pp. 703-705. IEEE, 2017

[10] Karne, R. K. ., & Sreeja, T. K. . (2023). PMLC- Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 477–483. https://doi.org/10.17762/ijritcc.v11i5s.7109

[11] Radha Krishna Karne and Dr. T. K. Sreeja (2022), A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER 10(4), 1092-1098. DOI: 10.37391/IJEER.100454.