World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Design and development of a motion activated internet protocol video surveillance system for crowd monitoring

Olufemi Oluseye Kehinde, Frederick Ojiemhende Ehiagwina *, Lateef Olashile Afolabi, Kabirat Oyinlola Raheem and Abdultawwab Ayotunde Ibiyeye

Department of Electrical/Electronic Engineering, The Federal Polytechnic Offa, Offa, Kwara State, Nigeria.

World Journal of Advanced Research and Reviews, 2024, 23(02), *098–110*

Publication history: Received on 22 June 2024; revised on 28 July 2024; accepted on 31 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2100

Abstract

Internet Protocol (IP) cameras are powerful tools in security and crowd monitoring implementation owing to their efficient communication over a wide geographical area. However, for any authorized personnel to initiate recording based on an event, to report a security breach, or even to stop recording when an uninteresting scene is presented, such would have to sit at the reach of the control which is not always possible. In this proposal, we implement a motion activated internet protocol (MAIP) based video surveillance system using network video management for crowd monitoring. The system can activate itself to initiate video recording on detecting motion or event using its in-built features of the network cameras and Video Management Software (VMS). The system will result in an effective and efficient motion detection video surveillance with necessary features that allow for quick recording, conserved bandwidth, greater storage, space conservation, reduces CPU load on recording servers and also allows for integration with other systems.

Keywords: Motion activated internet protocol; MAIP; IP camera; Surveillance System

1. Introduction

Surveillance systems involve the deployment of a camera-based system to monitor streets, shops and any other place of special interest. Issues around this such as legislative framework, privacy and the likes are mentioned in the following researches Kajalo and Lindblom (2011).

The latest trend in a video surveillance system is the use of Internet Protocol (IP) cameras. IP cameras are powerful tools in security implementation for proper and adequate communication over wide geographical coverage that have been applied in a wide-ranging area (Millan-Garcia et al., 2012, Manap et al. 2010a, Manap et al. 2010b). However, for any security personnel to initiate recording based on the event, to report a security breach, or even to stop recording when an uninteresting scene is presented, such would have to sit at the reach of the control which becomes impossible during a very serious case of emergency and criminal operation. These problems have led to the need for optimizing the surveillance capability which would be achieved through system automation and integration of a motion-detecting mechanism.

This research aims to design and install Motion Activated Internet Protocol Based Intelligent Video Surveillance System that will only initiate video recording on motion or event using the in-built features of the network camera and the video management software. We introduce more versatility and flexibility into the existing surveillance system. The intelligent motion detection feature of the network camera extends and supplements the human ability to monitor, and control. This system helps an individual to remotely and locally operate and monitor motion detected around the

* Corresponding author: Frederick O. Ehiagwina

protected building using IP based technology. This installation also features audio streaming that enables the voice to be heard too in a two-way manner from the monitoring unit to the camera unit.

Unmonitored crowds may constitute a threat to public safety. Thus, ensuring effective crowd management, and enabling rapid responses to security incidents within crowded environments is essential. It serves as a valuable tool for promoting security, compliance, and emergency preparedness in various public spaces, large-scale events, and critical infrastructure sites (Hamilton-Smith, McBride & Atkinson, 2021; Socha & Kogut, 2020).

The goal of the research will be achieved through the following objectives:

- System design and planning.
- Camera selection and network setup
- Software and hardware installations
- Integration and remote access
- Testing and optimization of the system

There are various types video surveillance systems such as Video Cassette Recorder (VCR)-Based Analogue Closed Circuit Television (CCTV) Systems, Digital Video Recorder (DVR)-Based Analog CCTV Systems, Network DVR-Based Analog CCTV Systems and IP Based Video Surveillance, which has some advantages for the analogue based surveillance system (Robert 2010, Olabosinde 2010).

1.1. Image Processing, Storage and Bandwidth Consideration

Types of video compression**:** There are three main video compression standards in use today: Motion Joint Photographic Experts Group (JPEG), Moving Picture Experts Group (MPEG)-4 Part 2 and H.264 (also known as MPEG-4 Part 10/AVC (Advanced Video Coding)). Each standard employs different techniques to reduce the amount of data transferred and stored in a network video system. H.264 is the latest standard that will become the video standard of choice in the coming years. Without compromising image quality, H.264 can reduce bandwidth and storage requirements by more than 80 per cent compared with Motion JPEG and as much as 50 per cent more than with the MPEG-4 Part 2 standard. H.264 and MPEG-4 Part 2 provide support for synchronized audio, while Motion JPEG does not (Bross, Chen, Ohm, Sullivan & Wang, 2021; Rao, Hwang & Kim, 2022).

Video resolution: A Video Graphic Array (VGA) resolution is 640x480 pixels. Computer screens have resolutions in VGA or multiples of VGA as shown in Table 1.

Table 1 VGA Resolutions

Display format	Pixels
QVGA (SIF)	320x240
VGA	640x480
SVGA	800x600
XVGA	1024x768
4x VGA	1280x960

1.2. Video Management System

An important aspect of a video surveillance system is managing video for live viewing, recording, playback and storage. If the system consists of only one or a few cameras, viewing and some basic video recording can be managed via the built-in web interface of the network cameras and video encoders. When the system consists of more than a few cameras, using a network video management system is recommended.

Several hundred different video management systems are available, covering different operating systems (Windows, UNIX, Linux and Mac OS), market segments and languages. Considerations include the choice of hardware platform (PC server-based or one based on a network video recorder); software platform; system features, including installation and

configuration, event management, intelligent video, administration and security; and integration possibilities with other systems such as point of sale or building management.

1.3. Hardware platforms

There are two different types of hardware platforms for a network video monument system: a PC server platform involving one or more PCs that run a video management software program, and one based on a Network Video Recorder (NVR), which is a proprietary hardware with preinstalled video management software.

1.4. Software Platform

Different software platforms can be used to manage video. They include using the built-in web interface, which exists in many network video products or using a separate video management software program that is either a Windows-based or a web-based interface.

Windows client-based software: When it comes to separate software programs for video management, windows client-based programs are the most popular. Web-based software programs are also available. With a Windows client-based program, the video management software must first be installed on the recording server. Then a viewing client software program can be installed on the same recording server or any other PC, whether locally on the same network where the recording server resides, or remotely at a viewing station located on a separate network. In some cases, the client application also enables users to switch between different servers that have the video management software installed, thus making the management of video in a large system or at many remote sites possible.

Web-based software: A web-based video management software program must be installed first on a PC server that serves as both a web and recording server. It then allows users on any type of networked computer anywhere in the world, to access the video management server and thereby, the network video products it manages, simply by using a web browser.

1.5. Video Motion Detection

Video Motion Detection (VMD) is a common feature in the video management system. It is a way of defining activity in a scene by analyzing image data and differences in a series of images. With VMD, motion can be detected in any part of a camera's view. Users can configure several "included" windows (a specific area in a camera's view where motion is to be detected), and "excluded" windows (areas within an "included" window that should be ignored). Using VMD helps to prioritize recordings, decreases the amount of recorded video and makes searching for events easier.

2. Design and Analysis

2.1. Procedure

The general procedure followed are outlined below:

Creating a Motion-Activated Internet Protocol (IP) video surveillance system for crowd monitoring involves several key steps. Here's an outline of the process:

- Step 1: System Design and Planning
  - Define the areas within the crowd that need monitoring.
  - Determine the number and placement of IP cameras based on effective coverage and optimal viewing angles.
  - Identify the network infrastructure and storage requirements to support the surveillance system.
- Step 2: Selecting Motion-Activated IP Cameras
  - Choose cameras with advanced motion detection capabilities and the ability to transmit data over an IP network.
  - Verify the compatibility of selected cameras with the intended surveillance software or Video Management System (VMS).
- Step 3: Network Setup
  - Establish a robust and secure network infrastructure to support the IP cameras, including suitable switches, routers, and network cabling.
  - Configure the network to support power and data transmission (PoE) for IP cameras if applicable.
- Step 4: Surveillance Software and Hardware Installation

  - Install the chosen surveillance software or VMS on designated servers or computers.
  - Configure and initialize IP cameras with the chosen surveillance software, ensuring that motion detection settings are optimized for crowd monitoring.
- Step 5: Setting Up Motion Detection Zones
  - Define specific motion detection zones within the camera's field of view, focusing on areas in the crowd where monitoring is required.
  - Fine-tune sensitivity and other settings to ensure accurate motion detection.
- Step 6: Storage and Retention Policy
  - Establish storage parameters, including defining video retention duration, compression settings, and archival policies.
  - Implement data backups and secure storage solutions to safeguard collected video footage.
- Step 7: Video Analytics and Alarms
  - Configure the surveillance system to raise alerts or alarms when motion is detected within the defined zones.
  - Enable real-time video analytics to monitor crowd movements, crowd density, and identify potential security concerns.
- Step 8: Integration and Remote Access
  - Integrate the surveillance system with other security infrastructure, such as access control systems and alarms, to enhance overall security.
  - Ensure remote access to the surveillance system for real-time monitoring, configuring secure access through VPN or trusted network connections.
- Step 9: Testing and Optimization
  - Conduct thorough testing of the surveillance system to verify motion detection effectiveness, video quality, system stability, and alarm triggers.
  - Optimize camera settings, motion detection parameters, and network performance based on test results and actual crowd monitoring scenarios.
- Step 10: Training and Ongoing Maintenance
  - Train relevant personnel on the use of the surveillance system, understanding motion detection alerts, and interpreting live and recorded data for crowd monitoring.
  - Establish a process for routine system maintenance, including camera position validation, software updates, and integrity checks.

2.2. Principles of Operation

The IP based surveillance system uses the inbuilt motion detection mechanism of the network camera that would be tuned to sense video motion to initiate recording. Installed on the monitoring station within the network, is a Window Client-Based Video Management Software (VMS) that can be tuned to perform live viewing, recording and playback and event-triggered storage on the local hard drive of the laptop. The network camera operation is manipulated and managed via the built-in web interface and video encoders that are accessible through the laptop that is also attached to the network using Unshielded Twisted Pair Ethernet Cable. The VMS installed on the laptop is used for advanced configuration features such as motion detection, recording, video compression, event management, intelligent video, administration and security. These configurations ensure that the embedded video recorded on the VMS only records on the event-triggered basis. These greatly reduce bandwidth consumption and memory usage.

To achieve the set objectives of this project work, the concept, tools, procedures, a technology considered is analyzed in the following section.

2.2.1. Configuration, Management and Control

In the basic configuration of this design, the network camera, the monitoring unit and the recording section were configured with basic parameters such as camera name, system time, Network information, security, Recording schedule, client settings for video and audio formatting for preview and monitoring.

2.2.2. Network Camera

For initial minimum set-up that allows the network camera to operate and perform manual recording, the basic configuration is carried out via the application software and in-built web interface. The network cameras can be accessed over a network simply by typing the IP address in the Address/Location field of a web browser on a computer. For a camera located at address 192.168.8.222 this will look something like this:

http://11192.168.8.222/home

Once a connection is made with the network Camera, the Camera 'start page', along with links to the product's configuration pages, is automatically displayed in the web browser. This also provided an interface for management of video for live viewing, recording, playback and storage. Other advanced configuration that involves features such as software platform, system features, including installation and configuration, event management, intelligent video, administration and security together with the support for automatic recording to a central server will be configured with the video management systems. The video management system exists as a window client-based platform. The video management software was installed on the mini-laptop which is connected to the network to access other connected devices.

2.3. Windows Client-Based Network Management Software

With a Windows client-based program, ST507, the server part of the video management software was first installed on the monitoring unit which controls the operation of the local video recording database. Then a viewing client software program can be installed on the same PC, whether locally on the same network where the recording server resides, such as we have in this project design, or remotely at a viewing station located on a separate network. In some cases, the client application also enables users to switch between different servers that have the video management software installed, thus making the management of video in a large system or at many remote sites possible.

2.4. Video Management System Configuration

System features that provided support for the simultaneous viewing of video from multiple cameras, recording of video and audio, event management functions including intelligent video recording by video motion detection, camera administration and management, and user access control and activity (audit) logging.

2.5. Administration and Management Features

Apart from the configured basic camera settings, frame rate, resolution and compression format, some other advanced functionalities, such as camera discovery and complete device management were tested. Software programs that helped to simplify the management of network cameras in an installation often provided the following functionalities: Locating and showing the connection status of video devices on the network, setting IP addresses, configuring single or multiple units, managing firmware upgrades of multiple units, managing user access rights, and providing a configuration sheet, which enables users to obtain, in one place; an overview of all camera and recording configurations.

An important part of video management is security. The video management software enabled the following to be defined or set: Authorized users, passwords, different user-access levels; administrator-access to all functionalities; operation access to all functionalities except for certain configuration pages and viewer-access only to live video from selected cameras. Further configuration on the network camera may offer HyperText Transfer Protocol (HTTPS) encryption for secure communication; IP address filtering, which gives or denies access rights to a defined IP address; IEEE 802.1X to control network access; and user access log.

3. Installation, Configuration And Testing

3.1. Installation

The first stage in the design and installation of this project is the paperwork design and the analysis where the overall concept was visualized and the necessary settings were calculated as needed. The outcomes of this procedure were implemented in the installation and configuration of the surveillance system. After the necessary condition and scenario were satisfied, the testing stage was carried out with the different conditions of video motion detection. The subsequent section represents the account of the installation, configuration and testing carried out the project work.

3.1.1. Hardware: Network Deployment

All the required gadgets; Network switch, IP camera, Network Ethernet cable, Video management station were connected according to the network set up shown previously in Figure 1. The power supply was duly provided to those devices that require it. The process took the following steps:

- Each camera was connected to a Power over Ethernet (PoE) switch via Ethernet cables.
- Since a PoE switch was used for this project work, the Ethernet cable provided the needed power supply for the two cameras. This eliminated the usage of the supplied power cable for each camera.

- The monitoring and recording station was also connected to the switch via Ethernet cable.
- All gadgets were powered in preparation for the installation of software needed for the camera to operate and for subsequent configurations. The final hardware installation achieved is shown in figure 1.

Figure 1 Physical network set-ups

3.1.2. Software Installation

The software installation for this network involved three components: Installation Wizard, standalone Video server, standalone client.

3.2. Installation Wizard 2 (IW2)

The installation wizard was installed following the instruction of the monitoring station. A screenshot of the installation procedure is as shown in Figure 2.

Figure 2 Installation Wizard

After the installation, the installation wizard (IW) recognised each camera for smart set up and basic configuration on the LAN

3.2.1. Standalone Video Server and Client

The centralized management site contains the server components for video recording and the Live Client and Playback for Real-time monitoring and playback viewing respectively. These two components were installed on the monitoring station. The on-screen instruction was followed to complete the installation. Figure 3 shows a screenshot of the installation.

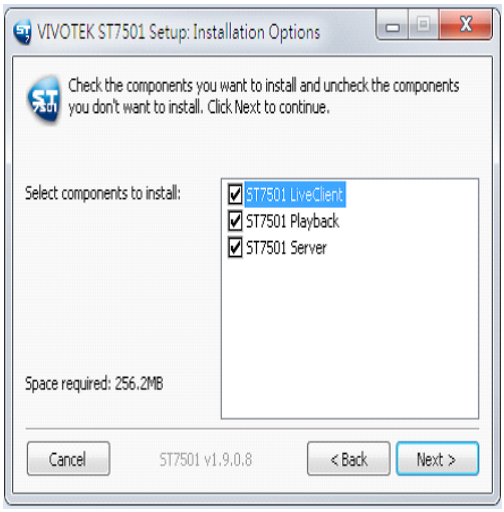

Figure 3 Screenshot of the installation

3.3. Configurations

Having carried out the design, followed by both hardware and software installation on the surveillance system, the project was configured, tested to ensure its workability per the goal of the project work.

The subsequent sections explain the configuration and testing of steps in three different areas of focus;

- Network Cameras
- Standalone Server
- Live Client and Monitoring Station

3.3.1. Network Camera Configurations

The camera configuration was achieved in two stages:

Basic Smart Setup Configuration: The first stage being the basic camera setup for network access via the smart setup panel of the Installation Wizard 2 interface. Once installed, the IW2 recognised the two networked cameras with their individual MAC Address.

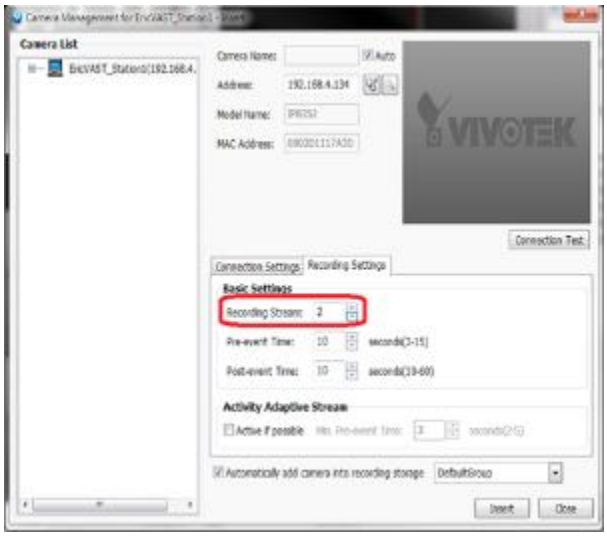

Figure 4 Advanced Mode Interface Navigation Menu

The smart setup button on the left side panel of the IW2 interface was clicked. This launched the camera built-in web interface for configuration settings that affects features such as camera hostname, system time settings, Network Access, basic access security, event detection window, percentage video motion detection percentage sensitivity and strength, audio and video format. Interface for video management for live viewing, recording, playback and storage was also configured. Figure 4 shows the screenshot showing the basic and advanced mode interface navigation menu.

Advanced Event and Recording Configuration: Other advanced configurations that involve features that focus on project objectives were configured in the Advanced Mode Interface. These include application configuration, event management, intelligent video motion detection profiles, administrative and security configurations. The video motion detection profile used was configured on the event window to fit in with the sensitivity value of 90% and percentage size of 10% (i.e. very sensitive to slight motion changes of relatively small object movement). The screenshot of the camera management profile is shown in Figure 5.

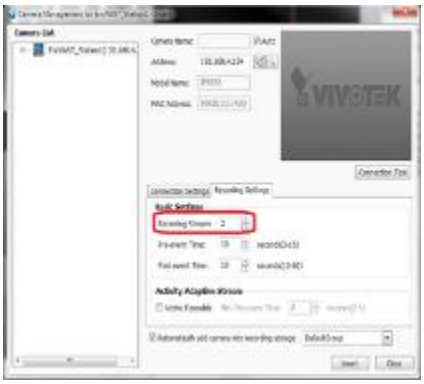

Figure 5 Screenshot of camera management profile

3.3.2. Standalone Server Configurations

The server configuration menu is accessible through the login prompt of the standalone live client monitoring station. The ST7501 Live Client program was launched and the login details required in the blank was supplied to the pop up shown below:

- The IP address of the monitoring station where the standalone server is situated
- User name of the server
- The password of the server

Once this login procedure was initiated, a monitoring interface for the Live Client was displayed with the menu bar as shown in figure 6.

Figure 6 Live Client pop window for Access to Server recording and video Monitoring

Here, the mission-critical operations such as connecting/removing a camera station, video orientations were configured. Other advanced-level configurations such as support for automatic recording to a central server, scheduled recording and logging, maintenance operation and as well as Motion-triggered operations were as well implemented accordingly. These configuration operations were carried out on the video management systems with the assistance of the drop-down menu bar as shown in figure 7.

Figure 7 Live Client expanded to show the functional part of the configurations.

The main attention was focused on the configurations sub-menus as highlighted below;

- The station on the device tree was activated by clicking on it.
- This order was then followed: Configuration > Camera Management on the menu bar (or right-click the station, then select Camera Management).
- The camera Management window on popping up the provided option for connecting the two cameras to the monitoring station using the IP address given to each device.

3.3.3. Client and Monitoring station configurations

The Video Monitoring station configuration was done to suit the design goal. These settings focus on features that have a direct effect on the motion detection and recording of data across the network. The settings configured are as stated next;

General setting: The station general settings were accessed following the direction; configuration > station settings > General settings on the menu bar. The station General setting popped up for configuration. In this section, the set up for information and event logging was performed for the station. The event window of the standalone Live Client was used to open an event window, which shows the real-time information for event triggers during testing of the setup.

Recording settings: Two recording profiles were configured for the two IP cameras after they were placed in the same default recording group on the recording setting profile management. One profile was set to favor continuous recording while the other was in favor of the event-triggered recording. The two profiles maintained the same features for the recording schedules with equal time frame, recording frequency and recording mode of week-base as a control on the testing case. The Event Trigger Recording Mode used the following parameters:

- Triggers (Motion and PIR)
- Digital input (Trigger state)
- Repeat Frequency (Week Base; Week Days only)

Association Settings for Event Triggering: ST7501 Live Client association management was configured for event trigger notifications from Digital Input/output DI/DO status on the networked camera for an event-based recording of linked network devices. The motion event configured was in favor of PIR and Video Motion Recording. The following steps were followed for the Association Management configuration:

- The DI/DO settings on the camera were enabled (High/Grounded) through the camera web interface configuration page. This was achieved by right-clicking on the device and clicking camera settings to open the configuration page.
- The navigation on the Live Client menu bar was then launched in the order of configuration > Association Management on the menu bar.
- The Association Management was selected.
- The event trigger was then enabled on each camera according to digital DI/DO requirements.
- Further configuration was done on the Live Client to set DO to correlate with the event Triggered Recording Mode previously configured.

Recording Path for Default Group: The default recording path chosen for the implementation is C:\Recording on the monitoring station for the storage of the video recorded.

Recording schedule: The two cameras were assigned to a recording schedule in the configuration panel. The recording schedule was first selected on the schedule drop-down list. The default settings were maintained since it assigned the two cameras under the station of the default schedule. A screenshot of this process is shown in figure 8.

Figure 8 Screenshot of the configuration window for the recording schedule

4. Conclusion

This research resulted in the development of a surveillance system for crowd monitoring and control. The motion-activated internet protocol (IP) Video Surveillance System for crowd monitoring offered numerous benefits and plays a critical role in maintaining security and safety in various public spaces and events. Benefits of the system include:

- **Proactive Threat Detection:** The motion-activated surveillance system is capable of detecting unusual movements or suspicious behavior within crowds, enabling security personnel to proactively address potential security threats.
- **Enhanced Situational Awareness:** By monitoring crowd movements and activities, security personnel gain a better understanding of crowd dynamics, facilitating effective crowd management and resource allocation.
- **Immediate Response:** The system can trigger immediate notifications or alerts upon detecting abnormal or unauthorized activities, enabling security personnel to respond promptly to potential incidents.
- **Crowd Density Monitoring:** The system can help monitor and manage crowd density, especially in areas where overcrowding poses safety risks, allowing for timely intervention to prevent potential stampedes or accidents.

- **Remote Monitoring and Management:** The ability to remotely view and manage crowd footage provides security personnel with real-time visibility into crowd activities, even in dispersed or large-scale event venues is another benefit of the designed system.
- **Evidence Collection:** The surveillance system can capture footage of incidents or disturbances, providing valuable evidence for post-incident analysis, investigations, and legal proceedings.
- **Emergency Response Coordination:** Surveillance footage can be used to guide emergency response efforts, ensuring that resources are effectively deployed, and that assistance is directed to where it is most needed.
- **De-escalation of Conflicts:** The system can aid in identifying and addressing potential conflicts or disturbances within crowds, contributing to the prevention of escalating situations and maintaining a safe environment.
- **Post-Event Analysis:** After an event or gathering, the video footage can be crucial for reviewing crowd behavior, mitigating security lapses, and planning for future events.
- **Compliance with Safety Standards:** For public spaces and large events, the use of surveillance systems for crowd monitoring can demonstrate compliance with safety regulations and emergency response protocols.
- **Deterrent and Prevention:** The presence of surveillance cameras can act as a deterrent to potential disruptive or unlawful behavior, contributing to a safer and more controlled environment.

The completed physical project was submitted to the Directorate of Research and Innovations, Federal Polytechnic Offa, Kwara State.

Compliance with ethical standard

Acknowledgements

This work was funded by Tertiary Education Trust Fund (TETFUND), Nigeria under the Institution Based Research (IBR) Grant Batch 13 RP disbursement. We also acknowledge the Research and Innovation Unit of the Federal Polytechnic Offa, Kwara State, Nigeria.

Disclosure of Conflict of interest

No Conflict of interest to be disclosed.

References

[1] Bross, B., Chen, J., Ohm, J. R., Sullivan, G. J., & Wang, Y. K. (2021). Developments in international video coding standardization after AVC, with an overview of versatile video coding (VVC). *Proceedings of the IEEE*, *109*(9), 1463-1493.

[2] Hamilton-Smith, N., McBride, M., & Atkinson, C. (2021). Lights, camera, provocation? Exploring experiences of surveillance in the policing of Scottish football. *Policing and society*, *31*(2), 179-194.

[3] Kajalo, S. & Lindblom, A. (2011). An empirical analyses of retail entrepreneurs' approaches to prevent shoflifting. *Security Journal*, 24(4), 269-282.

[4] Walby, K. (2005). Open-Street camera surveillance and governance in Canada. *Journal of Criminology and Criminal Justice*, 655-683.

[5] Manap, N. A., Di Caterina, G., Soraghan, J., Sidharth, V., & Yao, H. (2010, June). Smart surveillance system based on stereo matching algorithms with IP and PTZ cameras. In *2010 3DTV-Conference: The True Vision-Capture, Transmission and Display of 3D Video* (pp. 1-4). IEEE.

[6] Manap, N. A., Di Caterina, G., Soraghan, J., Sidharth, V., & Yao, H. (2010, July). Face detection and stereo matching algorithms for smart surveillance system with IP cameras. In *2010 2nd European Workshop on Visual Information Processing (EUVIP)* (pp. 77-81). IEEE.

[7] Millan-Garcia, L., Sanchez-Perez, G., Nakano, M., Toscano-Medina, K., Perez-Meana, H., & Rojas-Cardenas, L. (2012). An early fire detection algorithm using IP cameras. *Sensors*, *12*(5), 5670-5686.

[8] Olabosinde, O. O. Design and Construction of Passive-Infra-Red (PIR) and Digital Video Recorder (DVR) Based Surveillance System. B.Tech Project Report, Department of Electronics and Electrical Engineering, Ladoke Akintola University of Technology, Ogbomoso, (2010).

[9] Rao, K. R., Hwang, J. J., & Kim, D. N. (2022). *High Efficiency Video Coding and other emerging standards*. River publishers.

[10] Robert, L. P. (2010); How IP Based Video surveillance Works –Ways beyond Analog CCTV

[11] Socha, R., & Kogut, B. (2020). Urban video surveillance as a tool to improve security in public spaces. *Sustainability*, *12*(15), 6210.

Author's short biography

Olufemi Oluseye Kehinde:

Engr Dr O. O. Kehinde obtained his Bachelor degree in Electrical and Electronics Engineering in 1992 from Abubakar Tafawa Balewa University, Bauchi, Bauchi state, Nigeria. In 2013 he had his Masters Degree in Information Technology, from the National Open University of Nigeria, Ilorin, Study Centre. He finished his PhD in Electronics Engineering from Atlantic International University, Hawaii, USA.

He is currently a Chief Lecturer in the Federal Polytechnic, Offa, Kwara state, Nigeria, where he serves as the Director in charge of Research and Development. Engr Dr Kehinde is a corporate Member, Nigerian Society of Engineers (MNSE), a registered Member of Council for the Regulation Of Engineering in Nigeria (COREN) and Member, IEEE, where he equally belongs to Communication and Computer Society. Finally, he is a Member, Nigerian Institute of Electrical and Electronics Engineers (NIEEE).

Frederick Ojiemhende Ehiagwina:

Engr Dr Frederick Ojiemhende Ehiagwina was born in Benin City, Edo state, Nigeria. He obtained his Bachelor degree in Electrical Electronics Engineering from Ambrose Alli University, Ekpoma, Edo state, Nigeria in 2010. He obtained his Masters Degree and Ph.D. in Electrical and Electronics Engineering (Electronics and Telecommunication option) from the university of Ilorin, Kwara state Nigeria in 2016 and 2024 respectively. His research interest include: optimization of telecommunication systems, design and characterization of electronics system, reliability assessment of electrical and electronics systems, and renewable energy. He is currently a Lecturer and the acting Head of Department of Electrical/Electronic Engineering at the Federal Polytechnic, Offa, Kwara state, Nigeria. Engr Dr Ehiagwina is registered with the Council for the Regulation of Engineering in Nigeria (COREN), Nigeria Society of Engineers (NSE), amongst others. He has published more than 80 conferences and journal articles.

Lateef Olashile Afolabi:

Engr Lateef Olashile Afolabi was born in Offa, Kwara state, Nigeria. He obtained his Bachelor of Engineering degree in Electrical Electronics Engineering from University of Ilorin, Ilorin, Kwara state, Nigeria in 2008. He did his Masters Degree Electrical Engineering from the university of Ilorin, Kwara state Nigeria. He is currently pursuing his Ph.D at the Osun State University. He is currently a Lecturer at the Federal Polytechnic, Offa, Kwara state, Nigeria.

Engr Afolabi is a Cooperate member of Nigerian Society of Engineering (MNSE) and registered with the Council for the Regulation of Engineering in Nigeria (COREN). He is also a member Nigerian Institute of Management (NIM).

Kabirat Oyinlola Raheem:

Engr Mrs Kabirat Oyinlola Raheem obtained a Bachelor degree in Electrical/Electronics Engineering from Kwara State University in 2017. She is currently doing her Masters Degree in Electrical/Electronics Engineering from same University. She is currently a Lecturer at the Federal Polytechnic, Offa, Kwara state, Nigeria. She is registered with the Council for the Regulation of Engineering in Nigeria (COREN).

Ibiyeye Ayotunde Abdultawwab

Engr Ibiyeye Ayotunde Abdultawwab was born in Kwara State, Nigeria. He obtained his Bachelor of Engineering degree from Kwara State University in 2016. He completed his Master of Engineering degree at the Federal University of Technology, Akure, in 2019. He is currently a Lecturer at the Federal Polytechnic, Offa, Kwara State, Nigeria.

Engr Ibiyeye's research interests focus on Artificial Intelligence (AI) and sustainability. He is registered with the Council for the Regulation of Engineering in Nigeria (COREN).