Journal of the Nigerian Association of Mathematical Physics
***Volume 59* (January – March *2021 Issue*), pp157 – 164**

IMPLEMENTATION OF INTERNET PROTOCOL BASED VIDEO SURVEILLANCE SYSTEM WITH REMOTE VIEWING FEATURES

Mathew Olajide[1], Alexander Okandeji[2], Zaid Jagun[3], David Kuponiyi[4] and Steven Ukagu[5]

[1]Department of Electrical/Electronic Engineering, Olabisi Onabanjo University, Ogun State, Nigeria.
[2]Department of Electrical/Electronic Engineering, University of Lagos, Akoka, Lagos State, Nigeria
[3]Department of Computer Engineering, Olabisi Onabanjo University, Ogun State, Nigeria.
[4]Dept. of Electrical/Electronic Engineering, Gateway (ICT) Polytechnic, Saapade, Ogun State Nigeria.
[5]Dept. of Electrical and Computer Engineering, Igbinedion University, Okada, Edo State, Nigeria

Abstract

This work considers the design and implementation of an Internet Protocol (IP) based surveillance security system. In this design, the proposed IP cameras are IP addressable, thus they can be accessed from anywhere in the world via the internet or any wide area network provided the user has the sufficient network and security privileges to access the camera. The IP camera is connected directly to a Local Area Network and transports digital video signals across the network via Unshielded Twisted Pair cabling (or by wireless means), to any computer or server on the network which views the video feeds, receives and records the video footage for future use. Results obtained showed that the field of view for known and unknown persons can be determined mathematically thus, IP video surveillance offers great details on flexibility, remote access and remote control and can be easily deployed as it is appropriate for securing homes, industries and offices.

Keywords: Internet protocol, camera, wireless network, digital video signals, Local area network

1.0 Introduction

The geometric advancement in technology is increasingly causing a corresponding revolution in all areas of human endeavors. More commonly, in recent times, technology is used not only to proffer solution to problems but also to improve the pre-existing solutions to a problem. The world of technology is a very dynamic environment as a result of continuous research work embarked upon by researchers from both the university and the industry. Consequently, systems previously celebrated and highly instrumental in meeting human needs are fast becoming obsolete as they are gradually being edged out by newer developments. For instance, typewriters and fax machines have been replaced by computers, and old fashioned analogue film cameras have almost been completely replaced by digital cameras [1].

As the world is rapidly changing, security technology must therefore evolve to keep pace with the sophisticated threats. Most security agencies in developing nations still depend on human efforts in its capacity to combat crime. However, with the exponential rise in crime rate and security challenges, human resource and efforts must be augmented by security and surveillance solution that leverage on technological advancements for effective development. Market trends report from the industry support the fact that surveillance systems have moved from traditional analogue into digital, and internet protocol (IP) based technologies with access applications that are hardware independent and operate by mobile and wireless technologies [1]. Conventional surveillance use the closed-circuit television (CCTV) monitoring system. CCTV is a television system in which signals are not publicly distributed but are monitored primarily for surveillance and security purposes. The drawback of CCTV systems is that they rely on strategic placement of cameras, and observation of the camera's input on monitors [2]. Because the cameras communicate with monitors and/or video recorders across private coaxial cable runs or wireless communication links, they gain the designation "closed-circuit" to indicate that access to their content is limited by design only to those able to see it [2]. Closed-circuit television, also known as video surveillance, is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. It differs from broadcast

Corresponding Author**:** Alexander O., Email: aokandeji@unilag.edu.ng, Tel: +2349039383220

television in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint (P2MP), or mesh wireless links. Though almost all video cameras fit this definition, the term is most often applied to those used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, and convenience stores [3]. In contrast to CCTV systems, IP surveillance refers to a security system that presents to a user, the ability to monitor and record video/audio over an internet protocol based computer network such as a local area network of the internet [3].

Fig.1 Schematic diagram for IP surveillance system (Image courtesy en.wikipedia.org)

IP surveillance sometimes also known as network video or IP CCTV uses the IP network technology as the backbone for transporting information. As a result of the digital nature and method of video distribution, IP based surveillance system introduce a host of advanced functionalities that enhance greater control and management of live and recorded video data thereby making them highly suitable for security surveillance applications. Some of these include remote accessibility, high image quality, scalability, flexibility, cost effectiveness etc. [3].

In contrast to existing works, the aim of this work is to design and implement an IP based video surveillance system with remote viewing features. In particular, the IP based video surveillance system incorporates remote viewing and storage of live video feeds, and also remote motion control of the camera, all monitored with the use of a Personal Computer (PC) giving rise to the possibility to view cameras from different locations with very excellent quality images. A schematic diagram for IP surveillance system is shown in Figure 1.

2.0 Theoretical Analysis

In the proposed system, for a typical IP video surveillance system which is PC controlled (using serial communication for the interfacing), IP cameras are used. The cameras are IP addressable, thus they can be accessed from anywhere in the world via the internet or any wide area network (WAN), provided the user has the sufficient network access and security privileges to the camera. The IP camera is connected directly to a Local Area Network (LAN) and transports digital video signals across the network via Unshielded Twisted Pair (UTP) cabling (or by wireless means), to any PC or server on the network which views the video feeds, receives, and records the video footage for future use. The network over which the camera transports the digital video signal is entirely wireless, thus the PC on which surveillance footage is viewed is not limited to a particular position. As long as the PC is within the coverage area of the wireless network, video surveillance can be viewed on the PC irrespective of location. Also, smart phones and Personal Digital Assistants (PDA) with wireless fidelity (Wi-Fi) capabilities can be used to view video footage from the camera, thus providing increased flexibility. The component used include cameras, network video recorder (NVR), connecting cables, router (with internet access). The proposed system is also provided with solar power so as ensure uninterrupted power supply and provide twenty-four hours' surveillance of the area. Figure 2 shows the block diagram of the proposed system.

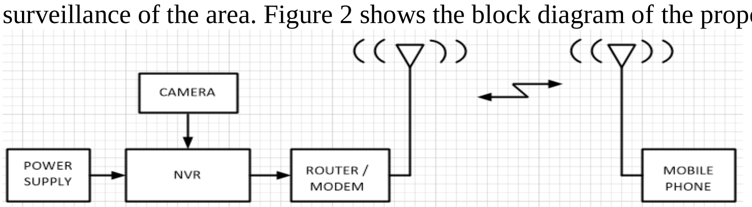

Fig. 2 Block Diagram of IP Based video surveillance system

2.1 Principle of Operation

In general, IP cameras capture images in much the same way as a digital camera, and compress the files to transmit over the network. IP cameras may be used with a wired network connected via Ethernet cable to a broadband modem or router, or wirelessly via a wireless fidelity (Wi-Fi) router. An IP camera captures and sends video footage over an IP network, allowing users to view, record, store, and manage their video surveillance images either locally or remotely over the network infrastructure. This IP security camera can be placed wherever there's an IP network connection. It has its own IP address and unlike a webcam, doesn't require a connection to a PC in order to operate. Along with streaming video footage, IP network cameras can include a number of additional functionalities such as pan/tilt/zoom operation, motion detection, audio surveillance, integration with alarms and other security systems, automated alerts, intelligent video analytics, and much more. Many IP cameras can also send multiple streams of video using different compression technologies for live viewing and archiving [3].

3.0 Experimental Work

3.1 General Overview of the Section

The block diagram of the proposed design as shown in Figure 1 consist of 5 blocks with arrow lines showing the direction of communication within the system. The blocks are described below.

3.2 Power Section

The power section oversees the provision of electrical energy needed to power up the system. The system makes use of a hybrid power system which include power supply by PHCN (mains) and Solar power system (solar).
The setup for the power section is shown in Figure 3.

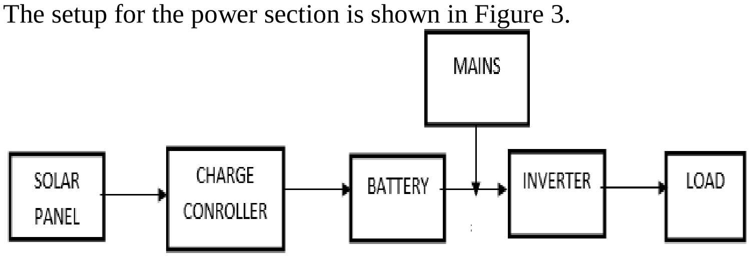

Fig. 3 Block Diagram of Power Section

The load in Figure 3 simply represents the IP video surveillance system. The inverter is incorporated with relay which provides automatic switching between the mains and solar on interruption or restoration of power supply (mains). The power consumption of appliances is generally given in Watts; it is necessary to determine the power consumption of the design. Table 1 shows the component part of the system and their current, voltage and power rating.

Table 1. Power Consumption of Design Components

Component	Power(w)	Hours/day (h)
Camera	24	24
NVR	45	24
Router	12	24
Lighting	100	12

The daily ampere per hour of each component is thus calculated as given below:

$Amp\_hour\ load\ =\ (power/voltage)\ x\ hours\ of\ operation\ per\ day(h)$...(1)

Where the operating voltage of the camera, NVR, router, and lighting are 12V, 48V, 12V, and 230V, respectively.
Table 2 shows the calculation of daily amp-hour of each component.

Table 2. Amp-hour of each component

Component	Calculation	Ah (1 day)
Camera	(24/12) x 24	48
NVR	(45/48) x 24	22.5
Router	(12/12) x 24	24
Lighting	(100/230) x 12	5.23
Total		99.73

It is worth noting that this work was carried out at the College of Engineering and Environment studies, Ibogun campus, Olabisi Onabanjo University, Ogun State, Nigeria. Thus, the following data was obtained.

Efficiency and loss-corrected load (AH (corr)):

$$\frac{99.73Ah}{0.8} = 124.66AH$$

Worst case equivalent sun hours (ESH) for Ibogun campus is 3.5hours

Solar array current requirement: $\frac{124.66Ah}{0.8} = 35.62A$

Using Roy solar 150w monocrystalline solar panel (10.99A @ 22V);

The numbers of panels needed = $35.62/10.99\ = 3.24$ panels

Approximately, the number of panels needed is 4 panels.

Autonomy or reserve time:

Choosing a day of autonomy with 80% maximum discharge: $1\, x \frac{124.66}{80}\% = 155.8Ah$
Using MBH 200AH, one battery is needed to provide the required autonomy: $155.8/200 \approx 0.8$
The solar powering system and the mains (i.e. power supplied by the utility providers) are both connected to the inverter. They are connected through a relay in such a manner that the relay performs automatic switching between the two, such that only one of the supply is allowed to feed the load at a time.

3.3 Camera

IP-based CCTV systems are designed to provide the ability to monitor, record, and stream video over a network to computers or other equipments. The system can use existing local area networks (LANs), wide area networks (WANs), and/or wireless LANs (WLANs) to save on installation costs. However, for added security, an organization could install its own private area network (PAN) cabling and support hardware. Power over Ethernet (PoE) technology is also an option within an IP-based system to increase savings and reliability. PoE enables various networked devices to receive power and data through one standard cable, which can offer significant cost savings when designing CCTV systems. A typical dome camera is shown in Figure 4.

Fig.4 Dome camera (Image courtesy en.wikipedia.org)

Dome camera is a type of camera which is mostly used indoor. Dome camera has 120 degrees' coverage area. Since the NVR has PoE, the camera was powered via the RJ 45 interface instead of using the direct current (DC) inlet. The camera was powered and connected to the NVR via Cat 5E cable. Category 5 cables can be used to carry frequencies of up to 100 megahertz (MHz) and handle data rates up to 1,000 megabytes per second (Mbps). The cables are terminated with an RJ45 connector. Table 3 shows cables of the cat 5E for input/output connector.

Table 3: Termination of Cat 5E cable

Name	Cable color	Function
12V DC	Brown/White	DC 12V.
GND	Blue/White	Ground
NC	Purple/White	Not used
NC	Gray	Not used
DI	Green/White	Digital signal input
DO	Orange/White	Digital signal output

3.3.1 Installing the Camera

The cable trunks were first put in place. Then the cables were laid from each camera to the NVR port, after which the camera was installed. The following were considered during installation.

3.3.1.1 Justification for camera lens

Choosing the correct camera lens in this study is more critical than in many other types of system. There are many IP based surveillance system in operation that are less effective, this could be due to insufficient information on the applied camera. Selecting the correct camera lens, the following real life situation must be considered:

I. **Field of view (FOV)** - Area under inspection that the camera needs to acquire.
II. **Smallest feature** - The size of the smallest feature that needs to be detected in the image.
III. **Working distance (WD)** - Distance from the front of the lens to the object under inspection.

The justification for camera lens selection is shown in Figure 5 and Figure 6.

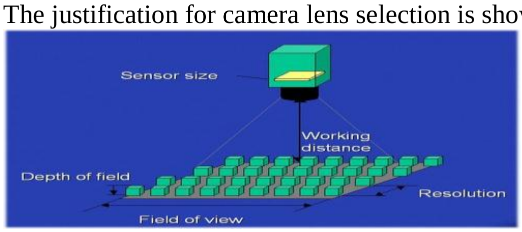

Fig. 5: Justification for camera lens selection (Image courtesy en.wikipedia.org

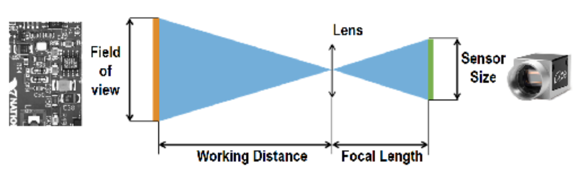

Fig. 6: Justification for camera lens selection (Image courtesy en.wikipedia.org)

IV Select the minimum required camera resolution and determine the correct focal length for the given application. This is achieved by:

i. **Calculating the minimum sensor resolution:** Knowing the field of view and smallest feature to be detected.
ii. **Selecting a camera:** Once the camera is selected, the sensor size can be used to calculate the focal length.

Figure 5 and Figure 6 justifies the selection of a particular camera lens based on (i)-(iv).

3.3.2 Sensor Resolution:

The resolution of an image is the number of pixels in the image. This is in two dimension; for example, 640X480. The calculations can be done for each dimension separately; but for simplicity, this is often reduced to one dimension. To make an accurate measurement of the image, there is a need to use a minimum of two pixels per smallest feature of the image that needs to be detected. To do the calculation for the minimum sensor resolution, multiply two (pixels/smallest feature) times the size (in real-world units) of the field of view divided by the size of the smallest feature as shown in the following equation [3]:

$$Sensor\ Resolution = Image\ Resolution = 2\left(\frac{Field\ of\ view\ (FOV)}{Smallest\ Feature}\right) \quad \text{.. (2)}$$

The area of the office used for this study is measured as follows:

- Length = 1.2192 m
- Breath = 0.9144 m
- Height = 3.0 m

3.3.3 Determining the Viewing Area or Field of View (FOV).

In this study, the major goal is to identify a person's face, or just detect a person walking far away. The first thing is to understand that the number of pixels per ft. (or per m) which determines the details of what can be seen [4]. The higher the resolution of the IP camera, the wider the area that can seen at a specific pixel/ft. When there are, enough pixels covering a person's face, such person can be recognized [4]. The lens makes it possible frame the field of view. A lens that allows the user to see an area 10 ft. (3 m) away or a different lens that magnifies an area that's over 10,000 ft. (3048 m) away [5]-[7] can be selected.

The lens controls how wide the field of view will be. The wider the field of view, the less pixels per ft (or meter) is obtainable. In Figure 7, the line is broken into small sections or horizontal pixels. The more elements per distance (pixels/m or pixels/ft.), the more details of what can be seen. As the lens is adjusted to provide a wider view, the number of pixels/ft. (m) decreases and the less the details that can be seen [6].

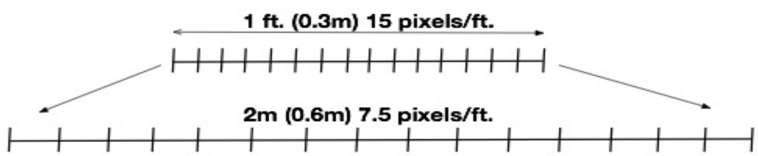

Fig.7: Field of view

The resolution required to identify a person's face will be determined with good light. A user requires about 80 horizontal pixels/ft. (260 pixels/m) to identify a known face. However, a lot more resolution is needed to identify an unknown person. Specifically, this could be about 150 pixels/ft. (492 pixels/m) [9]. To calculate the widest field of view, divide the number of horizontal pixels (available from the camera) by the desirable pixels/ft. As given in [9], the field of view can be determined by:

$$Field\ of\ Fiew = \frac{Total\ Horizontal\ Resolution}{Pixels\ Per\ ft.} \quad (3)$$

Table 4 present a list of common IP camera resolutions and their respective pixel with FOV using resolution to determine a person's face.

Table 4. Types of IP camera with their resolutions.

Types of IP camera	Horizontal Resolution	Vertical Resolution	FOV(for known person 80- pixels/ft) ft	FOV(for unknown person- 150 pixels/ft) ft	FOV(for known -person 80 pixels/ft) m	FOV(for unknown- person 150 pixels/ft) m
1MP	1280	720	16	8.53	4.8768	2.60096
1.3MP	1280	1024	16	8.53	4.8768	2.60096
2MP	1920	1080	24	12.80	7.3152	3.90144
3MP	2048	1536	25.6	13.65	7.80288	4.161536
4MP	2688	1520	33.6	17.92	10.24128	5.462016
6MP	3072	3072	38.4	20.48	11.70432	6.242304
8MP	3840	3840	48	25.60	14.6304	7.80288

The office dimension used for the study area has a length of 1.2192m as stated above, while the data analyzed from Table 1 justified our selection of camera of 2MP used for this study, and FOV for known and unknown person was 7.3152m and 3.90144m, respectively. These parameters were greater than length of the office used.

3.3.4 Calculating Distance based on the Camera Lens Angle

To calculate the distance based on the details required to be seen, the best way is to measure the distance using trigonometry. We start with the angle of the lens mounted on specific cameras. The lens plus the sensor size determines the actual angle so we rely on the angles provided by the camera manufacturer or the lens manufacturer. We can use the segment of a circle or a right-angle triangle to calculate the distance from the camera. The circle segment is more accurate, but the triangle method is easier because we can use a right-angle triangle. We make use of a 30-degree lens, 2-megapixel camera in this study. The resolution of the camera sensor is typically 1920 (H) x 1080 (V) pixels. It is our desire to identify a known face so we need 80 pixels per ft. To achieve this, we follow the steps outlined below:
Step one is to draw a triangle with the peak of the triangle at the lens, and the base at the field of view. To make the calculations, split the triangle into two right triangles 30^0. The right-triangle calculator will be used to calculate the distance to the viewing area. From Table 1, the 2-megapixel camera provides a maximum width of 24 ft (7.3 m). Since we cut the triangle in half, the opposite side (O) is equal to 12 ft (3.7 m).
Suppose the selected camera has a variable lens, and we decide to set the lens at 30-degrees, cut that in half equals 15-degrees. Using the right-angle triangle calculator, it is seen that the hypotenuse side (H) is 46 ft. (14 m) away from the camera lens. The adjacent length is the same distance as working distance (WD) which is calculated as 13.52m. Figure 8 shows the camera lens angel.

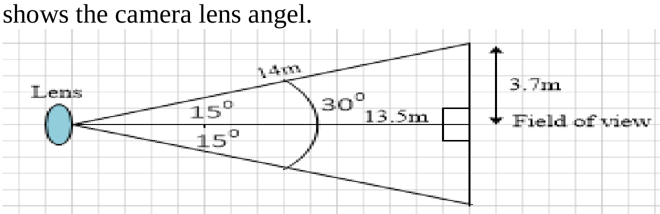

Fig. 8: Camera Lens angle

Table 5 shows the other specifications for the chosen camera as described by the manufacturer includes:
Table 5. Camera specifications

Features	Specification
Lens size	2.8mm
Lens type	Fixed lens
Resolution	2mp
Max. FPS and resolution	30fps at 1080p
Night vision range	98ft
Compression	H.264, MJPED
Sensor size	1/2.8”
Video bit rate	32kbps – 8Mbps
Image resolution	1920 x 1080
Power supply	12 DC ,PoE (5.3w)

3.4 Network Video Recorder (NVR)

NVRs record digital video data transmitted over an IP network from multiple CCTV digital cameras. NVRs can be configured to record video in a digital format to a disk drive, portable storage device or a mass storage device [5]. NVRs differ from digital video recorders (DVRs) as video input is delivered from an IP network. With an NVR configuration, video is encoded and processed at the camera and streamed to the NVR for storage or remote viewing [2]. Coupled with the NVR is the PoE and the hard dick (which provides storage space).

3.4.1 Calculating the Storage Need

In order to appropriately calculate the storage requirements of a network surveillance system, there are a number of elements to be considered. These elements include number of cameras required in the installation, the number of hours a day each camera will be recording, how long the data will be stored, and whether the system uses event triggers such as video motion detection or continuous recording. Additional parameters such as frame rate, compression, image quality and scene complexity will be considered. The type of video compression employed also has effect on storage calculations. The H.264 compression format is by far the most efficient video compression technique available today [6]. With a compression of high quality, an H.264 encoder can reduce the size of a digital video file by more than 80 percent compared with the motion JPEG format, and as much as 50 percent more than with the MPEG-4 standard. This means that less network bandwidth and storage space are required for an H.264 video file. With motion JPEG, storage requirements vary depending on the frame rate, resolution, and degree of compression. With H.264 and MPEG-4, bit rate is the key factor in determining the corresponding storage requirements.

3.4.2 Video Compression Format in H.264

The video compression format in H.264 is given by
Bit rate / 8 (bits in byte) x 3600s = Kilobyte (KB) per hour / 1000 = Megabyte (MB) per hour
MB per hour x hours of operation per day / 1000 = Gigabyte (GB) per day
GB per day x requested period of storage = storage needed
It should be noted that the values in Table 6 are based on lots of motion in a scene. With fewer changes in a scene, the values can be 20 percent lower. The amount of motion in a scene can have a massive impact on the storage required. Table 6 shows the amount of storage needed for two cameras.

Table 6. H.264 Calculation Table

Camera	Resolution	Image size (KB)	Frames per second	MB / hour	Hours of operation	GB / day
No. 1	CIF	110	5	49.5	24	0.4
No. 2	CIF	1250	15	112.5	24	0.9

Calculated Total for the 2 cameras and 30 days' storage = 39GB

3.4.3 Video Compression Format in MPEG -4

The video compression format in MPEG-4 can be calculated as shown below:
Bit rate / 8 (bits in a byte) x 3600s = KB per hour / 1000 = MB per hour
MB per hour x hours of operation per day / 1000 = GB per day
GB per day x requested period of storage = storage needed
The above formula does not take into account the amount of motion, which is an essential factor that can influence the size of storage needed. Results for MPEG-4 calculation are shown in Table 7.

Table 7 MPEG-4 Calculation Table

Camera	Resolution	Bit rate (Kbit/sec)	Frame per second	MB/hour	Hours of operation	GB/day
No .1	CIF	170	5	76.5	8	0.6
No. 2	CIF	400	15	180	8	1.4

Calculated total for the 2 cameras and 30days of storage = 60GB

3.4.4 Video Compression Format in Motion JPEG

The calculations for the video compression format in motion JPEG are shown below:
Image size x frames per second x 3600s = KB per hour / 1000 = MB per hour
MB per hour x hours of operation per day / 1000 = GB per day
GB per day x requested period of storage = storage needed. Results for JPEG video compression format are shown in Table 8.

Table 8. Calculation motion JPEG Table

Camera	Resolution	Bit rate (Kbit/sec)	Frame per second	MB/hour	Hours of operation	GB/day
No .1	CIF	13	5	234	8	1.9
No. 2	CIF	13	15	702	8	5.6

Calculated total for the 2 cameras and 30days of storage = 225GB

3.4.5 Video Management Software

Video management software is a key component of any video surveillance solution. It is the software that provides the tools for recording, monitoring and analyzing surveillance footage. While a standard web browser often allows for remote viewing, dedicated video management software is required for viewing and managing of multiple cameras at once [9]. The most basic IP surveillance camera software provides live viewing, recording, and retrieving of video footage. More advanced NVR software platforms offer simultaneous viewing of multiple cameras, and multiple recording modes (including continuous, scheduled, and triggered recording). Other features may include the ability to handle large image files with high frame rates, fast search capabilities, pan/tilt/zoom control, audio support, and remote access via web browser as well as cell phones and other handheld devices. Some software programs also support intelligent surveillance using sophisticated video analytics such as facial recognition and advanced motion detection.

3.5 Router and Modem

In technical terms, a router is a Layer 3 network gateway device, meaning that it connects two or more networks and that the router operates at the network layer of the OSI model [3]. Routers connect a modem via a fiber, cable, or DSL modem to other devices to allow communication between those devices and the Internet. Most routers, even wireless routers, usually feature several network ports to connect numerous devices to the internet simultaneously.

Typically, a router connects physically, via a network cable, to the modem via the "Internet" or "WAN" port and then physically, again via a network cable, to the network interface card in whatever wired network devices available. A wireless router can connect via various wireless standards to devices that also support the particular standard used. The IP address assigned to the "WAN" or "Internet"

connection is a public IP address. The IP address assigned to the local network connection is a private IP address. The private IP addresses assigned to a router is usually the gateway for the various devices on the network [3]. Wireless routers, and wired routers with multiple connections, also act as simple network switches allowing the devices to communicate with each other. For example, several computers connected to a router can be configured to share printers and files amongst themselves.
A router is the first line of security from intrusion into a network. Enabling the highest level of security on the router is the best way to keep the computer system and information safe from attack. Routers often act as the DHCP servers in small networks, issuing unique IP addresses [3].

4.0 Results and Discussion

The cameras were viewed remotely form different areas in Nigeria. Table 9 shows the location where the cameras were installed, and the different locations from where the camera was viewed. Figure 9 and Figure 10 shows the video feed from Fashina and Oshungboye area of Ibogun, Ifo, Ogun State, Nigeria.

Table 9. Results

S/N	Location of camera	Viewers Location	Image quality
1	OOU Campus Ibogun ogun state	Ikorodu area Lagos state	Good
2	OOU Campus Ibogun ogun state	Abeokuta area Ogun state	Good
3	OOU Campus Ibogun ogun state	Bariga area Lagos state	Good
4	OOU Campus Ibogun ogun state	Oshungboye ibogun Ogun state	Bad
5	OOU Campus Ibogun ogun state	Fashina ibogun Ogun state	Good
6	OOU Campus Ibogun ogun state	Ifo ogun state	Good
7	OOU Campus Ibogun ogun state	Songo ogun state	Good
8	OOU Campus Ibogun ogun state	Iyanpaja lagos state	Good

Fig 9: Image of video feed from Fashina area Ibogun

Fig 10: Image of video feed from Oshungboye

4.1 Discussion

Several tests were carried out on the system to confirm the level of its performance and efficiency. The IP surveillance system was viewed remotely from different locations to measure the efficiency of the system. It was observed that the live feed when viewed from most remote areas were of good quality due to strong network coverage. From the results, it was observed that the cameras can be viewed remotely provided that the two conditions below are satisfied;

I. There is internet access at the router (surveillance system)
II. The viewer has internet access on his or her mobile device.

5.0 Conclusion

IP-based video management platforms allow users added flexibility and control of a surveillance system. As additional features are integrated into the system, it creates a more total solution for the security needs of an organization. Consequently, the idea of IP video surveillance with great details on flexibility, remote access and remote control is interesting and can be deployed as it can be used to effectively secure homes, industries and offices.

References

[1] Karimaa, A. (2011). "Mobile and wireless access in video surveillance system," *International Journal of Digital and wireless communications*, (IJDIWC) **1**(1): 267-272.
[2] Saver. 2013, CCTV-Tech handbook . In Saver, CCTV hand book. pp. 34-35.
[3] Ruichao, L., Jing, H., Lianfeng, S. (2009). "Design and Implementation of a Video Surveillance System based on 3G network." In proc *wireless communications amd signal processing conference*., pp. 1-4.
[4] Fullerton, E. (2008). "The history of video surveillance," A milestone systems white paper.
[5] Chen, Y., Hu, R., Xiao, J., Wang, Z. (2019). "Multisource surveillance video coding with synthetic reference frame," *Journal of visual communication and image representation,* Vol. 65, Article 102685, pp. 123244-123254.
[6] Du, L., Zhang, W., Fu, H., Ren, W., and Zhang, X. (2019). "An efficient privacy protection scheme for data security in video surveillance, "*Journal of visual communication and image representation*, Vol. 59, pp. 347-362.
[7] Sharleen, J. Y., Cedric, A. M., and Wilson, M. T. (2019). "An SDN-based framework for improving the performance of under provisioned IP surveillance networks," *Journal of Network and Computer applications*, Vol. 132, pp. 49-74.
[8] Amira, B. M., and Ezzeddine, Z. (2018). "Abnormal behavior recognition for intelligent systems: A review" *Expert systems with Applications,* Vol. 91, pp. 480-491.
[9] Cermeno, E., Perez, A., and Siguenza, J. A. (2018). "Intelligent video surveillance beyond robust background modeling," *Expert systems with Applications*, Vol. 91, pp. 138-149.