INTERNATIONAL JOURNAL OF RECENT TRENDS IN ENGINEERING & RESEARCH
Impact Factor 4.101 ISSN -2455-1457
RECENT ADVANCES IN ELECTRONICS & COMMUNICATION ENGINEERING (RAECE-2K17)

Analysis Of Physical Parameters Using Embedded Programmable Operating System

K PRANUSHA
STUDENT, ECE Department
Nalla Narasimha Reddy Educational Society's
Group of Institutions

A SUSHMA
STUDENT, ECE Department
Nalla Narasimha Reddy Educational Society's
Group of Institutions

Abstract—In the last decades, monitoring cameras begin to play a vital role in securing sensitive systems such as government sites or establishments. Generally, these kinds of cameras are fixed-location (i.e. outdoor camera) such that the viewpoint is limited to small area and not covering the whole place. In addition, there are some drawbacks that appear when using these kinds of cameras such as being breakable (intentionally or not) which may lead to camera malfunction or breaking in the linked electrical wires that may cause disconnection between the camera, monitor and its receiver. However, the main problem is the lacking of secure protecting system that prevents intruders from entering into the system disabling or malfunction it.

In this research a new system is proposed in order to solve these problems by using wireless-mobile camera with embedded programmable operating system which enables controlling this camera remotely by sending wireless commands through the embedded component called *Arduino* card controller. This card enables the connection between the camera and the server to be programmatic by the user or developer. The main goal of this research is to design a monitoring system to detect any suspicious events and to ensure that the transferring monitoring data from the camera to the server is not infiltrated by unauthorized person by applying a set of techniques from image detection, object tracking and security algorithms to the instructions or the program of the camera. Compared with other researches, this work achieved the following goals: 1- Using *Arduino* card for programming the camera. 2- IP camera does not require user name and password. 3- The images and the other information are (encrypted) when sending to/from computer, 4- Using Mobile-wireless camera. 5- Process of keys exchanging between camera and computer. The results of this research are good and achieved the main goals of new developed technique.

Index Terms—Wireless camera, Arduino card, Surveillance, Monitoring system, IP camera, CCTV systems, Video encryption.

INTRODUCTION

A surveillance system is a collection of processes dedicated to monitor the actions of people, things or processes of sensitive systems to ensure that the system is working correctly and to take the necessary actions in case of incidents or intrusion. For this reasons it is necessary to choose high quality cameras with high resolution to provide excellent view or the specified area. In addition these systems should have the ability to record, monitor (for a long time) and archive the events for many areas in order to restore and view them easily at any time by using either Digital Video Recorder (DVR) in case of ordinary camera or Network Video Recorder (NVR) in case of using network and IP camera [1]. The cameras may be stationary or may rotate in different directions to achieve more coverage of activities in an area. Such rotation of cameras is achieved with the use of DC motors or stepper motors [2].

In fact, surveillance systems depend on operators which often work in a room with lots of monitors and their task is to constantly watch the monitors. If incidents happen, they warn the security or police. Some monitors show the video stream of a single camera and some show multiple streams on a single monitor simultaneously or sequentially. However, in some areas video recorders record the output of each camera which can be used as footage in case of incidents. One obvious disadvantage of this approach is that operators are not able to prevent incidents or limit their damage, since the videos are only watched afterwards. Another disadvantage is that it takes a significant amount of time to search for the right video images, especially when the suspect arrives at the scene hours before the incident and a large number of cameras are involved [2].Current surveillance system replaces (partially or totally) human operators by automatic intrusion detection system. Some of them consist of an array of sensors, a control panel and alerting system. Sensors detect intruders by infrared motion detectors (active and passive types), ultrasound motion detectors etc. The sensors may be directly wired to a control panel

that provide sensor power, or may communicate wirelessly [3]. Using the active infrared as a sensor to detect intrusion has advantages of fast response, and is insensitive to mechanical and acoustics noise. However this system can only be used to detect intrusion in an idle area with no motion and does not provide facial recognition of the intruder [2]. Besides, there has been an existing monitoring system known as Closed Circuit Television (CCTV) which has been in use. A major setback with CCTV systems is its fixed nature and lack of flexibility. The monitor on which activities are viewed is always at a fixed position, thus for effective real time surveillance monitoring, the security personnel must always be at the position where the monitor is permanently stationed which is quit task if long hours are to be involved [4]. All the shortcomings of the already developed existing security systems are taken care of by the introduction of a PC based surveillance system and smart software based operators. In this system, a typical Internet Protocol (IP) video surveillance system which is PC controlled (using serial communication for the interfacing), IP cameras are used. Software operator uses some IT and computer science techniques of image processing, artificial intelligence and others in order to monitor, detect and alarm in case incidents occur. However, even these techniques could be threatened by intruders. For example it is possible for the intruder to inject pre-recorded video into the system to malfunction it especially in wireless camera as it is easy to connect any station inside the Wi-Fi shield and enter the system. The following sections give a brief description of the problem of this research and its solutions.

In this paper, a description of the proposed method is presented. The paper is structured as follows:

In section 2, a preview for the related work which this paper depends on is given. In sections 3 and 4 a description, comparison and the functional details of the IP camera are introduced. Section 5, 6 and 7 are related to the threat design and the main structure of the proposed system. Sections 8, 9 and 10 provide the implementation, advantages and analysis of the system and finally conclusion of the system is discussed in section 11.

I. Related Works

Since early decades, the human race in seeking new strategies to extend its viewing ranging is continuing in developing. With the rise of technology in the twentieth century, cameras are found to be a very useful tool to survey a large area with limited resources. As in many other application areas where digital devices have replaced their analog predecessors, manufacturers and consumers have been losing interest in conventional film cameras and have been turning instead to digital cameras. Users with the conveniences of digital cameras can record, store and manipulate photographs electronically using image sensors and built-in computers. Features such as displaying an image immediately after it is recorded, the capacity to store thousands of images on a small memory device and the ability to delete images from this device in order to allow its further re-use, and the ability to edit images and even record them with sound make digital cameras very attractive consumer electronic products [5]. However, with the increasing numbers of cameras it becomes more difficult to watch every monitor and prevent incidents in the surveillance area. For this reason, currently researches seek possibilities to automatize the process of video surveillance [1]. For example, security applications are increasingly migrating from analog to digital technology; meanwhile, the IT and security markets are rapidly converging. These two developments have led to increased interest and viability for IP network-based solutions and the use of the Internet [6].These new technologies are reflected on the process of developing monitoring cameras. Instead of using the previous simple systems which consist of one camera, a monitor and a person to control them for the whole time, the new surveillance system consists of many mobile-wireless cameras controlled by a dedicated program that controls the movements of camera, recording and storing of the data without the need for a person to control them the whole time.

With these developments many researches and articles have been published which are related to the security of surveillances system

Cletus et al. [2] designed an IP-based security surveillance system which 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).

Shortly forward, Maarten [7] gave an approach to emulate human operators in monitoring and watching by using techniques from Computer Vision and Artificial Intelligence P-N Learning to enable the tracker to learn from its mistakes. This model is designed to be able to detect suspicious behavior in a non-public area.

After that, Kil-sung et al. [8] made a project to transmit video information to HOST via Streaming Server or FTP server using IP by developing host-active application program. This program can retrieve video information from HOST with only IP camera's IP address. By installing cloud server in the HOST, where smartphone can send videos to it regardless of network realms such as Wi-Fi, LTE or AP and transfer smartphone's video information to cloud server anytime using wired or wireless networks and to save video information in designated directory, which was synced with Host's Private Cloud server, and it is found out that users can ubiquitously check whether video was saved using Private Cloud server.

In addition, Gradimirka et al. [9] made a study deals with the basic characteristics of the IP cameras uses in video surveillance systems and compares them with the analog ones. The IP video surveillance system multiview function mode was also studied. Furthermore, the study dealt with the IP camera power charge principles in the video surveillance systems via Ethernet in cases with and without PoE switch. This study proves that surveillance

concept based on video systems with IP cameras provides great efficiency and decreases the price of the system, since the existing computer network is used for transfer of audio and video signal within the system of video surveillance with IP cameras.

The next year, Abeer [10] designed a secure digital system for a building based on behavioural tracking to be able to determine activity and recognize normal/abnormal behaviours across a network of distributed cameras. This research depends on an automatic suspicious behaviour detection model and use multi-cameras to apply them into investigation through architecture design of smart environment into an academic environment to having a high degree of detection with a rate of a low false alarm for tracking person behaviour into video sequences.

In addition to academic researches ,many companies compete in producing the last solution for surveillance system such as: *Dahua* technology which is one of the world suppliers of video surveillance solutions ,Q-See which is also is a global leader dealing with supplying homes and offices with wireless CCTV solutions, premium digital video recorders, security cameras with exceptional night vision capabilities, and a wide range of accessories and LOREX system which provides efficient solutions for video security system. It offers a wide range of efficient and easy to set up security video systems for anyone who wants to do it alone. As easy as plug and play, most of their products come with easily connected DVRs and cameras for viewing over a Smartphone [11].

II. Common Types of Surveillance Cameras

In general, there two main types of surveillance cameras which are in common use:

A. Analog Cameras

An analog camera provides image information as continuous signal levels that are either displayed directly on monitors or that are digitized outside of the camera [12]. This type uses Charged Coupled Device (CCD sensor and then digitizes the image. However, it needs to convert it back to analog so it can be received by an analog device (i.e. monitor).These functions are done using recording and/or control equipment [13].

B. Digital Cameras

In a digital camera, the digitization of the image information is carried out inside of the camera after the image information is captured by a sensor. The transformation from an analog to a digital signal is performed by additional electronics inside of the digital camera, which are not available in an analog camera [12].This type can have either a Complementary Metal Oxide Semiconductor (CMOS) or CCD sensor. Table 1 lists the main differences between the two types.

Table 1. Comparison between Analog and Digital Cameras

Feature	Difference
PRICE	The latest digital solutions are price competitive with analog products
SYSTEM COST	Digital Power over Ethernet (PoE) cameras are robust, reliable and easy to maintain. Therefore costs are reduced.
Stability	Digital cameras have better stability over time and temperature.
NOISE IMMUNITY	Digital cameras are more resistant to electromagnetic noise.
PERFORMANCE	Digital cameras allow higher video performance than analog cameras.
ADVANCED FEATURES	The provision of advanced features is only possible on digital cameras. Force of habit may cause some users to miss the opportunities presented by the latest digital technology.
EASE TO USE	Digital cameras are much easier to customize than analog cameras.
SOFTWARE INTEGRATION	Many software packages are available that support fast and efficient integration of digital cameras into an application.
CABLE USED	Digital cameras with PoE can be connected with only a single cable.

III. The Functional Details of Ip Camera

What is commonly known as an IP camera is a camera that digitizes and processes analog images, encodes them internally and then transmits the video information digitally over Ethernet connection to a computer or similar device. An IP camera is typically equipped with an embedded web server and can be accessed and controlled over any IP network such as a WAN, LAN or Internet. IP camera employs an analog image sensor which is either CCD or CMOS (CMOS gives a high quality image over CCD).The analog signal from the sensor is then converted to digital using encoder and then compressed internally and transmitted via an IP protocol (Ethernet) and either stored in the camera or on a network video recorder(NVR). By utilizing a standard web browser the user can view an IP camera's video output from any local or remote location. IP camera combines the capabilities of a camera with some PC functionality and does not require a direct connection to a PC to operate and can be placed anywhere in the network [12].

The main characteristics of IP-based cameras:

1- Reliance in connectivity on any switch or router or other IP cameras.
2- Easy controlling the displays of cameras.
3- Ability to link these cameras to mobile and tablet where images are sent to these devices via the Internet

Typically, IP camera can be wired or wireless. Wireless camera is easy in installation in the location and is more comfortable to use. However the distance rate that these cameras could cover is lower that wired camera and they are more intercept able to intrusion than wired cameras. For that reason it requires employing a secure algorithm in order to protect its Wi-Fi shield.

But the downside of these cameras is that most of them use ready to write programs where come from the manufacturer such that the program which the camera works on could not be editable manipulated or changed but come on diskettes. However some companies produce cameras that their program could be edited such as *Arduino* Company and which is depended in the proposed system.

IV. Surveillance System Threats

From the study of the security of the surveillance camera we could list the main threats as:

1- Threats that occur because of the intruders that could enter the system and destroy it internally (the surveillance system) or externally (breaking the camera).
2- Threats that occur because of human mistakes (inability to watch every events correctly for 24 hours).
3- Threats that occur in the connecting media (break in wired cabling or noising waves in wireless).

There are many types of threats as describe below [15]:

1- Replay attack:

Replay attack is an attack method where the basic concept is to first record a valid message and then later replaying the same message. This method is used on systems that use constant authentication information, such as passwords or electronically transmitted biometric data. This attack could be reduced by adding some features to the system such as limiting the lifetime of a session. Another better solution is to use the old session identifier as an identifier for generating a new one. If this approach is used the clients identification information does not have to be sent to the server more than once, regardless of how long the user stays online.

2- Man in the middle attack:

In this type of the attack, the hacker could listen and inject data or messages into the session by taking the personality of one of the authorized users.He may also try to disconnect the session of one party and continuo as the disconnected party. The main goal of the man in the middle is to get the imprtant data or informtion by eavesdropping the connection or by directly by impersonating as a legal user.This attack is fairly easy to carry out if the system does not protect it assets very well such as not using encryption, authentication, integrity and other means.

3- Denial of Service attack (DoS):

DoS is one of most common attack that usually conducted to stop or (at least slow the provided service of the attacked system). This type of attack is done by fillling the target with data or message sthat are sent by the attacker to flood the system resources and cause the CPU to stop working or reset to conduct it .Another form of DoS attack is occurred in large system by involving a large numbers of computers in this attack at the same time, which is commonly known as zombie attack. IM systems is depend on the design of centralized servers are vulnerable to this kind of attack for many reasons such as just to cause annoyance or to block one party of the session.

Also there are many difficulties when apply security for example:

1. Applying security requires to understand the requirements of the system very well and expecting the various situations that may happen in the system under the whole frame of confidentiality, integrity and authentication.
2. When developing a security mechanism, it must be viewed from variety points of view to discover the weakness of the algorithm. Sometimes the attacker discovers a weakness in the algorithm that is far away from the viewpoint of the developer.
3. The statement problem is generally complex and could not easily interpret to a security mechanism.
4. When designing different security mechanisms, it is necessary to decide where to use them.
5. Security mechanisms involve more than a particular algorithm or protocol.
6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer who tries to close them.
7. There is a natural tendency on the part of users and system managers to get a little benefit from security investment until a security failure occurs.
8. Security requires regular and constant monitoring.

These threats and security problems are overcome in the proposed system in this research.

V. Design Criteria

The proposed system is mainly based on designing a secure multi-camera surveillance communication environment in a crowed surveillance area to monitor and track any suspicious events happening in this area. The main goal of the work is that the tracking information is secured in a way that the intruders could not view, edit and maintain the transmitting information among these cameras in addition to controlling the cameras. The reason for use multi camera is that it not possible for a single camera to monitor the whole area in order to track suspicious events happening in the chosen area. The main goals of the research include the following:

1- Design a system model that is capable of detecting suspicious behavior.
2- Covering the whole surveillance area by using mobile camera that could move 3600 degree.
3- Solving the cabling problems by using wireless camera.
4- Protect the video tracking information by encrypting it using an encryption algorithm.

5- Share this tracking information with other cameras in the environments in a secure way.
6- The camera is put in uneasy to see location so it would be invisible that it is protected it from destroying intentionally.

VI. PROPOSED SYSTEM STRUCTURE

The basic structure of the proposed system consists mainly of the following:

A. Digital Camera

The digital Camera is the main part of the system which depends in point's images for the produce of monitoring targets using the camera application. The type of the camera which the proposed system uses has linked camera type: (**Pixy cum5 US-made**) which have the ability to track colors and shapes us shown in Fig.1 below.

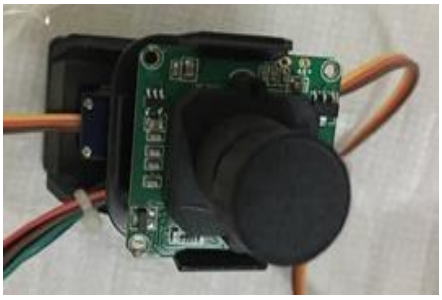

Fig.1. Digital Camera

B. Servo Motor Connection

There are several types of engines that are used to control rotation of the camera which depends on usage type. The proposed system uses a motor engine which could turn the camera 360^0 degree to cover the most remote area us shown in Fig.2 below.

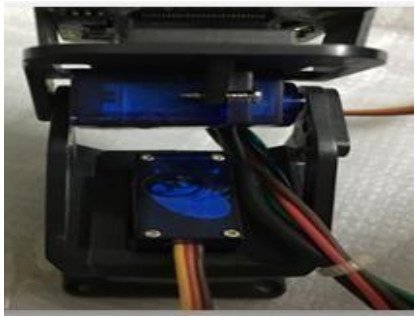

Fig.2. Servo Motor

C. Wi-Fi Shield

This is used for wireless connectivity. The proposed system is supposed to use Wi-Fi card from (*adafruit States Company*) to be 100% compatible with card *Arduino*. Using this card we can communicate with the server desktop computer through a router connection device us shown in Fig.3 below.

Fig.3. Wi-Fi Shield

D. Arduino Card

This is an electronic board that is considered to be open hardware for development. It is possible to add a lot of ideas and projects related to automatic control in an easy and simple way through the use of open programming language *(Arduino C*), the programming is controlling a board using a special program called *(Arduino IDE: Integrated Development Environment*), it's found in free download web *http:// Arduino.cc* [14]. There are many types of *Arduino* card. The proposed systems used (*Arduino Uno*) which is shown in Fig.4 below.

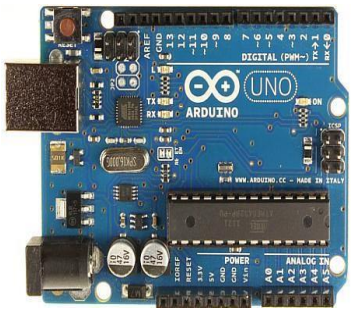

Fig.4. Arduino Uno card

VII. PROPOSED SYSTEM IMPLEMENTATION

The proposed system is based on cameras that use Arduino (Uno) card which available in the IT-market. This card resembles the motherboard for the camera which connects the main parts of the camera, the Wi-Fi adapter shield in addition to the transferring engine server and motion motor. This card makes the camera a smart device able to be programmed and developed by updating and editing its embedded operating system. The proposed system depends on developing the way of data transferring among these parts to be amenable to intrusion. The programming language used and approved by the card Arduino is the C language developed by the company. Fig.5. describes the architecture of the proposed surveillance system.

The type of the camera used is Pixy cum5 US-made, which has the ability to track colors, shapes and store their information in its internal storage. The proposed Meta libraries to manage the camera are (pixy.cpp, pixy.h) in C language. These libraries are equipped by the

manufacturer and found on its website. These libraries resemble the basic focus of the research goal which will be bounded with the main program in C# to insert security into camera instructions list.

Arduino Company launched a complete line of parts of the program for this type of cameras which are changeable ones and are compatible with the Arduino card including Wi-Fi card for the purpose of wireless connectivity which is supposed to use (adafruit) States Company and is compatible 100% with Arduino card. Using this card the camera can communicate with the server desktop computer through a router or other connection device.

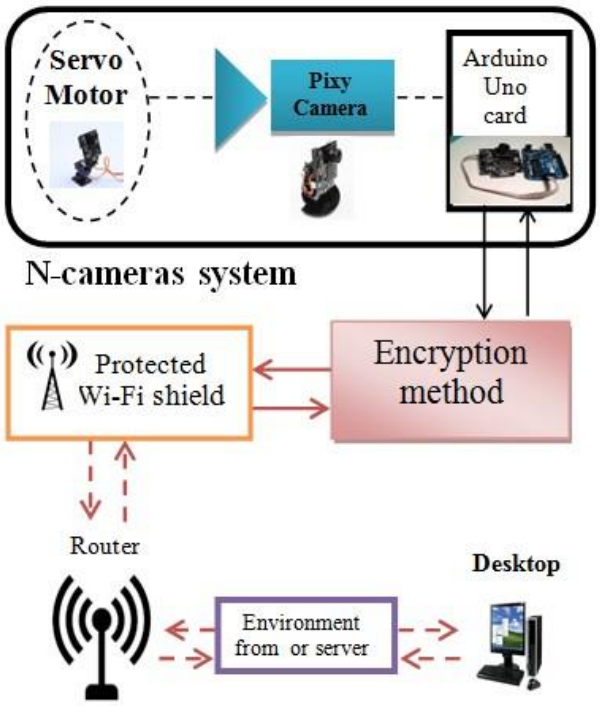

Fig.5. Proposed System Structure

In order to increase the surveillance area, a mobile camera should be used. This is done by binding the camera with moving engine and controlling its movements. There are several types of engines depending on usage type. The proposed system uses the two dimensional moving motor to move the camera horizontally. In this case a good integrated control scene could be achieved.

VIII. Proposed System Advantages

The proposed system provides many characteristics that can be listed as follows:

- The video and the tracking information are shared safely from intrusion through the system.
- The cameras are controlled automatically without any manual intervention.
- There are many instructions written at once to direct the camera in any direction or zooming.
- When cards Arduino are used with camera wireless prove succeeds because, this new method contain a security system to prevent the data moving from hacker.
- The camera is hidden and not visible to anyone trying to break (intruders).
- The use of multiple cameras allows us to see the place from different angles.

IX. Proposed System Analysis

From comparing the proposed work with previous regimes shown in [2][7][8][9][10] we notice that most of them do not provide security solutions for intrusion protection system while the proposed system does. In brief we could list the solutions which the proposed system introduces in table 2 below:

Table 2. Comparison of the Proposed System with Previous Works

Criteria	Proposed work	Previous work
Card Arduino	Using this card for programming the camera	Not found
IP Address	Not using user name and password	Uses User name and password
Data Encoded	The images and the other information are encoded (encrypted) when sending to/from computer.	A data direct sent without encoding
Movement	Using Mobile camera	Fixed/mobile camera
key Exchanging	The keys Exchange between camera and computer	There is no key used in these cameras
Wireless Connection	Uses a wireless to connect	Uses wire to connect

X. Conclusions

Surveillance systems reflect new possibilities with the continuously development in IT technologies. It is common that the main requirements that any surveillance system should give are: reliability, speed, flexibility and cost reduction. However, security is a primary concern everywhere to anyone and every system requires being secured. This research has presented an idea of secure surveillance system to provide flexibility, remote access and remote control with great care to security. This model is appropriate for securing sensitive industries and buildings. . The work depends on using PC based IP Surveillance Security System improved by using motor engine with a design of camera moving control mechanism In addition a techniques of motion detection and security scheme to protect the video and transferr data is also presented. So that the new IP systems of video surveillance could be easily and efficiently integrated with other systems such as sensitive building, access control, alarm systems and so on.

REFERENCES

[1] Marco Schwartz, "*Wireless Camera with Arduino and the CC3000 Wi-Fi Chip"*, Open Home Automation, 2013.

[2] Rahman M. and others, *"Microcontroller Based Home Security and Load Controlling Using Gsm Technology"*, I.J. Computer Network and Information Security, 2015.

[3] Zhang T., *"The Design and Implementation of a Wireless Video Surveillance System"*, 2015.

[4] Dahua technology, *"Video surveillance Solutions"*, Dahua Technology Co., 2015.

[5] Maureen A., *"Virtual Examination Supervision System for Nigerian Universities"*, I.J. Modern Education and Computer Science, 2016.

[6] Stewart B., *"Adventures in Arduino"*, John Wiley & Sons Ltd, the Atrium, United Kingdom, 2015.

[7] Maarten Somhorst, "*Multi-camera Video Surveillance System*", delft university technology, 2012.

[8] Kil-sung Park and Sun-Hyung Kim, research:"*A Research Using Private Cloud with IP Camera and Smartphone Video Retrieval*" Department of Information & Communication Engineering, Soonchunhyang University, Asan, Chungnam, Korea, 2014.

[9] Gradimirka Popovic1, Nebojsa Arsic1, Branimir Jaksic1, Boris Gara2, Mile Petrovic1 , "*Overview, Characteristics and Advantages of IP Camera Video Surveillance Systems Compared to Systems with other Kinds of Camera"*, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 5, September 2013

[10] Abeer Salim, "*Designing A Digital System for the Security of a Building Based on Behavioral Tracking*", University of Technology, Computer Science Department, 2015.

[11] Purdum J., *"Beginning C for Arduino"*, Ecosoft, Inc., Cincinnati, Ohio, USA, 2015.

[12] Björn Weber, whie paper: "*Analog vs. Digital Cameras*", basler IP-cam company, Germany, 2012.

[13] Amariei C., *"Arduino Development Cookbook"*, Packet Publishing Ltd., UK, 2015.

[14] AbdulAllah Ali, E. Book:" *Simply-Arduino*" , 2012.

[15] Student, "Security of campus Facilities and Crime Prevention", University of Dayton, 2015.

