American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-12, pp-58-69
www.ajer.org
Research Paper Open Access

# Security Devices Application Studies in Crime Prevention and Policing in Nigeria.

Olumuyiwa Oludare FAGBOHUN[1] and Olayiwola Ademola ONI[2]
[1]*Department of Electrical Engineering, Faculty of Engineering, Ekiti State University, Ado-Ekiti, Nigeria.*
[2]*Department of Civil Engineering, Faculty of Engineering, Ekiti State University, Ado-Ekiti, Nigeria.*

***ABSTRACT:*** *Crime prevention aims at presenting an unattractive target to criminals, by removing opportunities, and the studies of devices required to accomplish this task is the aim of this study. The different types of security devices available to reduce and deter crime is presented. A study was made on metal detectors, alarms, and closed circuit television networks systems among others and their areas of application highlighted. It was discovered that alarm systems, closed circuit television (cctv) and internet protocol ( ip) camera systems are generally suited for day to day security and crime protection, with the believe that the police and other government and private security outfits will find the study useful in their search for electronic packages of assistance in helping them in combatting the ever increasing crimes in our society.*

***Keywords****: Metal detectors, magnetometers, imaging systems, cctv and ip camera systems, burglar alarms, sensors, recording systems.*

## I. INTRODUCTION

Crime prevention is the attempt to reduce victimization and deter crime and criminals. The prevention and detection of crime are the basic core functions of every police force. Howeverthese functions should not be seen as the responsibility of the police alone, we should all have a role to play and we should all do our bit to minimize the possibility, that we become a victim of crime. For the most part, crime carriedout all over the world is against property not people, crime is often carried out on the spur of the moment, when criminals take advantage of opportunities that are presented to them for example an unlocked car, a house with a window or door left open or personal property left unattended [1]. Crime against humanity is termed terrorism [2]. The ultimate goal of crime prevention is to reduce risk of being a victim in order to accomplish this effectively, it is important to remove opportunities for a criminal to take advantage of you or your property. Attempting to prevent either victimization or criminalization by presenting unattractive target to the criminal, by removing opportunity is often referred to as target.There are numbers of different security devices available, e.g. cctv cameras security finger prints. X-ray machine, handheld device (body scanners), home security system, alarms, eye scanners, street security device, residential security device, industrial security device, monitoring system, sensors, and metal detectors.

## II. METHODS & MATERIALS

The area of applications of individual security devices was assessed with the advantages that can be derived over others, with respect to;

i. Homes and Residential security systems,
ii. Commercial security systems,
iii. Industrial security systems,
iv. Environmental security systems,
v. Urban areas and streets security systems
vi. On the spot security systems and vii. Vehicular security systems. the primary and secondary data were obtained from desk studies, with the various modern methods being employed in the state - of -art security systems highlighted.

## III. SECURITY DEVICES IN CRIME PREVENTION

### 3.1. Metal detectors:

A metal detector is a security device that detects metal either on a person's body or his / her luggage. They are various types of metal detector which are walk through metal detector and a hand held device. Metal detectors are mainly used in industries, banks [2,3]. Metal detector is a device which responds to metal that may not be readily apparent. The simplest form of a metal detector consists of an oscillator producing an alternating current that passes through a coil producing an alternating magnetic field. If a piece of electrically conductive metal is close to the coil, eddy currents will be induced in the metal, and this produces a magnetic field of its own. If another coil is used to measure the magnetic field (acting as a magnetometer), the change in the magnetic field due to the metallic object can be detected. A walk through metal detector is designed specifically for detecting small ferrous and non-ferrous items such as disposable prison blade, metal shanks, hand cuffs, detonator cap, jewel, coins, microprocessor, guns, knives and memory chips [1,2]. Almost all metal detectors are based on pulse induction (PI). Typical PI systems use a coil of wire on one side of the arch as the transmitter and receiver. This technology sends powerful, short pulses of current through the coil of wire. Each pulse generates a brief magnetic field. When the pulse ends, the magnetic field reverses polarity and collapses very suddenly, resulting in a sharp electrical spike. This spike lasts a few microseconds and causes another current to run through the coil.


**Figure 1:** A metal detector for scanning [2].

This subsequent current is called the reflected pulse and lasts only about 30 microseconds. Another pulse is then sent and the process repeats. A typical PI-based metal detector sends about 100 pulses per second, but the number can vary greatly based on the manufacturer and model, ranging from about 25 pulses per second to over 1,000.If a metal object passes through the metal detector, the pulse creates an opposite magnetic field in the object. When the pulse's magnetic field collapses, causing the reflected pulse, the magnetic field of the object makes it take longer for the reflected pulse to completely disappear. This process works something like echoes. In a PI metal detector, the magnetic fields from target objects add their "echo" to the reflected pulse, making it last a fraction longer than it would without them.A sampling circuit in the metal detector is set to monitor the length of the reflected pulse. By comparing it to the expected length, the circuit can determine if another magnetic field has caused the reflected pulse to take longer to decay. If the decay of the reflected pulse takes more than a few microseconds longer than normal, there is probably a metal object interfering with it.The sampling circuit sends the tiny, weak signals that it monitors to a device call an integrator. The integrator reads the signals from the sampling circuit [3,4,5], amplifying and converting them to direct current (DC).The DC's voltage is connected to an audio circuit, where it is changed into a tone that the metal detector uses to indicate that a target object has been found. A metal detector is really called a magnetometer (Magnet meter). A magnetometer produces a strong magnetic field [4,5,7]. Any metal objects passing through the magnetic field will react with the magnetic field and begin to conduct a very slight electrical current. This process is called induction [4,5]. These electrical currents cause their own much weaker magnetic fields. The magnetometer detects that new magnetic field and the interaction with the primary magnetic field it is producing. When the interaction reaches a certain per-determined threshold, the alarm is triggered. At this point officers will use hand-held magnetometers (known as wands) to pin-point the source of the alarm. The noise they make is an audible representation of the strength of the secondary magnetic fields produced by metal objects. Magnetometers can be so sensitive as to detect tooth fillings, titanium implants and other non-ferrous metals. Most metal detectors in airports are tuned so they are not triggered for tooth fillings or small metal implants like surgical pins. But they will be triggered by larger implants like knee replacements, and hip implants [3,6,8].

**Figure 2:** A metal detector for scanning [5].

### 3.2. X-ray screening machines:

**T**he machine functions by using a conveyor belt to pull or drive the vessel or bag that needs to be scanned into a chamber, in this chamber it sends a beam of x-ray capturing the image of the components in the bag, the data received is passed to a computer that analysis and processes the information to give a clear identification image for the user screener. X-ray machines are mainly at airports to screen passenger bags. Rapi scan x-ray system provides clear, high resolution monochrome and colour images of inspected items. Images can be enhanced bykeyboard selection of high and low penetration, inverse, video and zoom for a sector x 2, x 3 and x 4 magnification, further processing and enhancements of organic material and inorganic material. Shipping multi energy spectrum (MES) distinguishes between materials according to their inherent characteristics (electro densities) and classified by colours. Orange is used for low electron density,green for medium electron density, and blue for high electron density materials [7,9]. Most explosives and low electron density materials such as plastics, clothing and papers will be shown in orange, while medium electron density materials such as aluminum will be displayed in green. The high electron density material will be shown in blue. In situations where x-rays cannot penetrate an object due to combination of thickness and/or density, the image colour will be explosive (or the colour of selected material will be shown red).TIP (threat image production) is a special function that is present in a rapi-scan, it is embedded in the system and can be enabled or disabled. According to psychology when you are not concentrated at looking at a possible threat e.g. arms, drugs etc. A threat like a gun or more subtle cocaine could pass and the operator viewing the screen might not know due to brain fatigue, hence tip is set so that of a predator mixed time a fake alarm or fake threat is produced in the computer to test the operator alertness.

### 3.3. Closed circuit Television (CCTV) and ip Cameras:

The ideal cctv and ip camera system should provide excellent quality pictures in both daylight and darkness, be easy and flexible to use and provide high quality images for recording evidence or to help analyze an event. For deterrence, the potential burglars and thieves may see the camera and decide that the store in question is toomuch a risk and therefore not a good target. In prosecution, thieves and shop lifters may be caught on the camera and this can help catch and prosecute them.it is equally used to reduce fear of attack in that, If everyone knows that there is a camera they may feel safer in or around a business thus preventing potential criminals from attacking [10].In monitoring and intervention, if there is a security guard monitoring the area under cctv and ip camera system he or she may act on any suspicious behaviour and thus prevent crime from occurring, security guards may also deploy employees to a suspicious spot or near a person detected on the monitor [10,11].

**Table 1:** Some security devices applications in crime detection

| | Alarms | CCTV's | Metal detectors | X-ray Screening | Taut wire fence System | IP Cameras | Drones |
|---|---|---|---|---|---|---|---|
| Residential | * | * | | | | * | * |
| Industrial | * | * | * | * | * | * | * |
| Commercial | * | * | * | | * | * | * |
| Urban Networks | | * | | | | * | * |
| Environmental | * | * | | | | * | * |
| On the spot | * | * | * | | | * | * |
| Vehicular | * | * | | | | * | * |

* - applicable.

### 3.4. Working principle of a CCTV System

There are many different types of cctv systems available; analog and digital, wired and wireless and their modes of operation vary, however the basic components are in essence the same; a cctv camera, a cctv camera lens, a cctv monitor(for wired systems) and cables that carry the signals from one place to another.

The images collected are sent to the cctv monitor and recorded on video tape via a VCR or as digital information via a DVR (digital video recorder) [11]. A cctv camera lens will determine how far and how much detail the cctv camera can see. The cctv camera picks up the signal from the area being monitored and in a wired system, the cctv camera sends the signal through a coaxial cable to the cctv monitor. In wireless system no cable is needed instead the cctv camera broadcast the signal. Monitors can be watched by cctv controllers or left unmonitored. Recent advances in technology and software mean many cctvs are now equipped with advanced features such as motion recording and event notification. When set to motion, record devices will only record when the cctv cameras detect motion, this saves storage space because the device is not recording during periods of inactivity. Event notification is the process of sending text messages, recorded telephone messages or email when motion is detected [10,11].

3.5. **Alarm System**: is a device or system that gives an audible, visual or other form of alarm signal about a problem or condition. Burglar alarms: designed to warn of burglars, this is often a silent alarm, the police or guard are warned without indication to the burglar which increases the chance of catching him or her. A burglar system is designed to detect intrusion or an un-authorized entry into a building or area [12]. They are also called security alarms, security systems, alarm systems, intrusion detection system, perimeter detection system and similar terms. For a visual indication the alarm generating can be a light bulb, lamp, light emitting diode. e. t. c. For an auditory indication the alarm generating device can be a horn, siren, buzzer or similar item. Burglar system are used in residential, commercial, industrial and military properties for protection against burglary(theft) or property damage, as well as personal protection against intruders..Car alarms likewise protect vehicles and their contents. Prisons also use security systems for control of inmates. The mostbasic alarm consists of one or more sensors to detect intruders, and an alerting device to indicate the intrusion. However, a typical premises security alarm employs the following components: a). Premises control unit (PCU) or panel and b). Sensors. The premise control unit is the "brain" of the system, it reads sensor inputs, tracks arm/disarm status, and signals intrusions. In modern systems, this is typically one or more computer circuit boards inside a metal enclosure along with a power supply. The sensors are devices which detect intrusions. Sensors may be placed at the perimeter of the protected area, within it, or both. Sensors can detect intruders by a variety of methods, such as monitoring doors and windows for opening, or by monitoring unoccupied interiors for motions, sound, vibration, or other disturbances [12].Alerting devices indicate an alarm condition. Most commonly, these are bells, sirens, and/or flashing lights. Alerting devices serve the dual purposes of warning occupants of intrusion, and potentially scaring off burglars. Keypads are small devices, typically wall-mounted, which function as the human-machine interface to the system. In addition to buttons, keypads typically feature indicator lights, a small mulch-character display, or both. Interconnections between components. This may consist of direct wiring to the control unit, or wireless links with local power supplies. Security devices: Devices to detect thieves such as spotlights, cameras & lasers [12,13].

**Figure 3:** Some cctvs and ip cameras for monitoring [12,13] .

In addition to the system itself, security alarms are often coupled with a monitoring service. In the event of an alarm, the premises control unit contacts a central monitoring station. Operators at the station see the signal and take appropriate action, such as contacting property owners, notifying police, or dispatching private security forces. Such signals may be transmitted via dedicated alarm circuits, telephone lines, or Internet.Alarm connection and monitoring Depending upon the application, the alarm output may be local, remote or a combination.Local alarms do not include monitoring, though may include indoor and/or outdoor sounders (e.g.

motorized bell or electronic siren) and lights (e.g. strobe light) which may be useful for signaling an evacuation notice for people during fire alarms, or where one hopes to scare off an amateur burglar quickly. However, with the widespread use of alarm systems (especially in cars), false alarms are very frequent and many urbanites tend to ignore alarms rather than investigating, let alone contacting the necessary authorities. In short, there may be no response at all. In rural areas (e.g., where nobody will hear the fire bell or burglar siren) lights or sounds may not make much difference anyway, as the nearest responders could take so long to get there that nothing can be done to avoid losses [11,13].

Remote alarm systems are used to connect the control unit to a predetermined monitor of some sort, and they come in many different configurations. High-end systems connect to a central station or responder (e.g. Police/ Fire/ Medical) via a direct phone wire, a cellular network, a radio network (i.e. GPRS/GSM) or an IP path. In the case of a dual signaling system two of these options are utilized simultaneously. The alarm monitoring includes not only the sensors, but also the communication transmitter itself. While direct phone circuits are still available in some areas from phone companies, because of their high cost and the advent dual signaling with its comparatively lower cost they are becoming uncommon. Direct connections are now most usually seen only in Federal, State, and Local Government buildings, or on a school campus that has a dedicated security, police, fire, or emergency medical department (in the UK communication is only possible to an Alarm Receiving Centre – communication direct to the emergency services is not permitted). More typical systems incorporate a digital cellular communication unit that will contact the central station (or some other location) via the Public Switched Telephone Network (PSTN) and raise the alarm, either with a synthesized voice or increasingly via an encoded message string that the central station decodes [11,13]. These may connect to the regular phone system on the system side of the demarcation point, but typically connect on the customer side ahead of all phones within the monitored premises so that the alarm system can seize the line by cutting-off any active calls and call the monitoring company if needed. A dual signaling system would raise the alarm wirelessly via a radio path (GPRS/GSM) or cellular path using the phone line or broadband line as a back-up overcoming any compromise to the phone line. Encoders can be programmed to indicate which specific sensor was triggered, and monitors can show the physical location (or "zone") of the sensor on a list or even a map of the protected premises, which can make the resulting response more effective. For example, a heat sensor alarm, coupled with a flame detector in the same area is a more reliable indication of an actual fire than just one or the other sensorindication by itself.

Many alarm panels are equipped with a backup communication path for use when the primary PSTN circuit is not functioning [12]. The redundant dialer may be connected to a second communication path, or a specialized encoded cellular phone, radio, or internet interface device to bypass the PSTN entirely, to thwart intentional tampering with the phone line(s). Just the fact that someone tampered with the line could trigger a supervisory alarm via the radio network, giving early warning of an imminent problem (e.g., arson). In some cases a remote building may not have PSTN phone service, and the cost of trenching and running a directline may be prohibitive. It is possible to use a wireless cellular or radio device as the primary communication method. In the UK the most popular solution of this kind is similar in principle to the above but with the primary and back up paths reversed. Utilizing a radio path (GPRS/GSM) as the primary signaling path is not only quicker than PSTN but also allows huge cost savings as unlimited amounts of data can be sent at no extra expense.

### 3.5. Unmanned aerial vehicle/Drones

A UAV is defined as a "powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload". Therefore, missiles are not considered UAVs because the vehicle itself is a weapon that is not reused, though it is also unmanned and in some cases remotely guided [31].

Civil uses include aerial crop surveys, aerial photography, search and rescue, inspection of power lines and pipelines, counting wildlife, delivering medical supplies to otherwise inaccessible regions, and detection of illegal hunting, reconnaissance operations, cooperative environment monitoring, border patrol missions, convoy protection, forest fire detection and monitoring, surveillance, coordinating humanitarian aid, plume tracking, land surveying, fire and large-accident investigation, landslide measurement, illegal landfill detection, the construction industry and crowd monitoring [32,33].

US government agencies use UAVs such as the RQ-9 Reaper to patrol borders, scout property and locate fugitives. One of the first authorized for domestic use was the Shadow Hawk in Montgomery County, Texas SWAT and emergency management offices. Private citizens and media organizations use UAVs for surveillance, recreation, news-gathering, or personal land assessment. In February 2012, an animal rights group used a MikroKopter , hexacopter to film hunters shooting pigeons in South Carolina. The hunters then shot the

UAV down. In 2014, a drone was used to successfully locate a man with dementia, who was missing for 3 days[34].

Aerial surveillance of large areas is possible with low-cost UAS. Surveillance applications include livestock monitoring, wildfire mapping, pipeline security, home security, road patrol and antipiracy. UAVs in commercial aerial surveillance is expanding with the advent of automated object detection. Many police departments in India have procured drones for law and order and aerial surveillance. UAVs have been used for domestic police work in Canada and the United States. A dozen US police forces had applied for UAV permits by March 2013. In 2013, the Seattle Police Department's plan to deploy UAVs was scrapped after protests. UAVs have been used by U.S. Customs and Border Protection since 2005 with plans to use armed drones [35,36]. The FBI stated min 2013 that they use UAVs for "surveillance". In 2014, it was reported that five English police forces had obtained or operated UAVs for observation Merseyside police caught a car thief with a UAV in 2010 [37].

**Figure 4:** A drone with internet protocol camera for monitoring [33,36].

### 3.6. Sensor types

#### 3.6.1. Passive infrared detectors

A passive infrared sensor used to detect motion. The passive infrared (PIR) motion detector is one of the most common sensors found in household and small business environments. It offers affordable and reliable functionality. The term passive refers to the fact that the detector does not generate or radiate its own energy; it works entirely by detecting the heat energy given off by other objects [14]. Strictly speaking, PIR sensors do not detect motion; rather, they detect abrupt changes in temperature at a given point. As an intruder walks in front of the sensor, the temperature at that point will rise from room temperature to body temperature, and then back again. This quick change triggers the detection.PIR sensors may be designed to be wall or ceiling mounted, and come in various fields of view, from narrow "point" detectors to 360 degree fields. PIRs require a power supply in addition to the detection signaling circuit. Ultrasonic detectors usingfrequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event. There must be motion of an object either towards or away from the receiver.The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy. When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

#### 3.6.2. Microwave detectors

This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (mono-static) for indoor applications, and separate housings (bi-static) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dual-tec" alarm. Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder[14,15].

**3.6.3. Photo-electric beams**

Photo electric beam systems detect the presence of an intruder by transmitting visible orinfrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, itcan be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier [14,15].. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

**3.6.4. Glass break detection**

The glass break detector may be used for internal perimeter building protection. Glass break acoustic detectors
are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismicglass break detectors, generally referred to as "shock sensors" are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors “feel” these shock frequencies and in turn generate an alarmcondition. Window foil is a less sophisticated, mostly outdated, detection method that involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it [14,15].. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

**3.6.5. Heat detection system**

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarmsystem..

**3.6.6. Vibration (shaker) or inertia sensors**

These devices are mounted on barriers and are used primarily to detect an attack on the structure itself. The technology relies on an unstable mechanical configuration that forms part of the electrical circuit. When movement or vibration occurs, the unstable portion of the circuit moves and breaks thecurrent flow, which produces an alarm. The technology of the devices varies and can be sensitive to different levels of vibration. The medium transmitting the vibration must be correctly selected for the specific sensor as they are best suited to different types of structures and configurations [16]. A rather new and unproven type of sensors use piezo-electric components rather than mechanical circuits, which can be tuned to be extremely sensitive to vibration. The advantages are that they are very reliable with low false alarm rate and middle place in the price range. While the disadvantages include that it must be fence mounted and the rather high price deters many customers, but its effectiveness offsets its high price. Piezo-electric sensors are a new technology with an unproven record as opposed to the mechanical sensor which in some caseshas a field record in excess of 20 years.

**3.6.7. Passive magnetic field detection**

Thisburied security system is based on the Magnetic Anomaly Detection principle of operation. The system uses an electromagnetic field generator powered by two wires running in parallel. Both wires run along the perimeter and are usually installed about 5 inches apart on top of a wall or about 12"/30 cm below ground. The wires are connected to a signal processor which analyzes any change in the magnetic field.This kind of buried security system sensor cable could be embedded in the top of almost any kind of wall to provide a regular wall detection ability, or can be buried in the ground. They provide a very low false alarm rate, and have a very high chance of detecting real burglars. However, they cannot be installed near high voltage lines, or radar transmitters [14,15].

**3.6.8. E-field**

This proximity system can be installed on building perimeters, fences, and walls it also has the ability to be installed free standing on dedicated poles. The system uses an electromagnetic field generator powering one wire, with another sensing wire running parallel to it. Both wires run along the perimeter and areusually installed about 800 mill-metres apart. The sensing wire is connected to a signal processor that

analyses:amplitude change (mass of intruder),rate change (movement of intruder),preset disturbance time (time the intruder is in the pattern). These items define the characteristics of an intruder and when all three are detectedsimultaneously, an alarm signal is generated [14,17].The barrier can provide protection from the ground to about 4 metres of altitude. It is usually configured in zones of about 200metre lengths depending on the number of sensor wires installed. The advantages are that they must be concealed as a buried form, while the disadvantages include been expensive, short zones which mean more electronics (more money), high rate of false alarms as it cannot distinguish a cat from a human. In reality it does not work that well, as extreme weather causes false alarms.

**3.6.9. Microwave barriers**

The operation of a microwave barrier is very simple. This type of device produces an electromagnetic beam using high frequency waves that pass from the transmitter to the receiver, creating an invisible but sensitive wall of protection.When the receiver detects a difference of condition within the beam (and hence a possible intrusion), the system begins a detailed analysis of the situation. If the system considers the signal a real intrusion, it provides an alarm signal that can be treated in analog or digital form.The advantages are that they must be low cost, easy to install, invisible perimeter barrier, unknown perimeter limits to the intruder, while the disadvantages include extremely sensitive to weather as rain, snow and fog for example would cause the sensors to stop working, need sterile perimeter line because trees, bushes or anything that blocks the beam would cause false alarm or lack of detection [18].

**3.6.10. Micro-phonic systems**

Micro-phonic based systems vary in design but each is generally based on the detection of an intruder attempting to cut or climb over a chainwire fence. Usually the micro-phonic detection systems are installed as sensor cables attached to rigid chainwire fences, however some specialized versions of these systems can alsobe installed as buried systems underground. Depending on the version selected, it can be sensitive to different levels of noise or vibration. The system is based on coaxial or electro-magnetic sensor cable with the controller having the ability to differentiate between signals from the cable or chain wire beingcut, an intruder climbing the fence, or bad weather conditions [17,18]. The systems are designed to detect and analyze incoming electronic signals received from the sensor cable, and then to generate alarms from signals which exceed preset conditions. The systems have adjustable electronics to permit installers to change the sensitivity of the alarm detectors to the suit specific environmental conditions. The tuning of the system is usually accomplished during commissioning of the detection devices. The advantages are that they must be very cheap, very simple configuration, easy to install while the disadvantages include that some systems have a high rate of false alarms because some of these sensors might be too sensitive. Although systems using DSP (Digital Signal Processing) will largely eliminate false alarms on some cases.

**3.6.11. Taut wire fence systems**

A taut wire perimeter security system is basically an independent screen of tensioned trip wires usually mounted on a fence or wall. Alternatively, the screen can be made so thick that there is no need for a supporting chain wire fence. These systems are designed to detect any physical attempt to penetrate the barrier.Taut wire systems can operate with a variety of switches or detectors that sense movement at each end of the tensioned wires [19]. These switches or detectors can be a simple mechanical contact, static force transducer or an electronic strain gauge. Unwanted alarms caused by animals and birds can be avoided by adjustingthe sensors to ignore objects that exert small amounts of pressure on the wires. This type of system is vulnerable to intruders digging under the fence. A concrete footing directly below the fence is installed to prevent this typeof attack. The advantages are that they must be low rate of false alarms, very reliable sensors and high rate of detection.While the disadvantages include been very expensive, complicated to install and old technology.

**Figure 5:** Taut wire fence

**3.6.12. Fibre optic cable**

A fibre-optic cable can be used to detect intruders by measuring the difference in the amount of light sent through the fibre core. If the cable is disturbed, light will 'leak' out and the receiver unit will detect a difference in the amount of light received. The cable can be attached directly to a chainwire fence or bonded into a barbed steel tape that is used to protect the tops of walls and fences [20]. This type of barbed tape provides a good physical deterrent as well as giving an immediate alarm if the tape is cut or severely distorted. Other types work on the detection of change in polarization which is caused by fiber position change.The advantages are that they must be very similar to the Micro-phonic system, very simple configuration, easy to install, while the disadvantages include high rate of false alarm or no alarms at all for systems using light that leaks out of the optical fiber. The polarization changing system is much more sensitive but false alarms depend on the alarm processing.

**3.6.13. H-field**

This system employs an electro-magnetic field disturbance principle based on two unshielded (or 'leaky') coaxial cables buried about 10–15 cm deep and located at about 1 metre apart. The transmitter emits continuous Radio Frequency (RF) energy along one cable and the energy is received by the other cable. When the change in field strength weakens due to the presence of an object and reaches a pre-set lower threshold, an alarm condition is generated. The system is unobtrusive when it has been installed correctly, however caremust be taken to ensure the surrounding soil offers good drainage in order to reduce nuisance alarms [21].The advantages are that they must be concealed as a buried form, while the disadvantages include that it can be affected by RF noise, high rate of false alarms, hard to install..

**3.6.14. Wired, wireless and hybrid systems**

Thetrigger signal from every sensor is transmitted to one or more control unit(s) either through wires or wireless means (radio, line carrier, infrared). Wired systems are convenient when sensors (such as PIRs, smoke detectors, etc.) require power to operate correctly, however, they may be more costly to install. Entry-level wired systems utilize a Star network topology, where the panel is atthe center logically, and all devices "home run" its wire back to the panel. More complex panels use a Bus network topology where the wire basically is a data loop around the perimeter of the facility, and has "drops" for the sensor devices which must include a unique device identifier integrated into the sensor device itself. Wired systems also have the advantage, if wired properly, of being tamper-evident. Wireless systems, on the other hand, often use battery-powered transmitters which are easier to install and have less expensive start-up costs, but may reduce the reliability of the system if the batteries are not maintained. Depending on distance and construction materials, one or more wireless repeaters may be required to get the signal to the alarm panel reliably [21,22]. A wireless system can be moved to a new home easily, an advantage for those who rent or who move frequently. The more important wireless connection for security is the one between the control panel and the monitoring station. Wireless monitoring of the alarm system protects against a burglar cutting a cable or from failures of an internet provider. This full wireless setup is commonly referred to as 100% wireless. Hybrid systems use both wired and wireless sensors to achieve the benefits of both. Transmitters, or sensors can also be connected through the premise's electrical circuits to transmit coded signals to the control unit (line carrier). The control unit usually has a separate channel or zone for burglar and fire sensors, and better systems have a separate zone for every different sensor, as well as internal "trouble" indicators (mains power loss, low battery, wire broken, etc.).

## IV. SIMPLIFIED RESIDENTIAL ALARM SYSTEM FOR GENERALIZED DESIGN IN SECURITY AND CRIME PREVENTION.

For the household alarm circuit, an automatic siren is activated to keep other residence within the affected street at alert. In the designing of a medium power automatic alarm, an oscillator would be one of the basic components in construction. An oscillator is any device that converts a steady d.c. source of power into a periodically varying source of power. Any amplifier can be converted into an oscillator if it is arranged in such a way that an exciting voltage of the proper magnitude and phase is obtained from its output. The simplest form of oscillator circuit consists of a parallel combination of inductance L and capacitance C [23]. A timer NE555 integrated circuit was selected for the designing of a medium power automatic siren, based on its frequency of operation, frequency and amplitude stability, as well as its power output. This timer can be used to provide the basis for one-shot or a stable timing operations. The output can sink or source currents up to 200mA, so that a wide variety of loads can be driven [24]. The supply voltage range is 4.5 to 15v (9V was used) and maximum power dissipation is 600mW. The integrated circuit (IC) NE555CN was used for both the oscillator and the audio oscillator. A transistor was used for the driver and an 8Ω loudspeaker for the transducer.The design of the automatic alarm is as shown in Figure 1. This circuit was tested in the laboratory and gives a satisfactory output tone. The resistor $R_2$ was changed to a variable resistor in order to vary the frequency at the output 3 of the IC 1.The frequency at the output is calculated from equation 3 [25], i.e.

$$f_1 = \frac{1.44}{(R_1 + 2R_2)C_1} \quad \ldots..1$$

∴ When the rheostat is fully turned i.e. $R_2 = 120k$ , the frequency generated at the output will be

$$f_1 = \frac{1.44}{(18 + 240) \times 100 \times 4.7 \times 10^{-6}}$$

$$= 1.19Hz$$

When $R_2 = 20k$ , using equation 3, $f_1 = 5.28Hz$

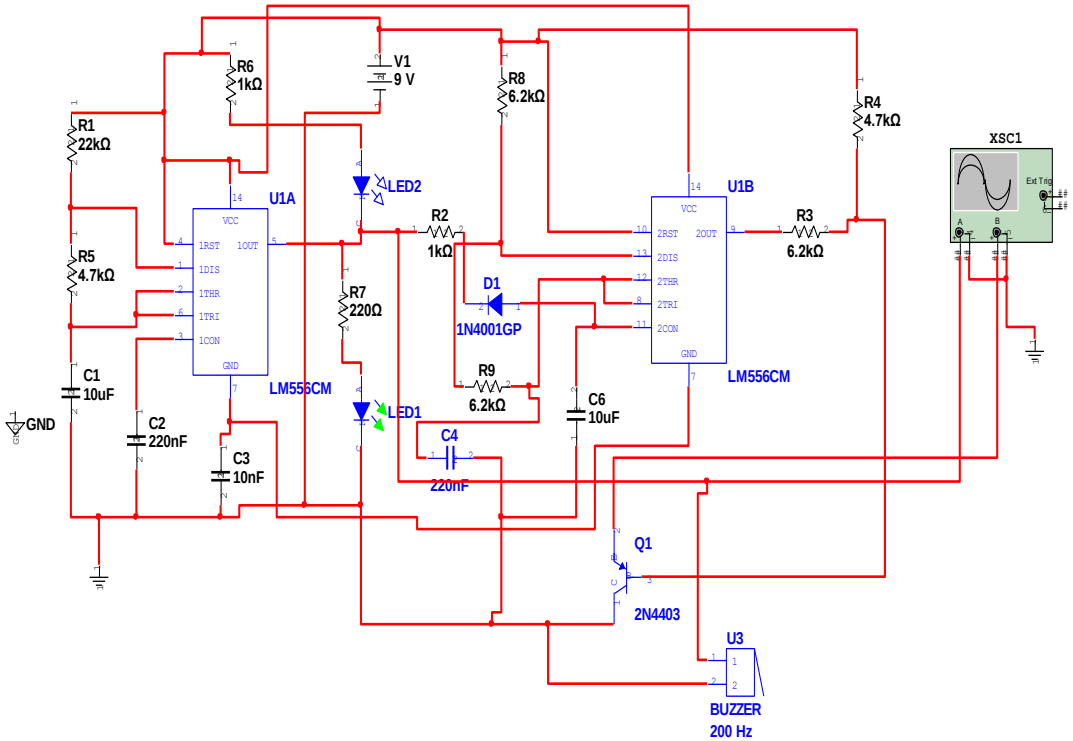


**Figure 6:** Medium power automatic siren circuit

The circuit produces square wave output that sweeps up and down in frequency. Modulation is provided by $V_{R1}$, $D_1$ and $C_2$; and the circuit also produces a two tone sound in a loudspeaker which is capable of handling 10watts. The transistor AD149, PNP Ge, Audio Output used acts as a driver for the 8Ω loudspeaker

and $D_3$ is a silicon rectifying diode used to remove the noise. The output frequency $f_2$ for the audio oscillator that is focused on the oscilloscope is due to $R_3$, $R_4$ and $C_4$.

$$f_2 = \frac{1.44}{(R_3 + 2R_4)\,C_4} \qquad \ldots\ldots\ldots\ldots 2$$

$$= \frac{1.44}{(5.7+11.4)0.22 \times 10^{-3}}$$

$$= 0.383 \times 10^3 = 383\text{Hz}$$

This alarm circuit operation can be extended for use to sense an intruder or visitor by connecting UIA pin 4 via a sensor placed a short distance from the house from the entrance main door such that, no matter what, the area covered by the switched sensor will be stepped on- by the intruder and this will switched on the circuit, in which case, the lights will start blinking. The alarm will not sound because the audio oscillator is not ON; but the person inside will surely be aware that an intruder is outside. The designed circuit is as shown in Figure 1.

Also U1A pin 4 and U2A pin 4 can be connected to other sensors installed on the windows of a house to detect the presence of an intruder to produce a two tone sound. The U2A pin 4 can be connected again to another sensor from the back door to produce a one-tone sound, and all this can be made to work simultaneously.

The output of the U4A AND gate, when in its high state, triggers an alarm whose circuit design was shown in Figure 1, and its response to signals is as shown in Figure 2. This alarm sinks currents up to 100mA, and drives a transducer of 10W, whose audio output is enough to awake nearby residents of imminent attacks. The current consumed by the MUX U7 and its associated circuitry including the 555 clock is about 85uA.

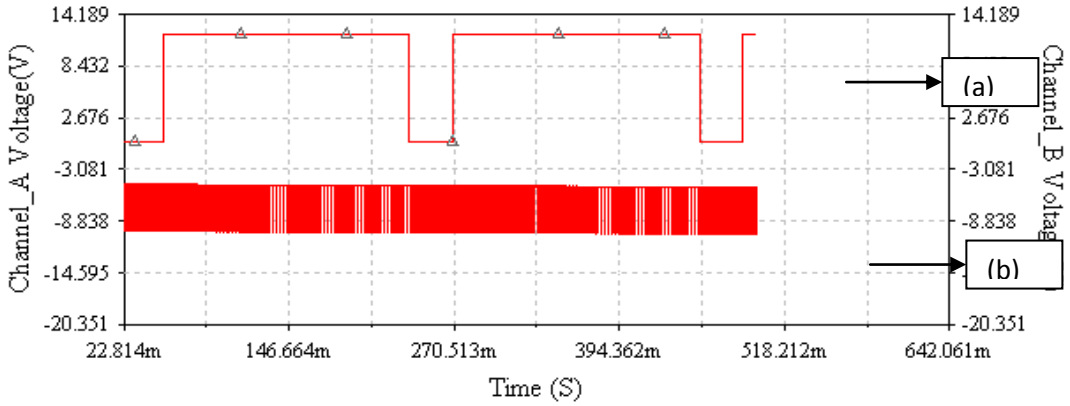


**Figure 7:** Response diagram of automatic siren designed a). Switching frequencies ($f_1$ – high and $f_2$ –low ) b). Output signal to the transducer.

## V. CONCLUSION

The application of cctv and IP cameras for crime prevention and policing offers a better universal advantages over other security devices as it supports monitoring and event capture and memory facilities. A combination of these security devices are suggested for use in the quest for total crime prevention in any of the outlined environment. It is believed that the police and other government and private security outfits will find the study useful in their search for electronic equipment in combating the ever increasing crimes in our Country.

## REFERENCES

[1] S.T. Andrew: *Computer Networks , 2nd edition* , Prentice –Hall international, inc. 1999
[2] A. Atayero, et al: *Designing a robust e-policing System for Developing Nations of the World*. Proceedings on 5thEuropean conference on e-Government. 2007, Pp 27-32
[3] T. Balogun: *Police welfares and state police agitation* ; 2nd national workshop on security of life and property in Nigeria, Sheraton Hotel Abuja, 2002, 25-26th June.
[4] P. Barry, and W. Barry: *Crime free housing; Butterworth Architecture*, Arnold publishersinc. 1991
[5] D.M. Calcutt.; J.C. Fredderick; G,H. Parchizadeh: *Microcontrollers, "Hardware, Software and Applications* "; Arnold publishers ,Londonm 1998
[6] J. Chan, and D. Breredon*: E- Policing: The impact of IT on police practices*". 2001, [ONLINE], www.cme.gld.gov.au
[7] C.J. Date: *" An introduction to database system,"* Reading, Massachusetts, Addison-Wesley, 1981.
[8] R. Duncan: *Revolution in home security* ; IEE communication Engineering magazine Pg 36 -42, 2003

[9] S.G. Eyindero: *" Policing Nigeria*" National workshop on security of live and property in Nigeria ,Pp23-32
[10] O.O. Fagbohun: *Improving the policing system in Nigeria* : "Using Electronic Policing" Journal of Engineering and Applied sciences, medwell journals, issn 1816-949x, Pp1223-1228. 2007
[11] A.L. Lance: "*Introduction to Microprocessor; Software, Hardware, Programming*", Prentice Hall of India Private Limited, second edition. 1988
[12] H.D. Lechner:"*The computer chronicles"*; Wadsworth publishing company/continuing education Bedmont, Califonia ,third edition. 1981
[13] D.B. Longdey and S.T. Shain:*The microcomputer users usage handbook.* Macmillan press Ltd. London. 1986
[14] W.H. Morie: *The American police Text and readings* , West publishing co.1980
[15] National Instruments*: NI Circuit design Suite* , Electronic workbench group, National Instruments Corporation.2008
[16] S.K.Odita : *Improving the Nigerian Police Force through training* ; Trinity press limited. 1992
[17] J.S. Warford: *Computer Science*; D C Heath and company, 3rd edition, 1991
[18] S.R. Pressman: *Software Engineering, A practitioner's approach;* McGraw- Hill international edition, 2nd edition. 1987
[19] O.O. Fagbohun: *Development of a receiver circuit for medium frequency shift keying signals*, IOSR Journal of Electrical andElectronic Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN2320-3331, Volume 9, Issue 2 Ver. V, Mar-Apr.2014 pp 28-35; American National Engineering Database ANED-DDL 12.1676/iosr-jeee-F09252835; DOI (Digital Object Identifier)10.9790/1676-09252835 J.E. Radzinowicz , and M.N. Wolgang : *Crime and Justice, the Criminal in society* (vol.1) 2nd Ed. 1999
[20] C. Sawyer, and J.K Stancey: *Using informational Technology 3rd edition*, Irwin/ McGraw- Hill companies. 1999
[21] P. Stollard: *Crime prevention through housing design* , T.J. press , Padslow, 1st Edition. 1991
[22] L.M. Varwel: *Internal security issues and policing*; Briston press inc.1978
[23] Wikipedia,: *Police Technology*. The free encyclopaedia, http://en.wikipedia.org / wiki/ police technology, 2006a
[24] Wikipedia,: *Security Systems* , The free encyclopaedia, http://en.wikipedia.org /wiki/ security systems, 2006b
[25] K.S. Williams : Textbook on Criminology, Blackstone press limited. 1998
[26] P. Woods: *"Putting the "E" into E-policing* : what governments and the police need to do to build an online police service, 2001, [ONLINE], www.crimeinstitute.ac.za. Sources date: 24th February 2006.
[27] M.D. Edward and S.A. Broadwell: computer in action ,Wardsworth Inc. 2008
[28] M. Prasad: "Location based services",2009 , [ONLINE], www.gisdevelopment.net/technology/lbs/
*[29]* O.O.Fagbohun,(2014):*Development of a low cost frequency shift keying signal transmitter for digital signal processing.* IOSR Journal of Electronicsand Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p-ISSN 2278-8735, Volume 9, Issue 5 Ver. 1, Sept-Oct. 2014 pp 36-43. American National Engineering Database ANED-DDL 12.1676/ iosr-jece-F09252835;DOI (Digital Object Identifier)10.9790/1676-09512635
[30] Saska, M.; Chudoba, J.; Preucil, L.; Thomas, J.; Loianno, G.; Tresnak, A.; Vonasek, V.; Kumar, V. Autonomous Deployment of Swarms of Micro-Aerial Vehicles in Cooperative Surveillance. In Proceedings of 2014 International Conference on Unmanned Aircraft Systems (ICUAS). 2014.
[31] *McFarland, Matt (17 September 2014). "In Switzerland, police find a use for drones". The Washington Post. Archived from the original on 20 September 2014.*
[32] *Pasztor, Andy; Emshwiller, John (21 April 2012). "Drone Use Takes Off on the Home Front". The Wall Street Journal.*
[33] *A Selvaraj (25 February 2014). "In a first, Tamil Nadu police use UAV in murder probe". Times of India. Archived from the original on 21 February 2015.*
[34] *PTI (20 April 2011). "Chandigarh police get UAV". The Hindu. Chennai, India. Retrieved 8 January 2015.*
[35] *Amie Stepanovich. "Unmanned Aerial Vehicles and Drones". Electronic Privacy Information Center. Retrieved 19 June 2012.*
[36] *Philip Bump. "The Border Patrol Wants to Arm Drones". The Wire. Retrieved 8 January 2015*