A Surveillance System to Counter Vandalism of Transmission Line Equipment

Asiimwe JohnPaul R, Kyohairwe Adella, Cosmas Mwikirize, Richard Okou
Department of Electrical and Computer Engineering
Makerere University Kampala
Kampala, Uganda
emails: {johnpaul.rutaremwa@gmail.com, adellakyohairwe@gmail.com,
mwikirize.cosmas@gmail.com, richoko@gmail.com}

Abstract—**This paper presents the development of a customized surveillance system to counter the vandalism of transmission line equipment on Uganda's national transmission operator's network. The system is based on the Raspberry Pi platform and incorporates a Minisense Piezo-vibration sensor, an Infrared-capable Camera board and a Huawei General Packet Radio Service (GPRS) modem. The system is able to detect vibrations arising from cutting of angle bars on steel pylons, take an evidentiary snapshot of the camera's field of view and annotates the snapshot with details such as Tower number, time and date. The system then relays this snapshot to a workstation in the monitoring centre and triggers an alert in the form of a blinking display. This surveillance system will be deployed on about 4800 steel tower pylons that are currently maintained by the transmission operator country-wide.**

Keywords - UETCL; Surveillance; Machine Vision; GPRS.

I. INTRODUCTION

Uganda Electricity Transmission Company Limited (UETCL) is responsible for transmission of high voltage power (above 66kV), bulk purchase from Independent Power Producers and bulk sale to Distributors and Concessionaires in Uganda [1]. Currently, the transmission network in Uganda spans a total length of 1600km with a total number of approximately 4800 steel towers. UETCL faces a major problem of vandalism of pylon equipment along its transmission network causing financial losses to the tune of $41,000 monthly [2].

The vandals steal tower angle bars, nuts, stay and earth wires and barbed wires, which in turn leads to weakening and possible collapse of the pylons [3]. The collapse of one tower on the network leads to uneven stresses on the two adjacent tower leading to a possibility of a domino effect. This leads to severe power outages, which in turn, would lead to loss of revenue to the company as well as adverse socio-economic challenges. An additional revenue loss is incurred as a result of the capacity charge for the period that the available power cannot be evacuated from the generating plants. It should be noted that replacement of towers is a very time-consuming process requiring about 4 to 6 months for concrete foundations to cure.

Investing in the energy sector is very costly, and therefore, installations should be protected from vandalism so as to safeguard value for money spent. To overcome the problem, UETCL has ensured construction of access roads along the transmission lines to enable routine inspection to detect weak towers and spot welding of the angle bar nuts. There are intensified military patrols into the heavily-affected areas. Sensitization campaigns with District Local Councils have been carried out to reach an objective of co-opting Whistle-blowers to safeguard the transmission lines. UETCL provided for special anti-theft Huck-bolts and fasteners on the towers constructed (up-to 3m above the foundation cap) and an anti-climbing spike system [3].

Surveillance has typically involved the placement of analog cameras in sensitive or strategic areas of a particular business for live monitoring [4]. This serves not only as a deterrent to crime, but also to record the movement of people and property [5][6]. Automated visual surveillance is becoming an increasingly important area of research in computer vision. Interest has been motivated by commercial applications, such as surveillance of airports and office buildings, as well as military ones, such as monitoring the battlefield to automatically collect strategic information [7][8].

Detecting humans in images is a challenging task owing to their predominantly variable appearance and the wide range of poses that they can adopt. The first need is a robust feature set that allows the human form to be discriminated cleanly, even in cluttered backgrounds under difficult illumination [9].

Machine vision has been defined as the use of devices for optical, non-contact sensing to automatically receive and interpret an image of a real scene in order to obtain information and/or control machines or process [10][11]. Histograms of Oriented Gradients (HOG) are feature descriptors, used in computer vision and image processing for the purpose of object detection [9].

A system that incorporates detection of vibrations arising from hacking actions of the vandals, automated capturing of images, Human Detection in Images, as well as relaying evidence and alerting monitoring personnel in real-time would go a long way in combatting of the vice of vandalism.

This paper presents the design and development of a customized surveillance solution in two sections. The methodology discusses the specification of a logical framework, design of a physical model, as well as the implementation of a working prototype. The final section deals with the assembly of individual components, power requirements, tamper-proofing and cost implications of the system.

ISBN: 978-1-61208-369-8

II. METHODOLOGY

A. *Context Diagram*

The prototype is deployed on individual steel tower pylons. It consists of a camera placed at the top of the tower, trained downwards towards the base. A vibration sensor is attached to the steel frame of the tower so as to detect the vibrations caused by the cutting action of the vandals.

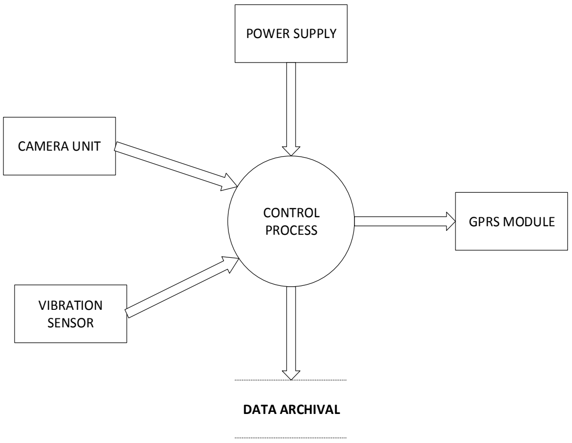


Figure 1. Context Diagram.

A microprocessor provides for implementation of the analytic algorithms to sift through the image data, as well as to take signal input from the vibration sensor. In addition, external storage is provided for the image data captured as well as a GPRS module to facilitate communication between the system and the command centre. A solar panel and battery unit is sized to provide the power requirement of the system setup. This is illustrated in the context diagram in Figure 1.

B. *Technology Architecture*

The Technology architecture model of the system is illustrated in Figure 2. The customized surveillance system is built upon the 512MB Raspberry Pi (R-Pi) Model B Single-board computer [12]. A single Pi NoIR infrared camera provides the image input at high resolution 1080pixel quality frames at a rate of 30 frames per second. The Pi NoIR unit communicates with the R-Pi via the Camera Serial Interface (CSI) located on the body of the R-Pi unit.

The customized surveillance system is built upon the 512MB Raspberry Pi (R-Pi) Model B Single-board computer [6]. A single Pi NoIR infrared camera provides the image input at high resolution 1080pixel quality frames at a rate of 30 frames per second. The Pi NoIR unit communicates with the R-Pi via the Camera Serial Interface (CSI) located on the body of the R-Pi unit.

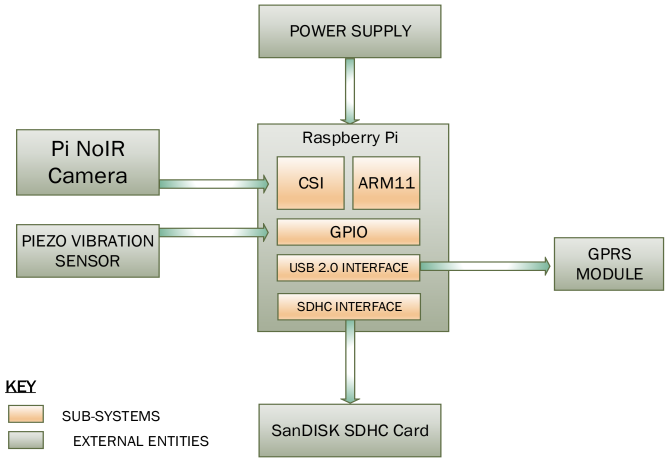


Figure 2. Technology Architecture.

A Piezo Vibration Sensor is connected via the General Purpose Input / Output (GPIO) interface and provides sensory input pertaining to the mechanical vibration of the steel frame to which it is attached. A battery power supply provides the power requirements of the R-Pi unit, as well as the attached external hard drive. The R-Pi requires a steady 5V and draws 2.5W during peak operation.

A 4GB San Disk Secure Digital High Capacity (SDHC) memory card is attached to the ARM11 microprocessor via the SDHC Card slot that is provided on the R-Pi unit to handle the storage requirements of the system. Finally, a generic GPRS module is connected to the USB interface on the R-Pi unit to provide communication capability to the system.

C. *3D-Modeling*

The 3-dimensional model of the proposed surveillance unit was created using SketchUp®Tools. The layout includes visualizations of the Raspberry Pi, a GPRS Modem as well as a deep-cycle Lead Acid battery and its associated Charge Controller and Voltage Regulator. All components were enclosed in a stainless steel box. This is illustrated in Figure 3.

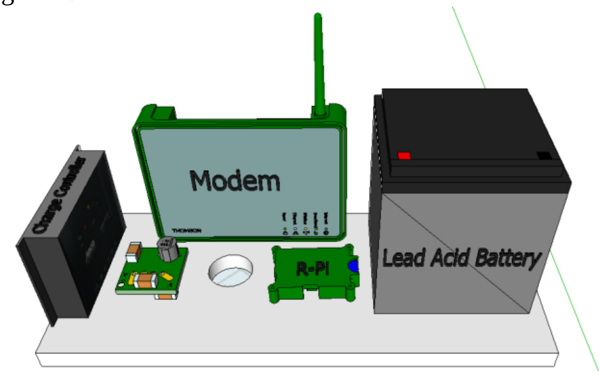


Figure 3. 3D Model.

A visualization was created of the proposed surveillance unit, and its intended mounting on the transmission line towers. The enclosing box is placed on the highest possible bracing of the steel pylon making considerations of maximum camera viewing angle. This is illustrated in Figure 4.

ISBN: 978-1-61208-369-8

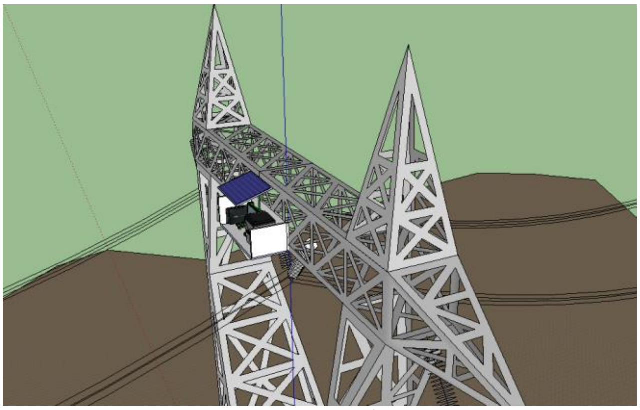


Figure 4. 3D Model of deployment.

It is screwed or welded to the bracing angle bars securely to prevent attempts by vandals at circumventing the security system. Also, placement at the height of the live conductors reduces the accessibility of the surveillance system and hence safeguards it against tampering. This placement is illustrated in the 3D model in Figure 4.

A solar panel was thus included in the visualization in Figure 4 to cater for the energy requirements of the system. It is placed vertically above the enclosing box to provide shadowing against direct sunlight and unnecessary heating. In addition, the placement of the solar panel above the enclosing box provides protection against the effects of direct precipitation (rain or hail).

D. *Vibration Sensor Interrupt*

A wiring schematic was generated using the TinyCAD software package. Of paramount importance was the specification of the connection of the Piezo-Vibration sensor to the GPIO pins of the Raspberry Pi. The circuitry was based on the implementation of a Monostable vibrator based on the 555 timer. This is illustrated in Figure 5.

This circuit layout is necessary to amplify and to shape the output of the vibration sensor into a clean square wave whose Positive going transition can be used to trigger the GPIO interrupt. A resistor between the Vibration Sensor terminals alters the sensitivity of the device while the Operational Amplifier ensures that the voltage output of the sensor is of the correct magnitude to trigger operation of the 555 timer Integrated Circuit (IC).

The Vibration sensor interrupt was implemented using Python, making use of the RPi.GPIO library. This was done by setting up the Pin 23 of the GPIO on the Raspberry Pi to wait for a Positive-going transition of a pulse occurring on the input to the pin. On the rising edge of the pulse generated by the 555-timer circuit, the microprocessor starts the camera routine by running a call to the peopledetect.py script. This is followed up by a system call to the ftpsync.py script.

E. *Automation of Camera Routine*

The Pi NoIR camera board is provided without an IR Filter. This allows it to take images or record video illuminated with IR Light, even in low visible-light conditions.

It is capable of producing 2592 X 1944 resolution still images, although this markedly slows down machine vision algorithms. Optimal performance was achieved with the camera limited to 600 X 450 resolution images.

A Human Detection Algorithm was written, based on Dalal Triggs' work [9] with HOG. The algorithm used in this project was heavily based on the examples included in the OpenCV 2.4.7 library distribution for Python. Upon detection of each instance of vibration, the camera is prompted to capture a single snapshot of the current field of view exposed to the camera.

Raspistill [13] is the command-line-driven application provided to take still photos using the Pi NoIR Camera board. The extra flags used with this command specify the output image name, photo resolution, exposure time (30 microseconds) and night time exposure mode. In addition, the command specifies that no preview window should be opened. All these flags were necessary to ensure an instantaneous capture of the still photograph. The final output of the image capture and processing routine is illustrated in Figure 6.

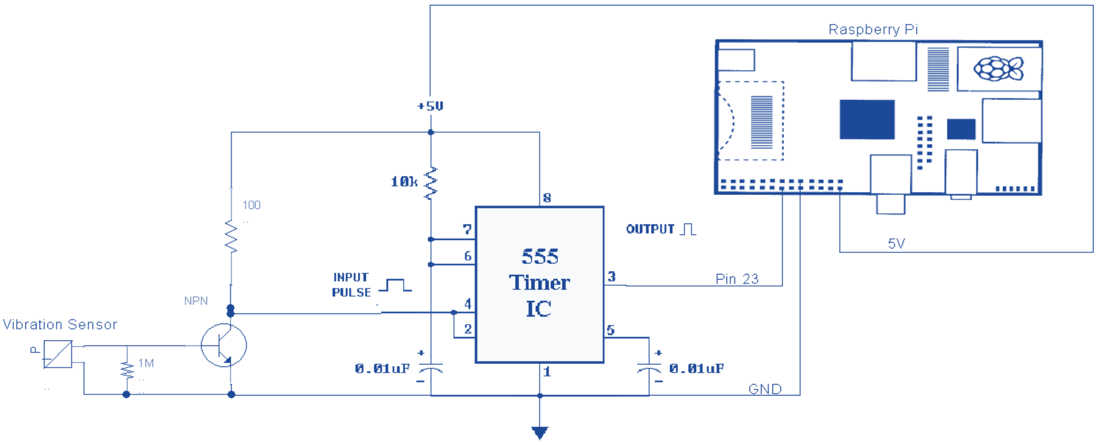


Figure 5. Schematic of Vibration Sensor Circuit.

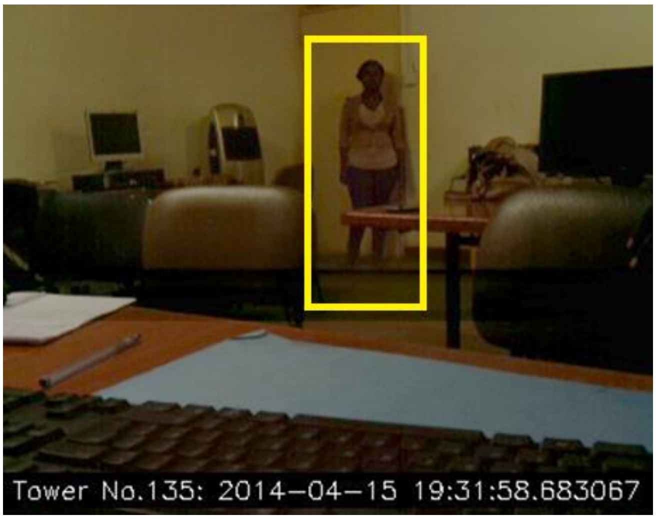


Figure 6. Annotated Critical Evidence Snapshot.

The HOG algorithm implemented by the python program to carry out the detection of Human forms within the captured image is run first. A yellow rectangular boundary is drawn around the region of the image within which the human form detection has been made.

Captioning of images is carried out by a sequence of commands. The first line places a black solid filled rectangle near the bottom of the input image. The second line of code is responsible for generating the text to place over the black rectangle.

The metadata text generated by the code includes the Tower number and location information. For purposes of this example, the code generated a random integer between 0 and 500 to simulate actual tower numbers attached to steel pylons on the transmission network.

In addition, the code creates a Timestamp including date and time information for accurate reference. The text is generated in white on top of a black background for maximum contrast. The SaveImage function is then invoked to store the output image, henceforth referred to as a Critical Evidence Snapshot (CES) [14], in a uniform output image and directory to allow the FTP transfer script to access it.

F. Automation of GPRS Dialup Connection

The Raspberry Pi supports usage of the Huawei E220 USB GPRS Modem. WV Dial is a script that facilitates initiating a dial-up connection from the Raspberry Pi to create an Internet connection via the Modem. USB Modeswitch, on the other hand, is a utility that toggles functionality of the USB device from Mass storage (which is enabled by default) to GPRS Modem (which is required for this purpose)

The WVDial Configuration file is edited via a command-line-based text editor, so as to configure the operation of the WV Dial script. The carrier-specific settings required to set up a Dial-Up connection to the internet are specified in this file.

G. Automation of FTP File Transfer

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. The transfer was done by using two Python scripts. The upload of the Annotated Critical Evidence Snapshot from the remote surveillance unit was automated with a system call to the ftpupload.py script.

The preliminary program routines in the script are responsible for creating a string value for the file name associated with the image being uploaded. This string value conforms to a uniform naming criteria including the current date and time of the snapshot capture. This is important for the proper curating of the CES archive on the monitoring station.

On the monitoring station, the download of Annotated Critical Evidence Snapshot was accomplished by a repeated call to the ftpsync.py script. This essentially synchronizes the directory contents on the FTP file server and the folder hierarchy on the local monitoring station. The download function queries the ftp file server directory and only downloads files that are currently on the server but are not listed on the local directory.

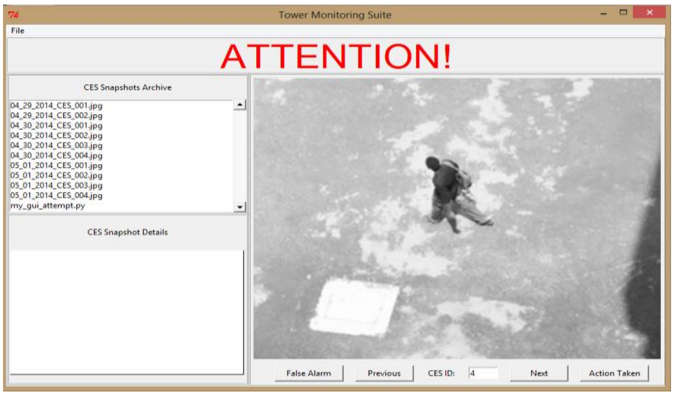
H. Implementation of a Front end monitoring panel

The actual GUI (Graphical User Interface) for the Front End Monitoring Panel was coded via Python, making particular use of the TkInter graphics library. The ordering of the widgets was achieved by nesting of several containers in varying orientations.

A single image is loaded from a directory, after being provided with the image file name. The image is then loaded into memory as a local variable. Finally, the variable is packed into the Frame container which was defined previously. Orientation and padding information was passed as variables to the pack function.

To implement a flashing alert signal, the color of the Text canvas item was repeatedly changed from the base Gray-95% to red and back to capture the users' attention every time a new CES image is acquired and registered on the system.

The <False Alarm> and <Action Taken> buttons were bound to the stop_blinking function. The complete layout of the monitoring panel is illustrated in Figure 7.



04_29_2014_CES_001.jpg
04_29_2014_CES_002.jpg
04_30_2014_CES_001.jpg
04_30_2014_CES_002.jpg
04_30_2014_CES_003.jpg
04_30_2014_CES_004.jpg
05_01_2014_CES_001.jpg
05_01_2014_CES_002.jpg
05_01_2014_CES_003.jpg
05_01_2014_CES_004.jpg
my_gui_attempt.py

CES ID: 4

Figure 7. Front End Monitoring Panel.

The Front End Monitoring Panel was designed to achieve the following functionality:

- Access and display locally stored CES images
- Allow browsing through the CES images in a sequence
- Continuously update the directory of CES images via FTP synchronization
- Alert the monitoring personnel of new CES images and prompt personnel to take action
- Allow personnel to flag CES as "False Alarm" whenever system presents False Positive
- Allow browsing through CES image archive

III. Prototype

A. Assembly of components

The assembly of components is as illustrated in Figure 8. A cast-steel casing was chosen for the housing of the system to protect the setup from attempts at vandalism. Furthermore, shock-proofing was provided by cushioning the components in a Styrofoam mould that was secured to the stainless steel case as illustrated in Figure 9.

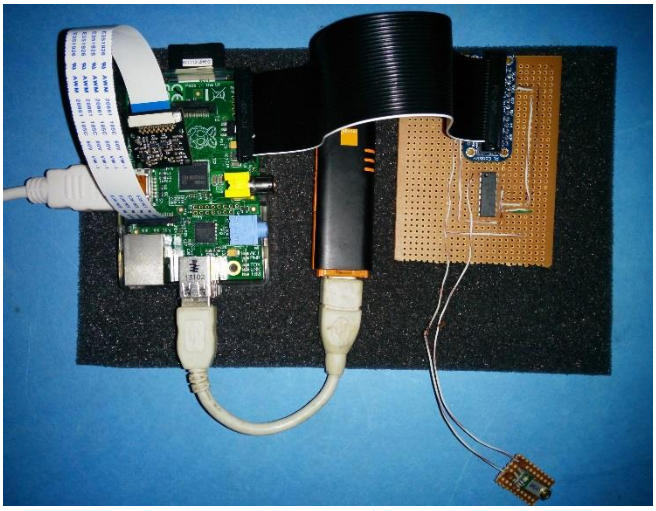


Figure 8. Prototype before Encasing.

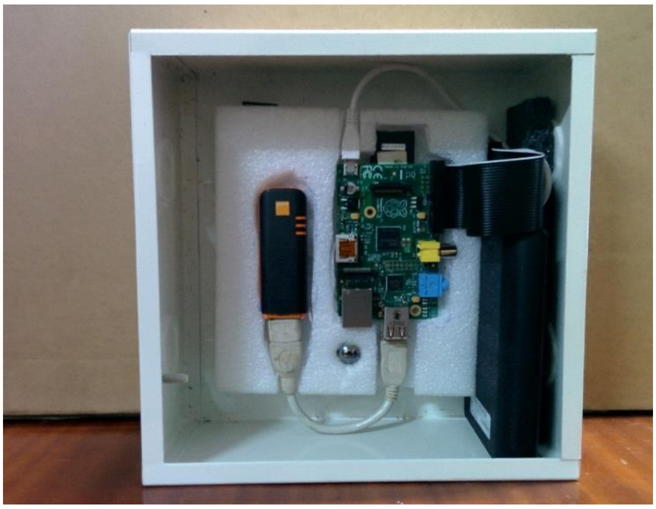


Figure 9. Prototype with Lid removed.

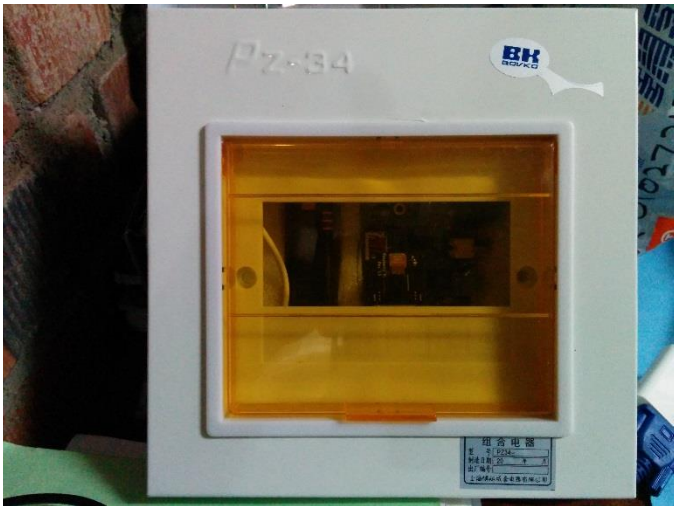


Figure 10. Remote Unit Prototype.

For purposes of this prototype, a 12000mAh battery bank was included to provide the powering requirements of the system. This is to be replaced with a deep-cycle Lead acid battery, charge controller and Solar panel before deployment and field tests.

A clear plastic window in the housing provided a viewing portal for the camera to ensure unobstructed viewing angles for the entire field of view. The final assembly of components and housing of a single surveillance unit is demonstrated in Figure 10.

B. Sizing of solar panel

The Raspberry Pi model B draws 3.5W of power. Even with a very efficient voltage regulator, there will still be some losses in our power system. It is best to assume 80% efficiency, and therefore approximately 4.0 Watts (the battery needs to give more power to cater for inefficiency in the regulator) will be taken from the battery to keep the Raspberry Pi powered. Following a rigorous sizing procedure, it was decided that a 30W/12V/2A mono-crystalline solar panel is required. A 40W mono-crystalline solar panel can also serve this purpose.

C. Sizing of the Battery

The Raspberry Pi will be taking approximately 8Ah of charge from the battery each day, and there may well be days (or multiple days in a row) without any sunshine and therefore, the battery should be sized to provide at least 7 days of power for the Raspberry Pi without sunshine and without the charge of the battery falling below 40%. Therefore, as 7x8=56Ah is at most 60% of the charge of the battery we need a battery of at least 56/0.6=93.33Ah. Thus, a 95Ah or 100Ah battery may be used. Hence, a 12V, 95Ah or 12V, 100Ah battery is used.

D. Testing of the system

The prototype has not yet been tested in a realistic deployment environment. This was mainly because it does not meet the minimum weather-proofing requirements for outdoor deployment. In addition, the national transmission operator was reluctant to effect the shutdown necessary to deploy the system on one of the live towers.

Possible test cases for the prototype system upon deployment on a remote tower would be designed to assess the accuracy and reliability, depending on mounting height, weather and conditions of illumination. Of further importance is the sensitivity of the system to different magnitudes of vibration, and the ability of the system to discriminate and discard different naturally occurring vibrations, such as those due to wind or earth tremors.

E. Tamper-proofing of prototype

No single solution can be considered as "tamper-proof". Often multiple levels of security need to be addressed to reduce the risk of tampering. Some considerations might include the following:

- The proposed surveillance unit is enclosed inside a steel casing which is either screwed or welded shut to prevent unauthorized access and improve tamper resistance.
- It is deployed at a height, 3m below the lowest hanging conductor to control or limit access to products or systems of interest.

F. Cost of the system

One of the motivations for this research was the need for a cost-effective solution to the problem of vandalism. The cost of hardware requirements for the prototype including the solar powering and battery was computed to be $700 per unit of the surveillance system. Assuming that installation is to proceed on all the 4800 transmission towers on the transmission network, this would total up to a rough cost of $3,360,000 for the initial investment.

This is easily justified by the capital cost of replacement of vandalized tower angle bars or the cost associated with the loss of supply due to power outages. Further, assuming a 100% efficacy of the system after installation and a total eradication of the problem of vandalism, this would imply a payback period of up to 7 years.

IV. Conclusion and Future Work

In this paper, the development of a remotely deployed surveillance unit and its accompanying central monitoring station software was presented. The justification for the proposed system was discussed at length in the introduction. The functional and design requirements of the system were presented in detail and then the methodology followed in implementation of the system specified by the functional and design requirements.

Finally, the outcomes of the research endeavor were laid out in the Prototype section. In addition, the final costing of the proposed system was done basing on the cost of the cost of implementing the prototype. The basis for further research and testing of the system was also presented.

This research has dug deep into the potential for the utilization of machine vision algorithms on the cost-effective platform of Raspberry Pi for Surveillance applications. However, we were unable to fully optimize the Human Detection algorithm to allow an acceptable frame-rate for live video analysis, as opposed to the still image analysis used in this project.

In addition, integration of the system into the widely accepted SCADA (Supervisory Control and Data Acquisition) would greatly facilitate its adoption in most transmission network operators. This is motivated by the fact that a similar system is already in place to monitor the different power flow parameters on the transmission network.

Securing of the communication channel is another important research area that needs deeper consideration. This will effectively deter technology-savvy criminals from compromising the integrity of the surveillance data relayed from the remote monitoring units. In addition, reliability of the GPRS network over the entire span of the transmission network needs to be ascertained.

Acknowledgment

This research was conducted under the iLabs@MAK Research Project, based in the College of Engineering, Design, Art and Technology at Makerere University with support from the Government of Uganda.

References

[1] UETCL, “UETCL Official Website,” [Online]. Available: http://www.uetcl.com/. [Accessed 05 August 2014].

[2] OPM, “Office of the Prime Minister,” June 1999. [Online]. Available: www.opm.go.ug/. [Accessed August 2014].

[3] UETCL, “Vandals, a cost and menace to the energy sector,” *The Transmitter*, pp. 11-12, October 2007.

[4] IPVM, Video Surveillance Book, 1st ed., Chicago, 2012.

[5] S. Mubarak, J. Omar and S. Khurram, “Automated Visual Surveillance in Realistic Scenarios,” *IEEE Computer Society*, pp. 30-39, 2007.

[6] S. Russo, “Digital Video Surveillance: Enhancing physical security with analytic capabilities,” California, 2008.

[7] Motorola Solutions Inc, “Motorola Optimized Video Security,” Illinois, 2011.

[8] Seagate Technology LLC, “Security Gets Smarter With Intelligent Video Surveillance Systems,” New York, 2012.

[9] N. Dalal and T. Bill, “Histograms of Oriented Gradients for Human Detection,” Paris.

[10] N. Zuech, Understanding and Applying Machihe Vision, 2nd ed., New York: Marcel Dekker, 2000.

[11] B. Gary and K. Adrian, Learning OpenCV, 1st ed., Cambridge: O'Reilly, 2008.

[12] Raspberry Pi Foundation, “About Us,” [Online]. Available: http://raspberrypi.org/about/. [Accessed 13 August 2014].

[13] Raspberry Pi Foundation, *RaspiCam Documentation*, London, 2013.

[14] D. Gorodnichy and M. Tony, “Automated video surveillance: ACE Surveillance (Annotated Critical Evidence) case study,” Ontario, 2008.