International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.2 (Mar-2019)

http://dx.doi.org/10.12785/ijcds/080203

Two Levels Alert Verification Technique for Smart Oil Pipeline Surveillance System (SOPSS)

Laith M. Fawzi[1], Salih M. Alqarawi [2], Siddeeq Y. Ameen [3] and Shefa A. Dawood [4]

[1] University of Science and Technology, Information Technology Directorate, Baghdad, Iraq
[2] Department of Computer Engineering, University of Technology, Baghdad, Iraq
[3] Quality Assurance Advisor, Duhok Polytechnic University, Duhok, Iraq
[4] Department of Computer Engineering, University of Mosul, Mosul, Iraq

Received 30 Dec. 2018, Revised 7 Feb. 2019, Accepted 16 Feb. 2019, Published 1 Mar. 2019

Abstract: The paper describes the design and implementation of a remote Smart Oil Pipeline Surveillance System (SOPSS), with the ability to detect and report vandalism activities in the pipeline system before it takes place via SMS, email or by a phone call. The proposed system enriches with a vast range of sensors to increase sensing capability and accuracy. Furthermore, a visual check added to overcome false alarms, where a video camera integrated with the system software to capture video footage and tracking the abnormal events. The results prove that the system can achieve monitoring and reporting in real-time, with a reduction in the utilized data size to reach 97%. This will increase bandwidth efficiency to 96%. In addition, this system small in size, portable and cost-effective. Therefore, the proposed system considered as an efficient technology for different monitoring purposes.

Keywords: Three Operation Modes, Microcontrollers, Multi Sensors, Visual Verification, Tracking.

1. INTRODUCTION

Pipelines are an effective way to transport various types of liquids such as crude oil and gas from production sites to market over long distances. Tampering in the pipelines may lead to leakage and environmental pollution, which reflects negatively on the lives and property. Therefore, there is a need to monitor the pipelines for safe use, in order to identify the violations when they occur to be handled by specialists [1]. Great efforts made by the oil companies to reduce the incidence of leakage and environmental pollution. The causes of oil pipeline leaks can be categorized into four main classes: Operational, structural, unintended, and intended damages [2]. The operational causes include leakage in oil and gas pipelines because of equipment failure, or human error, etc. The structural causes include the failure of the pipeline because of corrosion of pipelines. The unintended damages can be occurred because of the existence of works like construction or agricultural near by the oil pipeline area. The intended damage causes can be as a result of vandalism from terrorist attacks or theft [3]. In general, vandalism refers to illegal activity leads to the destruction of infrastructure by targeting vital installations such as oil and gas pipelines, etc. [4].

Many security and technological measures have were implemented to stop vandalism, leakages, and failure in oil pipelines. However, these measures rely heavily on human factor in monitoring since they did not achieve the desired results. Some did not adopt web-based and facing delay, whereas others cannot allow real-time monitoring [1], [3], [4], [5]. On the other hand, others have not the ability to take pictures and video to find out the reason for leakage or failure and to produce sabotage events report before their occurrence [6]. Moreover, others do not consider the ability of objects tracking for better decision-making, and network bandwidth efficiency, by using advanced image processing since the surveillance system should be able to use different types of alert methods and flexibility to choose different levels of monitoring [7]. Some researchers have considered issues related to secure monitoring system for petroleum transportation tankers [8].

In this paper, a Smart Oil Pipeline Surveillance System (SOPSS) presented to enable safe operation of the oil pipeline plant. This is achieved via monitoring the safety of oil pipelines remotely using a visual system enriched by a vast range of sensors to get higher sensitivity, accuracy, reliability, availability and performance with minimal usage of bandwidth, power,

E-mail address: laith_aldbagh@yahoo.com, prof-siddeeq@ieee.org, al_qaraawi55@yahoo.com, shefadawwd@gmail.com

and storage capacity. This system should be able to work under different modes of monitoring with different sensor levels and thresholds mastered by a web application hosted by the smart visual system. This web application interacts with a user via different terminals like desktop, laptop, tablet, and smart phone. The proposed system can ensure real and a reliable notification through using two levels of surveillance (multi sensors box and video camera) supported by visual verification technique. The system has the ability to send alert messages via more than one way, such as SMS, and email. However, in case the operator did not pay attention to the message or email, the system makes a call (ringing) to notify the operator for an event occurred. Thus, the necessary actions to handle the vandalism applied immediately.

The rest of the paper has organized as follows. Sections 2 and 3 illustrate the literature review and objectives of the proposed system. Section 4 presented the pipeline surveillance system requirements. On the other hand, sections 5, 6, and 7 show the proposed surveillance system hardware and software design. Section 8 demonstrates the proposed system analysis and evaluation.

2. Pipeline Surveillance System Requirements

From the research conducted, the following requirements are needed for any pipeline monitoring system to work properly, especially for long distance pipeline [1], [9], [10]:

1. Easy installation and less maintenance, without affecting the physical properties or the operation of the pipeline.
2. The real-time operation to detect any risk occurred at the pipelines on time.
3. Cost-effective.
4. Friendly user interface for easily manage the system functions from remote sites.
5. Able to detect intrusion in the area of interest before the vandals start sabotaging the pipelines.
6. Minimum false alarms to increase the system reliability.
7. Able to capture the footage of pipeline vandalism when occurred so that the authorities can use this evidence in a law court in prosecuting the culprits if needed.
8. The system should be scalable.
9. The system software must be intelligent.

3. The Proposed Surveillance System Design

The proposed surveillance system is composed of hardware and software parts used to sense any event occurred in the area of interest and take the necessary actions. For controlling the monitoring process, the oil pipeline divided into segments, each of about 250 m. The monitoring is carried out through instilling a set of sensors referred to as multi sensors box, connected with a video camera referred to as Smart Wireless Visual Sensor Box (SWVSB) as shown in Figure 1.

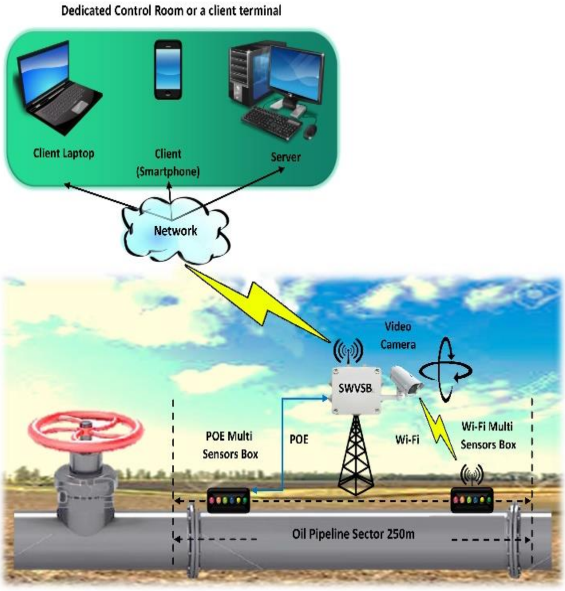


Figure 1. The Proposed System Scheme.

In the hardware part, there are group of models utilized to implement oil pipeline monitoring system. On the other hand, the software part (includes the software modules) performs the following actions: sensors initialization, connectivity verification, data processing, message notification, and video broadcasting which can be seen at a dedicated control room or a client terminal such as a computer or a smart device.

4. The Proposed System Hardware

The proposed hardware system composed of four categories: processing and controlling unit, system communication modules, power supply unit, and surveillance units as shown in Figure 2. The first three categories represent the proposed Smart Wireless Visual Sensor Box (SWVSB), while the last one represents the first and second level of the proposed surveillance system units (Multi-Sensor Box and Video Camera). These units connected together in a way to achieve the research objectives.

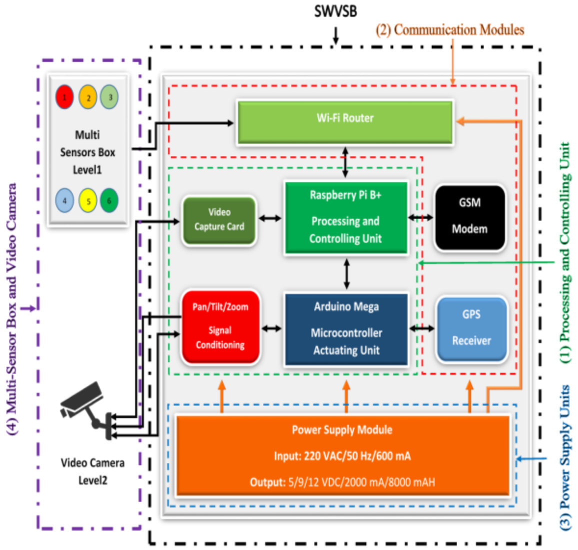

SWVSB
(2) Communication Modules
Multi Sensors Box Level1
1
2
3
4
5
6
Wi-Fi Router
Video Capture Card
Raspberry Pi B+ Processing and Controlling Unit
GSM Modem
Pan/Tilt/Zoom Signal Conditioning
Arduino Mega Microcontroller Actuating Unit
GPS Receiver
Power Supply Module
Input: 220 VAC/50 Hz/600 mA
Output: 5/9/12 VDC/2000 mA/8000 mAH
Video Camera Level2
(4) Multi-Sensor Box and Video Camera
(1) Processing and Controlling Unit
(3) Power Supply Units

Figure 2. The Proposed System Hardware Block Diagram

A. *Processing and Controlling Unit*

Processing and controlling unit introduces a real-time video processing system for smart monitoring and surveillance applications. It takes the appropriate decision through peripheral devices attached to it. The unit was implemented using ARM processor run on a 1GHz clock for processing with an Arduino Mega 2560 microcontroller. The ARM processor with communication facilities, power supply, and the memory represented in the Raspberry Pi B+ (RPI). The Raspberry Pi Model B+ incorporates a number of enhancements and new features such as improved power consumption, increased connectivity, and greater I/O. More details about the specification of the Raspberry Pi Model B+ is given elsewhere [11].

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560. It contains everything required to support the processing and controlling unit (Raspberry) via USB cable. A dedicated message format with serial protocol had designed and implemented over a USB connection between the RPI and the Arduino board. The Arduino main task is to respond to RPI message, control (adjust) the camera direction (azimuth and elevation) to the desired location (target), zooming and focusing. The camera control achieved by stepper motor shield stack on the GPIO bus of the Arduino. Furthermore, the Arduino feeds the RPI with time and location of the surveillance area by the GPS module that attached to the Arduino via GPIO bus. Therefore, the Arduino microcontroller board selected because of the large number of I/O and other essential peripherals. More details about the Arduino Mega 2560 board specification can be found elsewhere [12].

B. *System Communication Modules*

Networking and communication modules deal with sensors via different types of connection (Wi-Fi and Ethernet). However, the Raspberry Pi B+ unit has several connection ports. The functions of these ports are to communicate with;

1. Video input capture card via USB2 port,
2. Arduino Mega controller board via another USB2,
3. GSM modem via serial port, and
4. Wi-Fi router via Ethernet port to achieve connection with multi-sensors box and control room (wire and wireless).

as shown in Figure 3. The figure illustrates the types of connection for Raspberry Pi B+ with its peripherals.

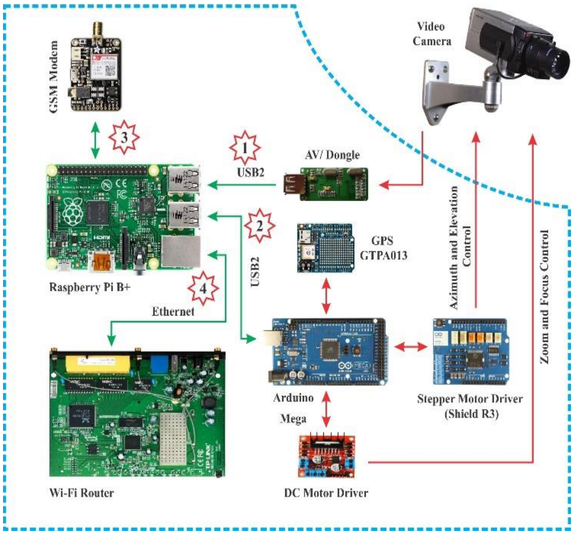


Figure 3. General Layout of Connecting Video Camera and Peripherals to RPI

C. *Power Supply Unit*

The system has been equipped with an efficient power supply unit and a battery to provide the required DC power to all system parts and its peripherals. However, when the main power is on, the battery charged within no more than 2 hours in the worst case. It can operate more than 3.3 hours in full load operation with the absence of the main power. The output DC power is 12W with different output voltage levels (5 / 7.5 / 9 / 12) to support different peripherals. This specification together with the others provided by the power supply unit are shown in Table 1. In this work, three units of the power supply connected in cascade form to provide sufficient power for the proposed system components and to maintain the continuous operation during AC power failure.

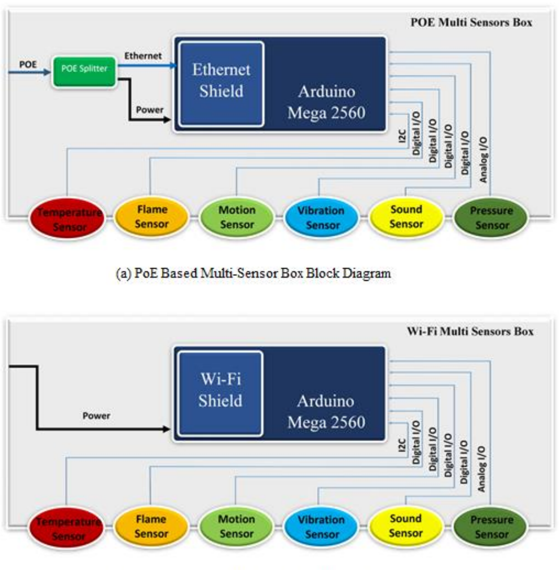
TABLE I. POWER SUPPLY UNIT SPECIFICATIONS

Input Voltage	100 – 240 VAC
Output Voltage (optional)	5V/7.5V/9V/12 VDC.
Output Power	12 W.
Battery Type	Lithium Battery.
QTY. and Capacity	(2200 mAhr × 4) × 3.
Battery Operation time	3.3 hours.
USB	DC 5V/1.0 A

D. *Surveillance Unit*

The proposed surveillance system consists of two monitoring levels; these are:

Level 1: multi-sensors box, which is a set of sensors connected together via Arduino Mega 2560 board as shown in Figure 4. In the proposed system, two types of multi-sensors boxes are designed (PoE and Wi-Fi). Each box contains multi types of sensors to sense temperature, flame, motion, shock, sound, and pressure. These sensors are connected via different types of buses which supported by the Arduino board. Such diversity in sensors gives the proposed surveillance system the ability to monitor oil pipeline, surrounding environment and observe the region of responsibility against different attacks. Each box has its own pre-configured set of thresholds and other sensor parameters, working in sleep and waking up upon modes of operation that depend on sensor readout change. The difference between the two types of multi-sensor boxes (PoE and Wi-Fi) is the method of connection and power supply. Figure 5 shows the multi-sensor box after implementation.



(a) PoE Based Multi-Sensor Box Block Diagram

(b) Wi-Fi Based Multi-Sensor Box Block Diagram

Figure 4. The Proposed Multi Sensors Box, (a) POE Based, (b) Wi-Fi Based

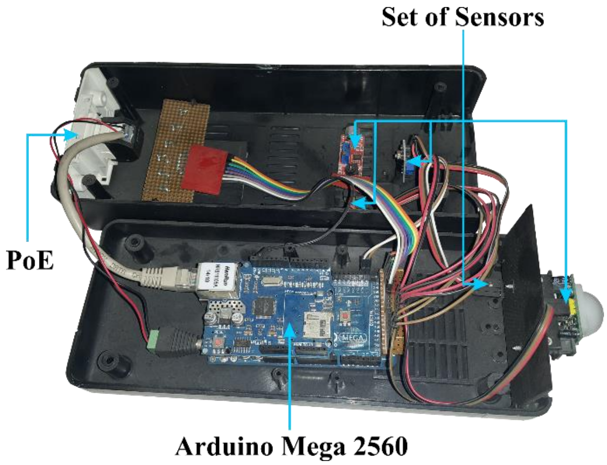


Figure 5. The Proposed Multi-Sensor Box Implementation

Level 2: In this level, a video surveillance camera used to capture video footage from the area of interest. The camera used to verify the availability of the event using histogram and frame subtraction methods. The camera is driven by stepper motors that make it capable of moving (-90 to +90) in Azimuth and (-15 to +55) in Elevation according to the object site. A stepper motor driver used to control the direction stepper motor via the Arduino SPI interface. Furthermore, a pair of DC Motor controllers used to control the zoom and the focus of the camera. The direction, zoom, and focus can be controlled automatically when the system is in auto mode (sensor event mode); while it can be controlled by the observer remotely via a web interface for manual monitoring (manual mode/patrol mode). The proposed video camera used in this work is CamScan DSP 36x Color Video Camera [13].

Finally, the SWVSB protected by a shield against various environmental conditions such as water, dust, and humidity. Moreover, the tampering and sudden shocks. Figure 6 shows the hardware system implementation.

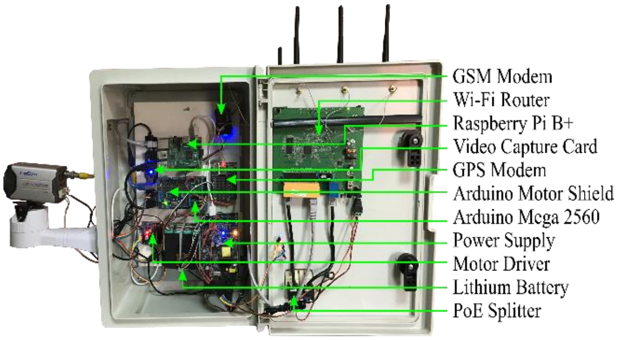


Figure 6. The Proposed System Implementation

5. The Proposed System Software

The system software architecture adopts an embedded Linux (Raspbian Wheezy) as an OS, which is a specialized version of Linux based kernel run on Raspberry Pi. The Linux C language used for programming supported by the Open Source Computer Vision Library (OpenCV) to manipulate the image processing part of this work. The adoption is because of computational efficiency and suitability for on real-time image processing [14]. On the other hand, Java and Python used to perform networking tasks and web services support. Figure 7 shows the general block diagram of the proposed system software.

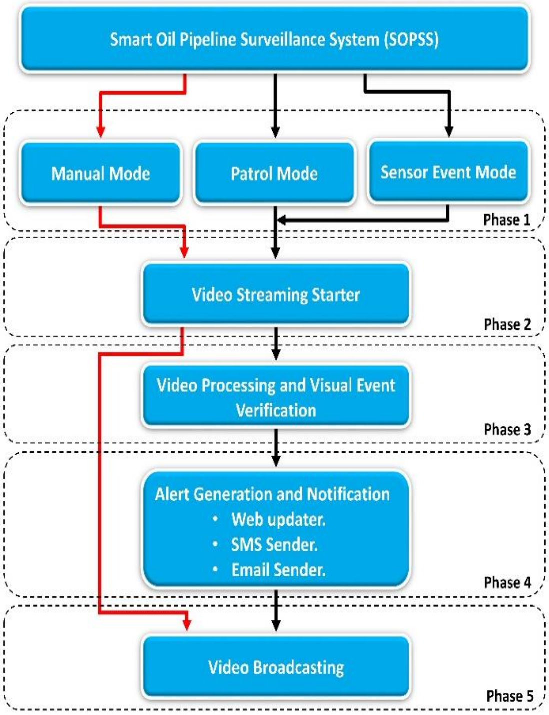


Figure 7. General Block Diagram for the Proposed System Software

As illustrated in Figure 7, the system software can work in three modes of operations: manual, patrol and sensor event (phase- 1). In manual mode, the observer has full control to move the camera in azimuth and elevation. In this mode, the broadcasted video does not pass through video processing/visual verification and alert generation/notification stages, since the responsibility of detection and notification on the observer. In patrol mode; and in order to monitor the oil pipeline in volatile weather conditions, the observer can monitor the area of interested periodically by setting the angle, direction, and speed of the camera movement. However, the system does not relay on sensors to generate the alerts, instead of, the system has the ability to generate the alerts (detect, identify, and track the object), using motion detection based on frame subtraction method. In the third mode, sensor event mode, the system will remain in sleep mode until the multi sensors box excited by a new event (motion, shock, fire, etc.). In this mode, an interrupt generated will wake up the system (SWVSB) and cause the camera to move automatically towards the event site. These three modes give the observer an easy and flexible way to choose the appropriate monitoring method in line with the nature of the work and surrounding weather conditions to increase the system reliability and control.

Phase 2 represents camera initialization setup to start video capturing process. In this phase, the video streaming starter is initialized (for all three modes) which includes; frame setup, zoom level setup, focus mode setup, and video stream preparation.

In phase 3, the actions of video processing and visual event verification initiated. This phase includes video stream source, frame hook, data coordination, target selection, and target tracking.

In phase 4, a notification alert will be generated which includes; get SWVSB geo-position, get the SWVSB identification code, get multi sensors box identification code, initialize email sending service, initialize GSM-SMS service, check connectivity, construct message and email, send alert message via email and/or SMS, ringing for alarm purpose, wait for acknowledgement to reset the system alert. Finally, the video stream is broadcasted in phase 5. Thus, the observer can see a real-time video stream for the monitoring area. This phase includes; frame construction /compression, and streaming.

The system has the ability to verify the truthfulness of the sensor alert, whether it true or faults, by motion detection procedures implemented in phase 3. The procedure started, is based on the alert generated by the sensor box. If both are true (sensor event and visual verification) the system considers this alert as the real one, otherwise, the system considers this alert as a false alarm. If the alert is real, then the system jump to phase 4 and generated the notification alerts (SMS and E-mail). Consequently, this will increases the system reliability and accuracy.

A. Video processing and Visual Verification

This section will explain the verification mechanism of the alerts. When the system activated as result of a specific event detected by one of the sensors, the system starts the process of video capturing. This process followed by a set of image processing procedures applied to the captured video. These procedures help to make sure the alert is real (not false) and to identify the cause of this event. For example, when the PIR sensor detects any movement in the area of interest, the system performs visual processing procedures to detect, identify, and track the causative before reporting the notification. These measures help to reduce the number of false alarms. These measures also apply to the rest of the sensors used.

The visual verification process divided into 6 stages as shown in Figure 8. However, the remaining two stages (7 and 8) in Figure 8 represent the broadcast preparation stages. It is clear from Figure 8 that stage (1), the vision system is categorized into three modes of operation (manual driven, periodic driven, and event driven) based on the operational requirements. In the manual driven mode, there is no video processing since the monitoring process done manually. Thus, the captured data is forwarded directly to the broadcast stage. In the periodic driven mode, the system starts video processing after a fixed time duration determined by the operator, whereas in event driven mode, the system starts video processing when a certain event occurred.

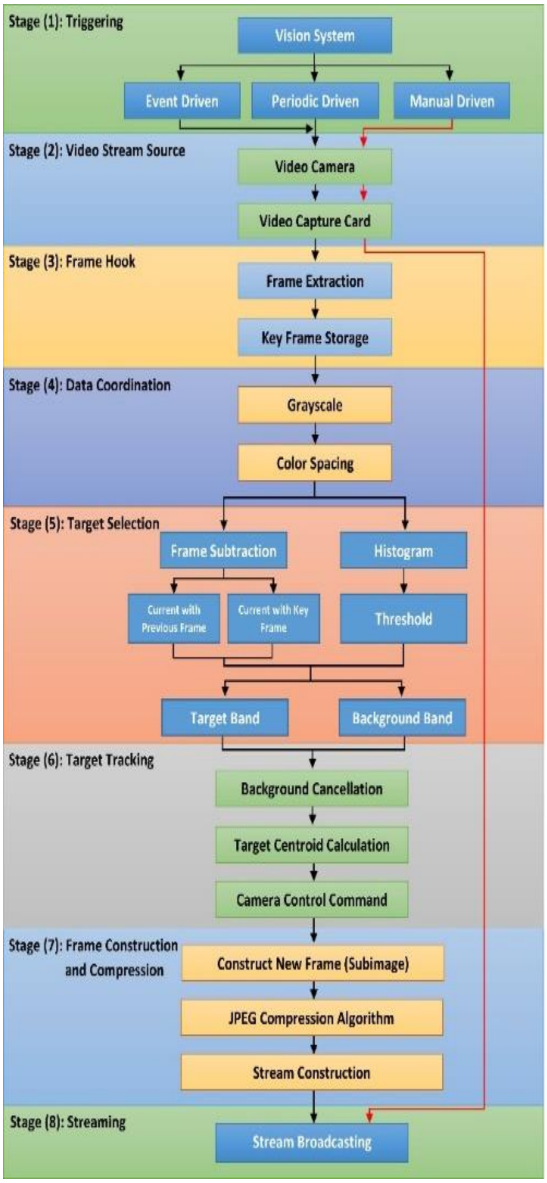


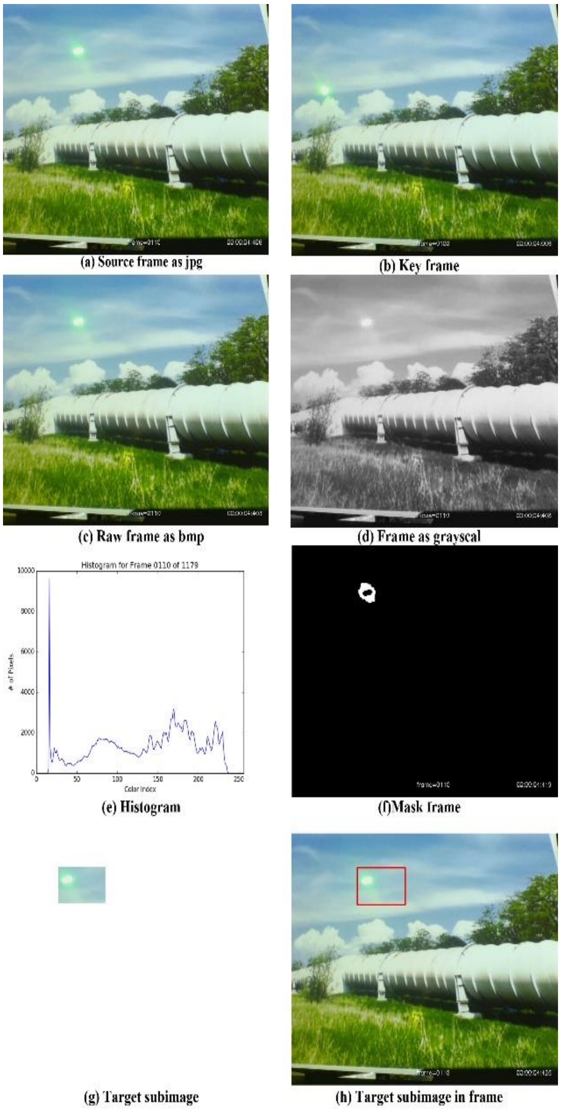
Figure 7. Visual Event Verification Stages for the Proposed System

On stage (2), and after the camera is activated using one of the modes in stage (1), the system will start to receive data from a video camera via USB video capture card as a digital video stream (MPEG4) and pass it to the next stage.

On stage (3), the video stream processed to extract the video frame, key frame, and then storing them in frame buffer as a raw data frame. In this work, a new key frame chosen from every 25 frames. Since the images (or frames) captured on stage (2) are in RGB color space format, there is a need to convert this format to grayscale. The conversion done by stage (4) to more computationally compatible format such as HSV color space format. The process of target selection started in stage (5) to isolate the target from its background. The selection process used to extract target parameters (edges and center) with minimum chance to lose. This will prepare target window tracking and camera tracking.

The selection process uses histogram and frame subtraction methods simultaneously. The histogram is used when the target band and its background is different (no overlapping region) then the target band can specified from background band. On the other hand, the subtraction is used when the target band and its background is identical (overlapping region), since subtracting (or normalizing) the current frame from the previous one (or key frame) helps to detect the target edges. Having achieved the desired results by the two methods, the decision reached depending on the previous histogram or frame subtraction decisions. Furthermore, the frame subtraction method achieved in two ways: if the movement of the target is slow, then the current frame is normalized with a key frame. However, if the movement of the target is fast, then the current frame normalized with the previous frame.

In target tracking, stage (6), and after determining the target band, background band, and target edges, the background frame cancellation is applied to separate the target from its background (object extraction), and to calculate target center. The output of this stage used as a feedback to direct the tracking window and the camera to follow the target. Thus, the target is always in the middle of the scene window. In some cases, if the target movement is slow, and still the target can be seen within the same camera possession, the tracking window can track the target without moving the camera. However, if the target movement is fast, the system still able to track the target by changing the tracking window and the camera position. Figure 9 shows a sample output of video processing and visual verification stages for the proposed system.



(a) Source frame as jpg

(b) Key frame

(c) Raw frame as bmp

(d) Frame as grayscal

(e) Histogram

(f)Mask frame

(g) Target subimage

(h) Target subimage in frame

Figure 8. The Output of Video Processing and Visual Event Verification

B. Broadcast Preparation and Monitoring

This section involves two stages (7 and 8) to perform the broadcasting process. On stage (7), a new frame containing only the target is constructed and compressed. This new frame represents the target as a sub-image within an empty frame that compressed using the JPEG compression to prepare the frame for encapsulation in the output stream. The output stream is ready to be broadcasted (stage 8) through the network to the monitoring site via the web streaming service. The JPEG compression technique used to ensure the high output frame and bandwidth consumption by reducing frame color depth and minimize the frame size of a sub-image that represents the detected target. The web server deploys a video broadcasting that supports MPEG 4/JPEG streaming with some characteristics that will enrich the display by offering stream cache and frame overlay features. However, the camera in the proposed system captures 25 frames per second. Thus, the system broadcasts the first frame containing the full image (key frame, 640 × 480 pixels), whereas the remaining 24 frames contain only the target sub-image (detected object, maximum 120 × 72 pixels) as shown Figure 10.

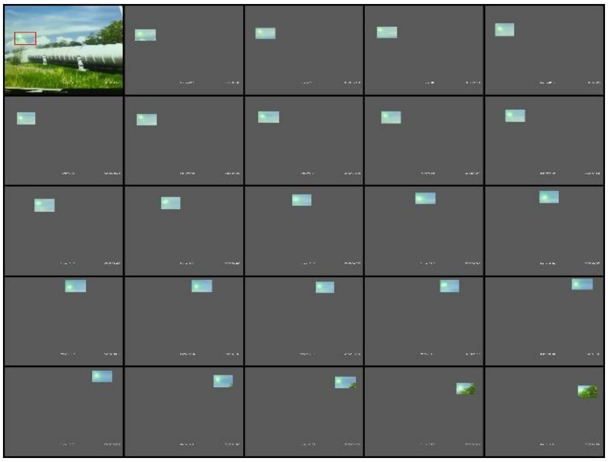
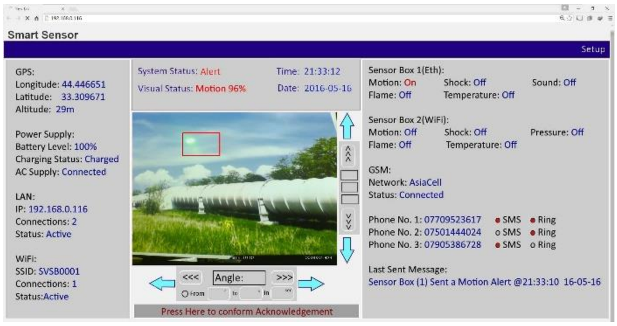


Figure 9. Stream Broadcasting for the Proposed System

Finally, a dedicated web server installed in SWVSB to support the stream broadcasting services and system control. By default the broadcasting deactivated for power consumption reasons and the service may be going live by either an event occurred, scheduled or manual monitoring task. The broadcasting service can be reached by web browser installed in any platform like smartphone, tablets and PCs devices. The observer can use this web browser to display the system web page. The system web page has a friendly Graphical User Interface (GUI) hosted on Raspberry Pi as a web server. The system web page can be used to implement the following functions: identify the authorized login, determined sensors activities (threshold and power on/off), set the appropriate warning messages, control the camera movement in manual/patrol mode, display the broadcasting video, show system setup/status, and reset the alert as shown in Figure 11.



Smart Sensor

GPS:
Longitude: 44.446651
Latitude: 33.309671
Altitude: 29m

Power Supply:
Battery Level: 100%
Charging Status: Charged
AC Supply: Connected

LAN:
IP: 192.168.0.116
Connections: 2
Status: Active

WiFi:
SSID: SVSB0001
Connections: 1
Status:Active

System Status: Alert
Visual Status: Motion 96%
Time: 21:33:12
Date: 2016-05-16

Sensor Box 1(Eth):
Motion: On Shock: Off Sound: Off
Flame: Off Temperature: Off

Sensor Box 2(WiFi):
Motion: Off Shock: Off Pressure: Off
Flame: Off Temperature: Off

GSM:
Network: AsiaCell
Status: Connected

Phone No. 1: 07709523617 ● SMS ● Ring
Phone No. 2: 07501444024 ○ SMS ● Ring
Phone No. 3: 07905386728 ● SMS ○ Ring

Last Sent Message:
Sensor Box (1) Sent a Motion Alert @21:33:10 16-05-16

Figure 10. The SWVSB Web Page Interface

6. PROPOSED SYSTEM ANALYSIS AND EVALUATION

In this section, the results obtained from the proposed SOPS system simulation for 48sec initiated by intrusion are presented. These results are divided into three categories: input/output data size, bandwidth consumption and system processing time.

A. Input / Output Data Size

The results of this subsection are divided into two parts as shown in Figure 12.

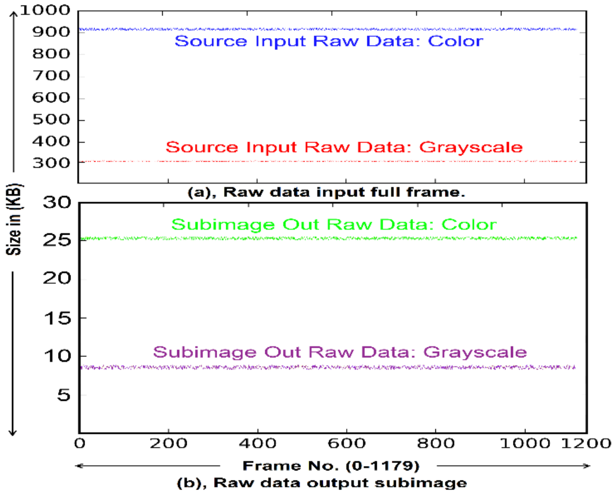


Figure 11. Input/output Data Size Comparison; (a) Raw Data Input Full Frame, (b) Raw Data Output Subimage

In the first part Figure (12-a), the proposed system receives the data stream in MPEG4 format (sequence of JPEG's) with (640×480) frame size, 24 bits color depth, and 25 frames per second frame rate. This will enable the proposed system to manipulate the incoming data and take the necessary actions. Initially, the received JPEG frames, extracted from MPEG4, decompressed to raw data. The source input raw data (colored) in BMP format with the same frame size (640×480), color depth (24 bit), and frame rate (25 frame/s). Next, the system converts the colored raw data to grayscale raw data with 8 color bits (0-255) from black to white gradient. The use of the grayscale format reduces the data size to 1/3 compared with colored input raw data. This will reduce the processing time without affecting system performance.

In the second part, the output data of the proposed system after making target extraction process is as shown in Figure (12-b). The figure shows two different sub-images (colored and grayscale). The sub-image out raw data (colored), provides 97% of data size compared to the input colored raw data. On the other hand, the out grayscale raw data provides 97% of data size compared to the input grayscale raw data, since only the target (sub-image) from the full frame is considered. On the other hand, Figure 12 (a and b) illustrates the reduction achieved in data size between the input and output data. Thus, the efficiency of the proposed system is increased.

B. Bandwidth Consumption

The results of this subsection are divided into two parts as shown in Figure 13.

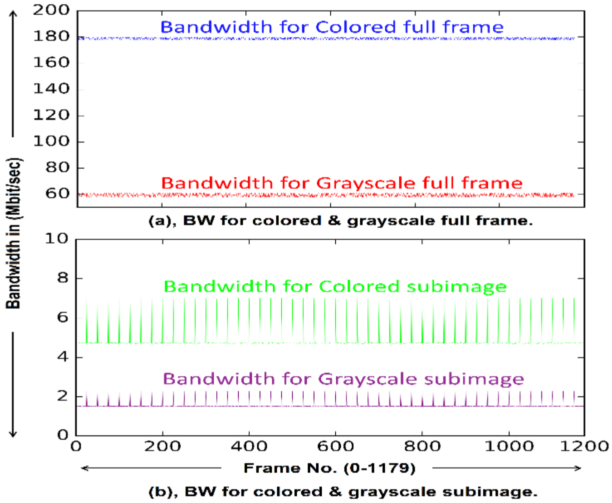


Figure 12. Stream Bandwidth Allocation Comparison; (a) Full Frame BW for Colored & Grayscale, (b) Subimage BW for Colored & Grayscale

Figure (13-a) shows the BW consumption of full frame without any image processing for the transmitted colored and grayscale images. In the case of transmitting a colored image with (640×480) frame size, 24 bits color depth, and 25 frames per sec, the BW allocation is about 180 Mbit/sec, while in grayscale the BW allocation is 60 Mbit/sec. The output is shown in “Figure (13-a)” represents the actual BW reserved by each frame for each type of broadcasting (colored or grayscale).

The second part, Figure (13-b), shows the BW consumption for the proposed system after a series of image processing. The proposed system sends the first frame as a full frame which called key frame (the high peak waves), while the remaining 24 frames are sent as sub-images in different size depending on target size. These sub-images contain the target image only with a maximum size up to (120×72) pixels. However, when the system transmits one colored image, the key frame consumes about 7 Mbit/sec, while the 24 sub-images consume about 4.7 Mbit/sec. Moreover, when the system transmits a grayscale image, the key frame consumes about 2.3 Mbit/sec and the remaining 24 sub-images consume about 1.6 Mbit/sec. The gain in BW allocation is the reduction in the bitrate. Thus, the proposed system can allocate about 96% gain in key frame and 97% gain in sub-image compared to the case of sending 25 full frames every second.

C. *System Processing Time*

In real-time systems, the system clock "the interval between two consequent tasks" must not exceed the full frame time 40 ms. This is because the frame rate is 25 frame/sec and there are 40 ms which represent the allowable time to implement all the required image processing tasks before receiving the next frame. “Figure 14” shows the accumulated percentage task processing and broadcasting time (stages in Figure 8) implemented in the proposed system, while Table II shows the time spent by each task individually.

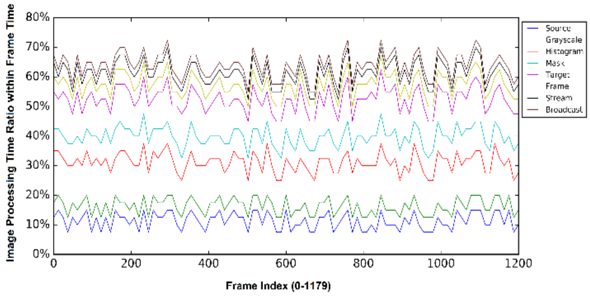


Figure 13. Percentage task processing time

TABLE II. MIN AND MAX TASK PROCESSING TIME

PARAMETER	VALUE
Source (input)	3-7
Grayscale	2-3
Histogram	5-8
Mask	3-5
Target	4-7
Frame	2-3
Stream	1-3
Broadcasting	2

Table II contains the minimum and maximum time required by each task. If the maximum time is considered, then the system needs 38ms to finish all image-processing tasks. This means that the proposed system is a real-time monitoring system that is able to detect and capture the unwanted events. However, when considering the highest line in Figure 14, (broadcasting line), it does not exceed 74% of total frame time in the worst case. This means that the system can operate with real-time capabilities.

7. CONCLUSIONS

The paper presents the design and implementation of Smart Oil Pipeline Surveillance System (SOPSS) using a visual system enriched with vast range of sensors (sound, temperature, motion, shock, flame, and pressure) based on the web server. These sensors increase system capabilities to explore risks in the surrounding oil pipeline region by double check the event occurrence by using sensors and video camera. This will avoid false alert notification. One of the most useful features of this proposed system is the web interface and its event log review. It can be accessed securely from any connected terminal to: review, setup, and control the whole monitoring system. The system can operate in three different modes; manual, patrol, and sensor event modes and broadcast the desired data in color or grayscale mode. The proposed system is able to make a reduction in data size that results in good bandwidth consummation improvement and the ability to achieve real-time monitoring system, where all the required tasks for each frame are performed with less than the frame duration time.

Finally, the work can be further extended by considering the data recorded by the logger review file for analyzing the behavior of the system (sensor events) which is highly recommended to improve the alertness decision-making criteria. This will make decision based on reading the output of different group of sensors boxes to increase system accuracy in intrusion decision making. Moreover, the proposed SOPSS can be considered as a strong candidate for different critical purposes or applications such as airports, border areas, vital installations, etc.

REFERENCES

[1] G. C. Ononiwu, P. U. Eze, O. J. Onojo, G. N. Ezeh, D. O. Dike, S. I. Igbojiaku, and O. C. Nnodi, “A Real-Time Oil Pipeline Anti-Intrusion System Using Acoustic Sensors,” Br. J. Appl. Sci. Technol., vol. 4, no. 26, 2014, pp. 3740–3756.

[2] W. Kent Muhlbauer and E. McAllister, Pipeline Rules of Thumb Handbook: Amanual of Quick, Accurate Solutions to Everyday Pipeline Engineering Problems, 5th ed. Boston: Butterworth–Heinemann, 2002.

[3] J. Agbakwuru, “Pipeline Potential Leak Detection Technologies: Assessment and Perspective in the Nigeria Niger Delta Region,” J. Environ. Prot., vol. 2, no. 8, 2011, pp. 1055–1061.

[4] G. N. Ezeh, N. Chukwuchekwa, J. C. Ojiaku, and E. Ekeanyawu, “Pipeline Vandalisation Detection Alert with Sms,” J. Eng. Res. Appl., vol. 4, no. 4, 2014, pp. 21–25.

[5] O. Shoewu, L. A. Akinyemi, K. A. Ayanlowo, S. O. Olatinwo, and N. T. Makanjuola, “Development of a Microcontroller Based Alarm System for Pipeline Vandals Detection,” J. Sci. Eng., vol. 1, 2013, pp. 133–142.

[6] F. Alsaade, N. Zaman, A. Abdullah, and M. Z. Dawood, “Enhancing Surveillance and Security of Oil Pipelines Transportation Using Wireless Sensor Network,” Middle-East J. Sci. Res., vol. 11, no. 8, 2012, pp. 1029–1035.

[7] A. O. Adejo, A. J. Onumanyi, J. M. Anyanya, and S. O. Oyewobi, “Oil and Gas Process Monitoring Through Wireless Sensor Networks: A Survey,” Ozean J. Appl. Sci., vol. 6, no. 2, 2013, pp. 39–43.

[8] S. Al-Qaraawi and M. Al-Sabbagh, “Simulation and Implementation of a Secured Monitoring System for Petroleum Transportation Tankers,” IJCCCE, vol. 16, no. 1, 2016, pp. 46–53.

[9] A. Azubogu, V. Idigo, S. Nnebe, O. Oguejiofor, and E. Simon, "Wireless Sensor Networks for Long Distance Pipeline Monitoring," Int. Sch. Sci. Res. Innov., vol. 7, no. 3, 2013, pp. 86–91.

[10] F. C. Obodoeze, T. I. Ozue, and M. C. Nnenna, "An Enhanced Multi-Agent System (MAS) Based Framework for Pipeline Vandalism Monitoring System Niger Delta Region," Int. J. Eng. Res. Technol., vol. 3, no. 12, 2014, pp. 981–986.

[11] "Raspberry products." [Online]. Available: http://www.raspberrypi.org/products.

[12] "Arduino." [Online]. Available: https://www.arduino.cc/.

[13] "CamScan." [Online]. Available: http://www.camscan.ca.

[14] K. Mistry and A. Saluja, "An Introduction to OpenCV using Python with Ubuntu," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 1, no. 2, 2016, pp. 65–68.

Laith M. Fawzi was born in Iraq. He received the B.Sc. degree in Electrical and Computer Engineering from Military Engineering College, Iraq, in 1999; and the M.Sc. degree in Computer Engineering in 2005 from University of Technology, Iraq, then Ph.D. degree in Computer Engineering in 2018 from University of Mosul . He worked as a lecturer in Al-Rafidain University College in Iraq until 2011, in addition to his work in the Ministry of Science and Technology (MOST), Iraq till now. His researches interest in the area of networks design. He has an experience in networking, communication and information technology (IT).

Salih M. Al-Qaraawi received B.Sc. in Electrical and Electronics Engineering in 1977 from University of Technology, Baghdad. Next, he was awarded the M.Sc. degree in Computer Engineering in 1980 from Control and Systems Engineering, University of Technology, Baghdad then Ph.D. degree in Computer Engineering in 1994 from University of Technology, Gdansk, Poland in the field of Fault Diagnosis and Reliability of computer networks. Professor Salih worked in University of Technology, Baghdad since April 1983- present. He was Dean Assist. of Control and Systems Engineering from 1996-2003 and 2006-2012 then the Dean of Computer Engineering, University of Technology since 2013 – present. He published about 30 papers in the field of computer networks, reliability, microcontroller's applications, and data communication and network security. He supervised over 10 Ph.D. and 33 M.Sc. students.

Siddeeq Y. Ameen received BSc in Electrical and Electronics Engineering in 1983 from University of Technology, Baghdad. Next, he was awarded the MSc and PhD degree from Loughborough University, UK, respectively in 1986 and 1990 in the field of Digital Communication Systems and Data Communication. From 1990- 2006, Professor Siddeeq worked with the University of Technology in Baghdad with participation in most of Baghdad's universities. From Feb. 2006 to July 2011 he was a Dean of Engineering College at the Gulf University in Bahrain. From Oct. 2011-Sep. 2015 he joined University of Mosul, College of Electronic Engineering as a Professor of Data Communication and next Dean of Research and Graduate Studies at Applied Science University, Bahrain till Sep. 2017. Presently, he is quality assurance advisor at Duhok Polytechnic University, Duhok ,Iraq. Through his academic life he published over 100 papers and a patent in the field of data communication, computer networking and information security and supervised over 100 PhD and MSc research students. He won the first and second best research in Information Security by the Arab Universities Association in 2003.

Shefa A. Dawwd received the B.Sc degree in electronic and communication Engineering, the M.Sc and the Ph.D degree in computer Engineering in 1991, 2000, and 2006, respectively. He is presently a faculty member (Associate Professor) in the computer engineering department / University of Mosul. His main research interests include image & signal processing and their hardware models, parallel computer architecture, hardware implementation and GPU based systems. He has authored more than 29 research papers. He has been an editorial member of several national and international journals.