INTERNATIONAL JOURNAL OF RESEARCH IN MECHANICAL, MECHATRONICS AND AUTOMOBILE ENGINEERING (IJRMMAE)
ISSN: 2454-1435 (Print) | 2454-1443 (online)
Volume 1 Issue 3 – www.ijrmmae.in – Pages 185-190

RADIO CONTROLLED SURVEILLANCE SYSTEM FOR BORDERS AND RESTRICTED AREAS

V.Velmurugan , Mohammed ismail,
AP/ECE, Department of Electronics and Communication Engineering,
Agni College of Technology , Thalambur.

ABSTRACT

Securing a country's border is not an easy task. Each country's border is an extensive and highly sensitive area, which often runs through difficult terrain. Usually it is impossible to continuously monitor the border by personnel only, as the border police force will always be short on personnel for a complete and continuous surveillance. The solution to monitoring and securing the border at all times is: Appliance of Highly Sophisticated Technology. Our paper titled Radio-Controlled Surveillance System for Borders and Restricted Area applies not only one, but various highly sophisticated technologies and consequently our border control system also consists of a PIR (Passive Infrared Sensor) to sense the human movement. The surveillance system is automated to fight against the intruders by turning on the sleeping gas tank (here: room sprayer). A web camera installed at the surveillance end capture and provides a constant data stream to a central command center when there is motion detection in the area to be monitored. All communication between such sensors and equipment is carried out by radio communication, in order to minimize the installation effort and to secure an uninterrupted, safe and secure operation.

Keywords: PIR, neural network, Biometric sensor.

1. INTRODUCTION

Each country's border is an extensive and highly sensitive area, which often runs through difficult terrain. Usually it is impossible to continuously monitor the border by personnel only, as the border police force will always be short on personnel for a complete and continuous surveillance. On the other side of the border there are the people interested in passing the border far away from the official border checkpoints. These could be professional smugglers of contraband, drugs and people, as well as illegal immigrants and the occasional trespassers. The set up of fences and walls often does not make sense for either political or financial reasons. Patrolling the border-by-border police is a personnel intensive effort – and the border patrols cannot be everywhere in any case. Furthermore, the vision of the border patrol personnel is impaired at night: Night-vision-binoculars can improve the border patrol personnel's abilities but still have a limited effect on the security of ones borders. This project overcomes all these difficulties by using an automatic sensing, surveillance and capturing mechanism.

II. LITERATURE SURVEY

Surface defect detection:

Steel strip is an essential industry raw material, and its surface quality is an important evaluation indicator. It is probably several kinds of surface detects (such as scratch, inclusion, scale, hole and pimple) when manufacturing steel strip because of billet, rolling equipment, techniques and so on. These flaws not only affect the appearance of the product, even more serious reduces the corrosion resistance, wear resistance and fatigue properties and so on. Simple surface defects like pits, bumps, scratches and hole create obvious problems for finishing operations, but more problematic is the fact that many times these defects do not become visibly noticeable until the operation is complete. Steel surface quality problems have been caused more and more concerned by the iron and steel enterprises.

Automatic metal surface inspection is a well known problem and is being considered for more than two decades. The steel quality control is currently done mainly by human visual inspection. Human inspectors classify the defects according to their cause and origin because the inspection results are used as feedback to correct the manufacturing process. The experience of the inspectors is essential, because there are no fixed defect criteria. The inspectors pass/reject decisions seem to be based on the types of defects and their extent, the maximum number of defects per unit of surface area and the total number of defects on the entire inspected strip. In addition the inspector's knowledge of the customer and the use of the strip have a great impact on the decisions. As the human visual inspection can provide a reliable quality control system for steel manufacturers. We are aiming through this research to detect steel defects by the image processing algorithm. Recently automatic visual inspection is popularly being used in that neural networks have taken major part for classification of defects according to image processing.

Existing system:

Traditionally steel sheets are inspected manually which is time extensive and labor intensive. Labor shortages and lack of overall consistency in the process resulted in a search for automated solutions; the development of machine vision system shows an improvement in efficiency. Recently automatic visual inspection is popularly being used. In order to find defects on steel surface edge preserving filter has been used. The image has been analyzed on separate x and y axis using laplacian filter. To analyze the horizontal coefficients double threshold was used and for vertical coefficient single threshold was used. But in thresholding method defect detection rate is less.[1][2]

Proposed System:

The surveillance unit has the following functions including: human presence detection, web camera enabling and disabling, triggering the video transmission module to transmit the video streams to the central command center wirelessly, making the alarm to siren and opening the valve of the sleeping gas tank to attack the intruders before the security personnel arrive at the intruded area. The wireless video transmission module consists of a web camera, video stream processor and the wireless video transmitter. The CMOS camera captures the video of the area to be monitored. The video stream processor does the streaming of the video frames. The streamed video signal is transmitted to the central command center using the broad bandwidth RF channel. The video transmission module is activated and deactivated by the control signal coming out of the microcontroller. The CMOS camera is turned only when any intrusion is detected.

III.BLOCK DIAGRAM

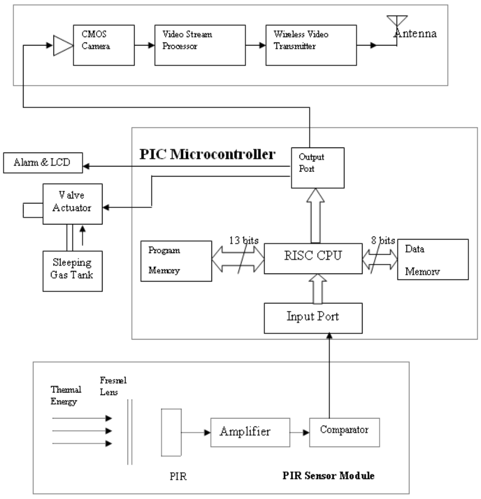

Figure 1: Block Diagram of Surveillance Unit

The surveillance unit has the following functions including: human presence detection, web camera enabling and disabling, triggering the video transmission module to transmit the video streams to the central command center wirelessly, making the alarm to siren and opening the valve of the sleeping gas tank to attack the intruders before the security personnel arrive at the intruded area.

The wireless video transmission module consists of a web camera, video stream processor and the wireless video transmitter. The CMOS camera captures the video of the area to be monitored. The video stream processor does the streaming of the video frames. The streamed video signal is transmitted to the central command center using the broad bandwidth RF channel. The video transmission module is activated and deactivated by the control signal coming out of the microcontroller. The CMOS camera is turned only when any intrusion is detected.

The PIR sensor module consists of PIR sensor, amplifier and the comparator. The PIR sensor is excited whenever the temperature changes in the sensitive area of the sensor. The temperature change is probably due to the movement of the human being. The reason is that each human being is capable of emitting heat source at the infrared wavelength. The low voltage signal from the sensor is amplified and converted into the bi-state voltage level, which is readable, by the microcontroller. Whenever the human motion is detected the output of the comparator goes high making the microcontroller to activate the Video module, alarm and the Sleeping gas tank valve.

In this paper, the usage of sleeping gas is not feasible. Hence the room sprayer is used. The valve of the room sprayer is controlled by the microcontroller depending upon the PIR module output. The alarm is also controlled by the micro whenever the intrusion happens.

When interfacing to the data memory block, EEDATA holds the 8-bit data for read/write and EEADR holds the address of the EEPROM location being accessed. These devices have 128 or 256 bytes of data EEPROM (depending on the device), with an address range from 00h to FFh. On devices with 128 bytes, addresses from 80h to FFh are unimplemented and will wraparound to the beginning of data EEPROM memory. When writing to unimplemented locations, the on-chip charge pump will be turned off. When interfacing the program memory block, the EEDATA and EEDATH registers form a two-byte word that holds the 14-bit data for read/write and the EEADR and EEADRH registers form a two-byte word that holds the 13-bit address of the program memory location being accessed. These devices have 4 or 8K words of program Flash, with an address range from 0000h to 1FFFh for the PIC16F877A. Addresses above the range of the respective device will wraparound to the beginning of program memory. The EEPROM data memory allows single-byte read and write. The Flash program memory allows single-word reads and four-word block writes. Program memory write operations automatically perform an erase-before write on blocks of four words. A byte write in data EEPROM memory automatically erases the location and writes the new data (erase-before-write). The write time is controlled by an on-chip timer. The write/erase voltages are generated by an on-chip charge pump, rated to operate over the voltage range of the device for byte or word operations.

Software interrupts are initiated with an INT instruction and, as the name implies, are triggered via software. For example, the instruction INT 33h issues the interrupt with the hex number 33h. In the real mode address space of the i386, 1024 (1k) bytes are reserved for the *interrupt vector table* (IVT). This table contains an interrupt vector for each of the 256 possible interrupts. Every interrupt vector in real mode consists of four bytes and gives the jump address of the ISR (also known as *interrupt handler*) for the particular interrupt in segment: offset format.

When an interrupt is issued, the processor automatically transfers the current flags, the code segment CS and the instruction pointer EIP (or IP in 16-bit mode) onto the stack. The interrupt number is internally multiplied by four and then provides the offset in the segment 00h where the interrupt vector for handling the interrupt is located. The processor then loads EIP and CS with the values in the table. That way, CS:EIP of the interrupt vector gives the entry point of the interrupt handler. The return to the original program that launched the interrupt occurs with an IRET instruction.

Software interrupts are always synchronized with program execution; this means that every time the program gets to a point where there is an INT instruction, an interrupt is issued. This is very different from hardware interrupts and exceptions as you'll soon find out.

HARDWARE INTERRUPTS

As the name suggests, these interrupts are set by hardware components (like for instance the timer component) or by peripheral devices such as a hard disk. There are two basic types of hardware interrupts: *Non Maskable Interrupts* (NMI) and (maskable) *Interrupt Requests* (IRQ).NMI in the PC is, generally, not good news as it is often the result of a serious hardware problem, such as a memory parity error or a erroneous bus arbitration. An NMI cannot be suppressed (or masked as the name suggests). This is quite easy to understand since it normally indicates a serious failure and a computer with incorrectly functioning hardware must be prevented from destroying data. Interrupt requests, on the other hand, can be masked with a CLI instruction that ignores all interrupt requests. The opposite STI instruction reactivates these interrupts. Interrupt requests are generally issued by a peripherical device.

Hardware interrupts (NMI or IRQ) are, contrary to software interrupts, asynchronous to the program execution. This is understandable because, for example, a parity error does not always occur at the same program execution point. This makes the detection of program errors very difficult if they only occur in connection with hardware interrupts.

EXCEPTIONS

This particular type of interrupt originates in the processor itself. The production of an exception corresponds to that of a software interrupt. This means that an interrupt whose number is set by the processor itself is issued. Exceptions occur generally when the processor can't handle alone an internal error caused by system software. There are three main classes of exceptions which will be discussed briefly. A fault issues an exception prior to completing the instruction. The saved EIP value then points to the same instruction that created the exception. Thus, it is possible to reload the EIP (with IRET for instance) and the processor will be able to re-execute the instruction, hopefully without another exception.

Trap: A trap issues an exception after completing the instruction execution. The saved EIP points to the instruction immediately following the one that gave rise to the exception. The instruction is therefore not re-executed again. Traps are useful when, despite the fact the instruction was processed without errors, program execution should be stopped as with the case of debugger breakpoints.

Abort: This is not a good omen. Aborts usually translate very serious failures, such as hardware failures or invalid system tables. Because of this, it may happen that the address of the error cannot be found. Therefore, recovering program execution after an abort is not always possible.

CONCLUSION :

Automation has been the keyword in this modern era of machines. Every process is being automated in this modern world. This project added one more area to the list of automations – Surveillance. Traditionally, providing security to a place only meant the use of manual forces. But, under conditions of extreme temperature and mountainous terrain, manual forces cannot withstand the onslaught of Mother Nature. In such cases, Automatic surveillance mechanisms are required.

Surveillance alone is just isn't enough. There is no point in seeing an intruder and just letting him go through. The intruder had to be captured. This project did just that. i.e. Both surveillance and capturing. A PIR sensor sensed humans passing through in the vicinity which in turn activated a CMOS camera and a sleeping gas controller. The sleeping gas sprayed made sure that the intruder did not escape. Also the entire scene can be watched at the control center because of the presence of a CMOS camera. Connecting the camera to the control room via high mountains was another problem faced. That was overcome by sending the audio and video by wireless means.Thus, with minimum manual effort, a human intruder in a far off place can be sensed and captured by the help of this Radio controlled Surveillance system.

FUTURE SCOPE

This project can be extended in many ways. A few of them are listed below. The range of PIR sensors is limited to a very particular area. So, this might not be all the more effective in sensing an object far away from it. To cover a wider area, some other sensing mechanism can be applied. The effect of sleeping gas on the intruder would wear off after a small period of time. Enough time must be given to the manual forces to retrieve the intruder. Some other alternate to sleeping gas can be considered. Wireless audio/video transmission is a power intensive operation. Some steps can be taken to minimize the power required. Compression techniques can be applied. Satellite imaging combined with this project can be more effective.

References:

[1].Baker.D (2006) 'Advances in Communications Electronic Warfare', Proceedings of IEEE Canadian conference on Electrical and computer Engineering, Vol.1, pp. 52-55

[2].Barna.C (2005) 'A testing method for PIR detectors system', Proceedings of International conference on computational Intelligence for modeling, control and automation, Vol. 2, pp. 995-998

[3].Gui.C and Prasant Mohapatra (2005) 'Virtual patrol: a new power conservation design for surveillance using sensor networks', Proceedings of the fourth international symposium on Information processing in sensor networks, Vol. 1, pp. 246-253

[4]Lu.R and Qi Hong (2006) 'Characteristics of a 12 domain MVA-LCD', IEEE Journal of Display technology, Vol. 2, Issue 3, pp. 217-222

[5.]Moghavvemi.M and Lu Chin Seng (2004) 'Pyroelectric Infrared sensor for intruder detection', Proceedings of TENCON 2004, IEEE Region 10 conference, Vol. 4, pp. 656-659

[6].Muller-Schneiders.S, Jager.T, Loos.H.S and Niem.W (2005) 'Performance evaluation of a realtime video surveillance system', Proceedings of 2nd joint international IEEE workshop on visual surveillance and performance evaluation of tracking and surveillance, Vol. 1, pp.137-143.

[7] E.J.S. Luz, G.J.P. Moreira, L.S. Oliveira, W.R. Schwartz, and D. Menotti, "Learning Deep Off-the-Person Heart Biometrics Representations", IEEE Transaction on Information Forensics and Security, vol. 13, no. 5, pp. 1258-1270, 2018.

[8] H. Kim and S.Y. Chun, "Cancelable ECG Biometrics Using Compressive Sensing-Generalized Likelihood Ratio Test", IEEE Access, vol. 7, pp. 9232-9242, 2019.

[9] M. Cadogan, PR Interval, [Online] Available: https://litfl.com/printerval-ecg-library/, Accessed on Apr. 24, 2019

[10] A. Nichole and B. Rodriguez, "Artificial intelligence for the electrocardiogram", Nature Medicine volume, vol. 25, pp. 22-23, 2019.

[14] A. Avati, "Evaluation Metrics", [Online]Available: http://cs229.stanford.edu/section/evaluation_metrics.pdf, Accessed in Feb. 1, 2019.

[15] Y. Zhu, X. Yin, X. Jia, and J. Hu, ''Latent fingerprint segmentation based on convolutional neural networks,'' in Proc. IEEE Workshop Inf. Forensics Secur. (WIFS), Dec. 2017, pp. 1–6.

[16] R. Cappelli, M. Ferrara, and D. Maltoni, ''Large-scale fingerprint identification on GPU,'' Inf. Sci., vol. 306, pp. 1–20, Jun. 2015.

[17] K. E. Hoyle, N. J. Short, M. S. Hsiao, A. L. Abbott, and E. A. Fox, ''Minutiae + friction ridges = triplet-based features for determining sufficiency in fingerprints,'' in Proc. IET Conf., Nov. 2011, pp. 1–6.

[18] D. Peralta, I. Triguero, S. García, F. Herrera, and J. M. Benitez, ''DPD-DFF: A dual phase distributed scheme with double fingerprint fusion for fast and accurate identification in large databases,'' Inf. Fusion, vol. 32, pp. 40–51, Nov. 2016.

[19] J. Li, J. Feng, and C.-C. J. Kuo, ''Deep convolutional neural network for latent fingerprint enhancement,'' Signal Process., Image Commun., vol. 60, pp. 52–63, Feb. 2018.

[20] K. Cao and A. K. Jain, ''Automated latent fingerprint recognition,'' IEEE Trans. Pattern Anal. Mach. Intell., vol. 41, no. 4, pp. 788–800, Apr. 2019.