REAL TIME INTRUDER SURVEILLANCE SYSTEM

Dr. K. Umapathy, T. Sri Devi, M. Navya Sri, R. Anuragh

Abstract—Internet of Things has become one of the most common aspect in our day-to-day life where the prominent aspect is Internet solely and people acquainted smart-phones which use internet. This paper describes about the execution of a sophisticated surveillance system which provides monitoring of intruder to homes thereby ensuring the security aspect. It utilize Raspberry pi, PIR sensor, Android Application, Pi Camera and also Finger Print Sensor. Since it’s preprogrammed and utilize Internet of Things it can be stated as “Smart” and straightforward to access by a human and it is purely economical.

Index Terms—Sophisticated, Raspberry pi, Android application, Smartphones, Pre-programmed, Internet of things

1 INTRODUCTION

Nowadays, safety and security has become inexorable. Since the recent technological influence has reached pinnacle, the demand for security systems are rising accordingly. With minimal human effort modern homes need smart systems. Pre-programmed security systems become more intelligent day by day with the arrival of digital and wireless mechanisms. A foreign view of his house can be accessed by a surveillance camera. Continuous observation of a place, person, group, or ongoing activity in order to gather information and detect intrusion defines the term “Surveillance”. In surveillance, Internet of things is a complex web of devices which bolsters it. The appliance helps the user to look at the house regularly and also in seeing who is entering the house when an alert is made.

2 LITERATURE SURVEY

“Visitor management system using raspberry pi”, [1] this paper aim is to replace the habit of passwords and RFID’s to access most highly secured systems and infrastructures with facial recognition.

“An Economical GSM/GPRS based wireless home security system” [2] this paper uses Zigbee and Beagle board for monitoring in real time security which will alert when amlaze and trespassing. It uses sophisticated techniques like camera, File Transfer Protocol server etc. Even though these ae important features it lacks in utilizing the alerting techniques such as calls, messages and electronic message etc. and also real time streaming technology.

“Monitoring in real time for home surveillance system which uses FTP server, Beagle Board and Zigbee”, [3] this paper uses IOT approach for motion detection using Pi. It uses File Transfer Protocol server for camera feeds and through electronic mail it also alerts user. This system does not have any type of alerts such as message and call.

“An IOT approach for motion detection using Raspberry Pi”, [4] this paper uses raspberry pi to explain the process of a monitoring system. The main drawback in the system is that whenever we need a real time stream we need to enter the respective Internet Protocol address frequently to observe the stream.

“Remote home surveillance system”, [6] this paper uses IP camera and Arduino board to explain the surveillance techniques. This paper describes the usage of a remote desktop application whenever the user wants to view it from outside. This technique won’t send any sort of notification to the user whenever anything suspicious happens at his place. As a consequence he has to continuously monitor his place and accordingly is that it lacks alerts based on sensors.

3 PROPOSED WORK

The brain of the system is Raspberry pi; it’s acting like server and also the controller. The pi receives the information from the sensor and can act in keeping with things (this is completed by coding). Here the camera is for both surveillance and also for the Face recognition.
When a motion is detected through PIR sensor, the camera is switched to face recognition, the system checks with the pre-loaded faces, **if there’s a match no alert is made and therefore the person can enter into the house by giving his/her fingerprint**, if there’s no match then an alert is made to a registered mobile, through the android application (only when internet is ON) and therefore the owner can question the unknown through the android application, this message is forwarded to Raspberry pi (conveyed to the unknown person through speaker), successively he can reply through Mic, and therefore the message is conveyed to the owner through android application.

Raspberry pi may be a low-cost credit-card sized single-board computer. The Raspberry pi utilize architecture of an Automated RISC Machine processor, moreover it is mostly utilized by up-to-date smart phones. The Raspberry Pi uses the Debian OS.

**TABLE 1**

<table>
<thead>
<tr>
<th>Surveillance</th>
<th>Audio input</th>
<th>Notification/ Received voice Message</th>
</tr>
</thead>
</table>

**Fig 2. Structure of Android Application**

**Fig 3. Raspberry Pi**

**Fig 4. Finger Print Sensor**
<table>
<thead>
<tr>
<th>Power</th>
<th>DC 4.5-5.0V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working current</td>
<td>Typical 40mA</td>
</tr>
<tr>
<td></td>
<td>Peak 150mA</td>
</tr>
<tr>
<td>Interface</td>
<td>UART (TTL logical level)</td>
</tr>
<tr>
<td>Baud rate</td>
<td>(9600/115200) Mbps, N=16,800</td>
</tr>
<tr>
<td>Image acquiring time</td>
<td>&lt;0.5s</td>
</tr>
<tr>
<td>Storage capacity</td>
<td>120,240,500</td>
</tr>
<tr>
<td>FAR</td>
<td>&lt;0.01%</td>
</tr>
<tr>
<td>Average searching time</td>
<td>&lt;1s (1:1000)</td>
</tr>
<tr>
<td>Working environment</td>
<td>Temp: -20°C to +40°C</td>
</tr>
<tr>
<td>RH</td>
<td>10%-85%</td>
</tr>
<tr>
<td>Outline Dimension</td>
<td>Size: 55.5 x 21 x 20.5 mm</td>
</tr>
</tbody>
</table>

**Fig 5. Pinout of Fingerprint Sensor**

**Fig 6. Pi Camera Module**

1. Raspberry Pi Camera Module
2. The lens which is capable of recording 4K, 1080P, 720P, 8MP still
3. Active Pixel Count is 3280 (H) x 2464 (V)
4. Power Supply of 2A is Highly Recommended

**Fig 7. Motion Sensor (PIR)**

1. Size: Rectangular
2. Price: $10
3. Output: Digital pulse high (3V) when triggered and digital low when idle.
4. Sensitivity range: up to 20 feet 110° x 70° detection range
5. Power supply: 5V-12V input voltage for most modules but 5V is ideal.
6. Lengths are determined by resistors and capacitors on the PCB and differ from sensor to sensor.
7. BIS0001 Datasheet (the decoder chip used)
8. RE200B datasheet (most likely the PIR sensing element used)
9. NL11NH datasheet (equivalent lens used)
10. Parallax Datasheet on their version of the sensor

**Fig 8. PIR Board Design and Pin Configuration**

1. Size: Rectangular
2. Price: $10
3. Output: Digital pulse high (3V) when triggered and digital low when idle.
4. Sensitivity range: up to 20 feet 110° x 70° detection range
5. Power supply: 5V-12V input voltage for most modules but 5V is ideal.
6. Lengths are determined by resistors and capacitors on the PCB and differ from sensor to sensor.
7. BIS0001 Datasheet (the decoder chip used)
8. RE200B datasheet (most likely the PIR sensing element used)
9. NL11NH datasheet (equivalent lens used)
10. Parallax Datasheet on their version of the sensor

4 RESULTS AND IMPLEMENTATION
After the detection of face, the Raspberry pi fragments every pixel into binary patterns and as well as Decimal patterns for the given image as shown in the Fig 9 (a). And further the process continues by extracting the image’s histogram and to LBP result (local binary pattern) and then finally to regions/grids such as Grid-X & Grid – Y as shown in Fig 9 (b).

![Fig 9. (a) Creating local binary pattern for image](image1)

![Fig 9. (b) Extracting histogram from image](image2)

![Fig 10. Extracted Histogram from an Image](image3)

![Fig 11. Output of Finger Print Sensor](image4)

![Fig 12. Video Streaming](image5)

![Fig 13. Motion Detection](image6)

5 CONCLUSION

Thus, this paper helps everyone protecting their house from thief, also from unknown when kids are alone in home. It’s self-controlling system, which may act in an intelligent way consistent with the condition. No alert is made when a known person face is detected, but they need to offer their Fingerprint to travel inside their house (When Locked). This can be implemented with home automation, safety of old persons and youngsters in future in order that most are safe and secured.

6 ACKNOWLEDGMENT

The authors wish to thank Ms. T. Srruthilaya, MTech (EDT), Trainee Engineer, National Institute of Electronics & Information Technology (NIELIT), Chennai.

7 REFERENCES


