Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

Smart Security System for Suspicious Activity Detection in Volatile Areas

Dr. Joy Iong Zong Chen,
Professor, Department of Electrical Engineering,
Da-Yeh University,
Taiwan.
Email id: jchen@mail.dyu.edu.tw

Abstract: The latest progress in the technology has led to automation and digitization in almost every fields, and has influenced a wide scope of application. This has caused enormous amount of data flow from each sectors, where the information contained in the data acts as the important component for the progress of the single person, organization, state, country and so on. These data with valuable information can be used in the constructive and the destructive perceptive based on the hands that handle it. So protective measures become very essential for preserving the data from unwanted access. This paves for developing a system to identify the suspicious movement in the volatile areas like military regimes, hospitals and financial organizations to safe the data. The method put forward in the paper incorporates the motion sensors and the face identification system to detect the suspicious activities and report to the lawful person. The algorithm for the system was developed using the python and tested for various sets of exemplary real time video recordings to know the accuracy in the detection.

Keywords: Smart Security, Suspicious Activity, Volatile Areas, Motion Sensors, Facial Identification.

Introduction

The two rapports which are entwined with each other are security and security. To avoid any inside or outside danger such as criminals or any person who aims to impede or undermine the organization's sustainable state, security measures are taken. The protection measures taken against the damages that may happen are known as the safety. The system to safe guard the data preserved in physical form in the volatile areas such as military regimes, hospitals, financial organization etc. From physical hacking for misuse is put forward in the paper. The system developed incorporates the sensors and the digital image processing to protect the confidential data such as the particulars of an officer, the machineries purchased, the case files and confidential letters in case of military offices, particulars of patients medical records in case of hospital, the particulars of the account details of the individuals the locker information's etc., in case of banks and even more., Apart from maintaining a system to discover the malicious network activities, the system to safe guard the physical data from the suspicious person is also very much necessary. So the method put forward scopes in developing a system to identify the persons involving in infrastructure sabotaging and performing unlawful access of sensitive information's.

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

The Internet of Things is nowadays a growing technology in the world. IoT's basic concept is to link every tangible thing to the internet so that it can communicate with other internet-connected devices and interchange information's and share the data in real time about the environment. Components with inbuilt sensor are linked to an IoT network that gathers data from multiple sources, examine the data in order to provide the highly valuable insights that can be helpful to specific needs. The present work utilizes the motion sensor (PIR Sensors) to identify the unwanted movements in the volatile areas. On identifying the doubtful movements the PIR sensor activates the detection system and enables the camera fixed to track the movement of the particular person.

These equipment's, equipped in sensing are capable of being controlled remotely using the portable devices empowered by internet. Many developing smart systems such as smart home, etc. comes under the embedded system empowered by internet. The most important goal of the facial recognition platform is the detection and authentication of an individual from a digital image. One way to do this is to compare the selection of facial features from the recorded image with the values in the data base that has the face features. The conventional approach suggests the detection of a person using a face recognition algorithm to extract facial features from the image of the subject's face. These algorithms used in extracting are categorized as geometric and photometric strategy.

The frames gathered according to the video captured using the web camera fixed are utilized in identifying the person involved in the illegal activity. It is the most significant part of the proposed frame the algorithm to recognize the face is relies on various aspects and circumstances. The work put forth is arranged with 2.literature survey, 3. Proposed work, 4. Result evaluation and 5, conclusion.

2. Literature Survey

The beginning of the era with automation and digital world always requires a safety and security measures as the data flow from different sectors have various security threats in different forms, either as malicious or suspicious activity through the network or physically over the data preserved in the network and physically respectively. These security systems might be a well- trained dog or person in charge of the area in the early days. Nowadays, the technological growth has led to utilization of modern equipment's in detecting the doubtful movements, minimizing the weariness of the humans and enabling an easy identification and tracking of person.

The literature survey presents certain security systems developed to secure the confidential data the author Freer, J. A et al [1] recommended the improvement to the previous work by putting forth the identification

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

based on the images captured using the CCTV engaged in surveillance. The images were produced in two different intensity levels and was coined as threshold and binaries.

The authors et al [2] and et al [3] has provided the detail of the facial recognition techniques utilized in the paper, the authors have developed the recognition based on the independent examination of the component and “cluttered images using a polynomial neural network” respectively. Viola et al [4], developed and utilized a separate algorithm termed as viola jones algorithm to perform a reliable identification. Oludele et al [5] developed an identification device enabled with the alarm to detect the unwanted activities.

Monzo et al [6] presents the comparative study on localizing the land mark of the face to identify the face utilizing the descriptors of the HOG. Ming et al [7] has devised the Efficient Kernel discriminate spectral regression for 3D face recognition." Shvachko et al [8] has performed the "The hadoop distributed file system." Suganthy, M et al [9] has conducted the "Principal component analysis based feature extraction, morphological edge detection and localization for fast iris recognition." Nguyen et al [10] has performed the "Low cost real-time system monitoring using Raspberry Pi."

Kodali et al [11] has performed the "MQTT based home automation system using ESP8266." Javare et al [12] has performed the. "Access control and intrusion detection in door lock system using Bluetooth technology." Muema, et al [13] presents the "Application of benchmarking and principal component analysis in measuring performance of public irrigation schemes in Kenya."

Raj, J. S et al [14] has presented the “QOS Optimization of Energy Efficient Routing in Iot Wireless Sensor Networks.” Kumar, R et al [15] has elaborated the "A novel report on architecture, protocols and applications in Internet of Things (IoT)." Pandian, A. P. et al [16] has puts forth the “Artificial Intelligence Application in Smart Warehousing Environment for Automated Logistics” Wang, H et al [17] devised a “Sustainable Development and Management in Consumer Electronics Using Soft Computation”

3. Proposed Work

The images of the head and the co- workers information who are authorized to enter the volatile areas are stored in the face database of the proposed model. The installation of the proposed model is carried out in the place where the data are preserved and the monitoring required. The structure of the proposed model is encompassed with the camera followed by the motion sensor (PIR-sensor) and the alarm module that raises alarm when activated. The block diagram below in figure.1 is the proposed frame work for the security system.

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

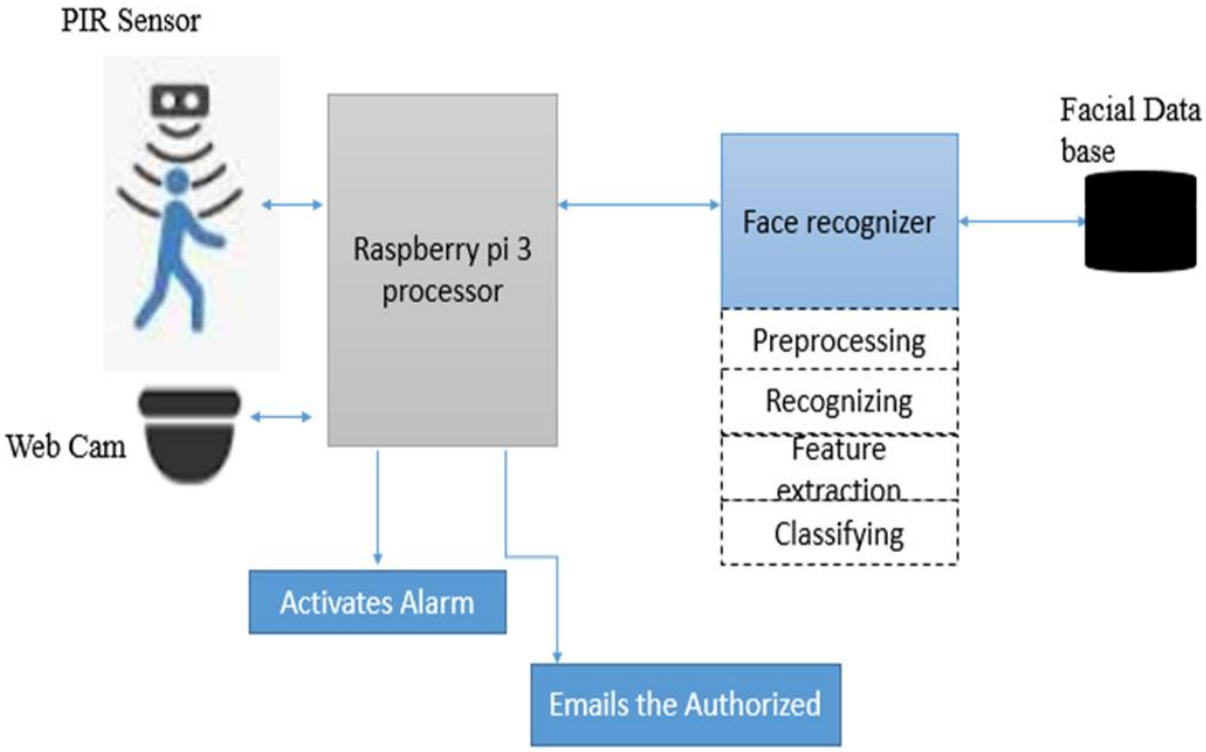

Figure.1 Proposed Frame Work

On detecting the any movement taking place in the restricted area the camera is immediately turned on, and the image of the person s captured and compared with the faces in the data base if the match fails then alarm system is activated and an email alert is sent to its lawful person. The proposed model is encompassed with the raspberry pi processor to process the information gathered and sent it to the required person to verify the authenticity of the person. The processor is programmed accordingly using the Java Script. The flow diagram below in figure.2 shows the process carried in the proposed frame work.

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

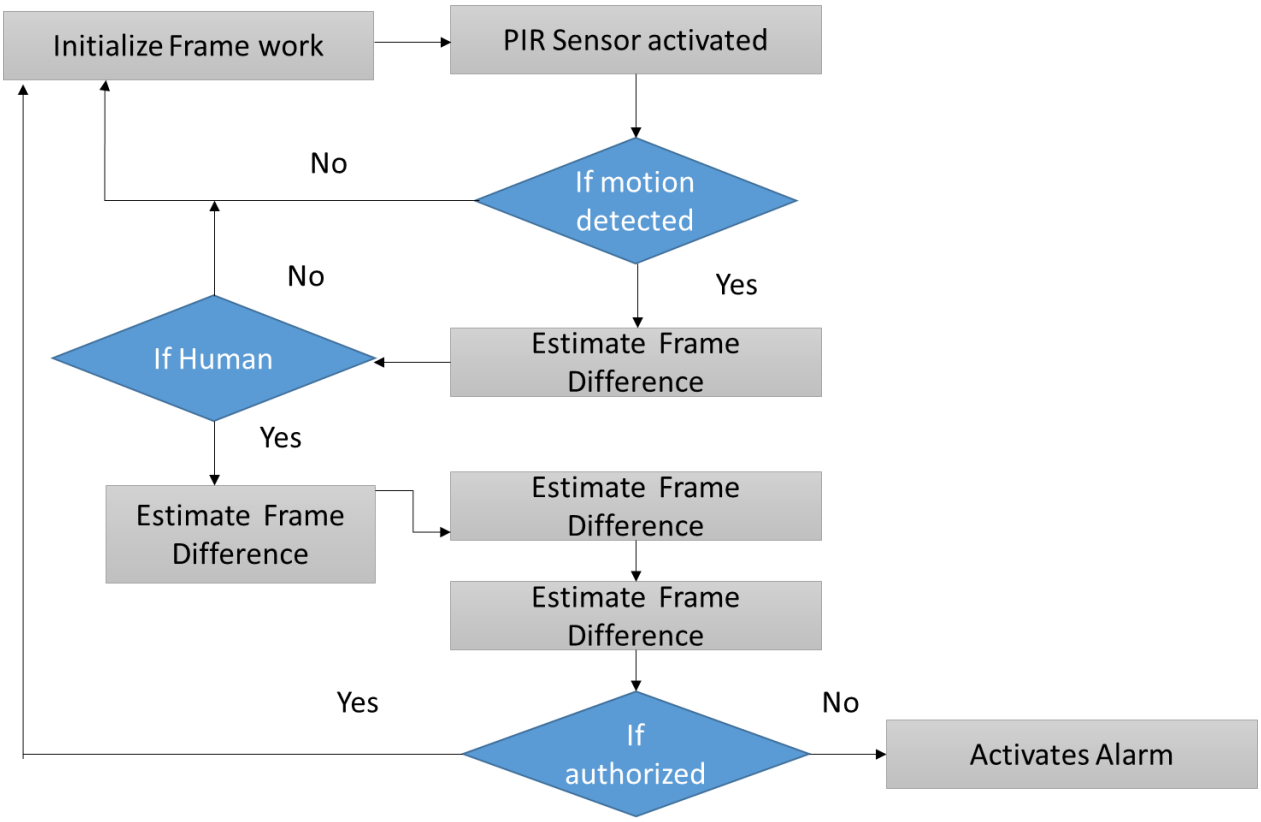

Figure.2 Flow Process of Proposed Frame work

The PIR sensor involved in detecting the movement of the human based on the framing difference, senses the motion according to the heat dissipated from the human body, the variation in the temperature in the atmosphere due to the movement of the humans is identified by the sensor and this is used in activating the camera.

The pseudo code for the Movement Identification is presented below in figure. 3 below

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

```
Algorithm Movement Detection (var a)
{ b := average of selected color in frame
1;
if abs(a-b)> threshold then
Movement Detected;
. else
 { wait(x seconds);
Algorithm Movement Detection(b);
}
}
```

Figure.3 Movement Detection

The process of facial recognition is done using the employing the K-nearest neighbor and the viola jones algorithm. The fundamental procedure involved in the process of recognizing the face, are listed below

1. The image captured in the camera is computed to get the rectangle attributes and for this is the image is characterized into an integral form. The value of the integral image is obtained by summing up the pixels above to the left point coordinate (x, y) the equation.1 below gives the integral form of image.

$$ij(x,y) = \sum_{x'<xy'<y} i(x',y') \qquad (1)$$

While $ij(x,y)$ is the image in integral form and $i(x',y')$ is the actual image. The classification is performed using the Ada Boost

2. The classifiers are connected in cascade to remove the image back ground and as well as elude the negatives and activate the analysis with the positive instance.
3. The repeated and the unnecessary data are removed in the preparing stage, by utilizing the principal component analysis that uses the orthogonal transformation. The process transforms the value of the images into values that could be probably correlated with the principal components and the extracted features are categorized using the K-NN.

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

The data‘s streamed are reserved in the HDFS the streaming of the data are performed without intervention using the Spark,

4. Results Evaluation

The proposed model is tested with the set of random images captured in the real time,, the images of the authorized person of the organization who could handle the secret repository are fed into the face data base. Now the model is tested with the random images of the worker in the organization based on the results of the face recognized the alarm system is activated. So the accuracy in detection is very important. The complete process implemented using the python and the Java, and tested for the accuracy in detection as the entire process relies on the accuracy of the detection. The accuracy is tested evaluated in the MATLAB, the Classifier are trained with only the authorized users and so any person apart from the authorized would be considered as the intruder.

The testing data set involves both the authorized as well as the unauthorized users. The figure.3 below presents the accuracy of the system in the process of training and testing, as well as classifying the authorized from the intruder.

Figure.3 Accuracy and Error in Training and Testing

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 01
Pages: 64-72
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.1.006

Based on the results observed and the accuracy and error incurred in the system ii is clear that the proposed model work 98.45% effectively in identifying the intruders. The accuracy achieved in the classification process and the error percentage incurred both in the training and testing proves this. So the proposed model helps in efficiently detecting the unwanted entries and reporting to the authorities.

5. Conclusion

The proposed method identifies and intimates the movement of the unauthorized by employing the motion sensors and the face detection algorithms. The proposed method engages the passive infrared sensor for the identifying the movements and viola jones for recognizing the face and KNN in classifying between the authorized and the unauthorized. The proposed method is tested using the random set of real-time images and the accuracy achieved proves that the proposed method is classifies effectively and intimates to the rightful by activating the alarm. The future process aims in live recording utilizing the cloud service and activating control using the mobile application.

References

[1] Freer, J. A., B. J. Beggs, H. L. Fernandez-Canque, F. Chevrier, and A. Goryashko. "Automatic video surveillance with intelligent scene monitoring and intruder detection." In *1996 30th Annual International Carnahan Conference on Security Technology*, pp. 89-94. IEEE, 1996.

[2] Bartlett, Marian Stewart, Javier R. Movellan, and Terrence J. Sejnowski. "Face recognition by independent component analysis." *IEEE Transactions on neural networks* 13, no. 6 (2002): 1450-1464.

[3] Huang, Lin-Lin, Akinobu Shimizu, Yoshihiro Hagihara, and Hidefumi Kobatake. "Face detection from cluttered images using a polynomial neural network." *Neurocomputing* 51 (2003): 197-211.

[4] Viola, Paul, and Michael J. Jones. "Robust real-time face detection." *International journal of computer vision* 57, no. 2 (2004): 137-154.

[5] Oludele, Awodele, Ogunnusi Ayodele, Omole Oladele, and Seton Olurotimi. "Design of an automated intrusion detection system incorporating an alarm." *arXiv preprint arXiv:0912.3921* (2009).

[6] Monzo, David, Alberto Albiol, Antonio Albiol, and Jose M. Mossi. "A comparative study of facial landmark localization methods for face recognition using hog descriptors." In *2010 20th International Conference on Pattern Recognition*, pp. 1330-1333. IEEE, 2010.

[7] Ming, Yue, Qiuqi Ruan, Xiaoli Li, and Meiru Mu. "Efficient Kernel discriminate spectral regression for 3D face recognition." In *IEEE 10th INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING PROCEEDINGS*, pp. 662-665. IEEE, 2010.

[8] Shvachko, Konstantin, Hairong Kuang, Sanjay Radia, and Robert Chansler. "The hadoop distributed file system." In *2010 IEEE 26th symposium on mass storage systems and technologies (MSST)*, pp. 1-10. Ieee, 2010.

[9] Suganthy, M., and P. Ramamoorthy. "Principal component analysis based feature extraction, morphological edge detection and localization for fast iris recognition." *Journal of Computer science* 8, no. 9 (2012): 1428.

[10] Nguyen, Huu-Quoc, Ton Thi Kim Loan, Bui Dinh Mao, and Eui-Nam Huh. "Low cost real-time system monitoring using Raspberry Pi." In *2015 Seventh International Conference on Ubiquitous and Future Networks*, pp. 857-859. IEEE, 2015.

[11] Kodali, Ravi Kishore, and SreeRamya Soratkal. "MQTT based home automation system using ESP8266." In *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, pp. 1-5. IEEE, 2016.

[12] Javare, Amirush, Tushar Ghayal, Jayant Dabhade, Ankur Shelar, and Ankita Gupta. "Access control and intrusion detection in door lock system using Bluetooth technology." In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 2246-2251. IEEE, 2017.

[13] Muema, Faith M., Patrick G. Home, and James M. Raude. "Application of benchmarking and principal component analysis in measuring performance of public irrigation schemes in Kenya." *Agriculture* 8, no. 10 (2018): 162.

[14] Raj, J. S. (2019). Qos Optimization of Energy Efficient Routing In Iot Wireless Sensor Networks. Journal of ISMAC, 1(01), 12-23.

[15] Kumar, R. Praveen, and S. Smys. "A novel report on architecture, protocols and applications in Internet of Things (IoT)." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1156-1161. IEEE, 2018.

[16] Pandian, A. P. (2019). Artificial Intelligence Application in Smart Warehousing Environment for Automated Logistics. Journal of Artificial Intelligence, 1(02), 63-72.

[17] Wang, H. (2019). Sustainable Development and Management in Consumer Electronics Using Soft Computation. Journal of Soft Computing Paradigm (JSCP), 1(01),56.