Controlling Software and Hardware Theft in college Laboratory through Image Processing

Darshan Bhadane , Information & Technology, MIT Pune , Pune-38
Mrs.Sajeeda Shikalgar , Information & Technology, MIT Pune , Pune-38

Abstract

Theft is being always a biggest threat to the security of the premises which leaves the owner of the premises completely shuttered. This theft is even a curse at the educational organizations where theft of any equipment or any hardware peripherals always creates a havoc to the other students. This theft includes the theft of software and hardware by the known or unknown persons who access the facility on the premises. So to deal with this kind of scenario proposed methodology put forward an idea of providing a security for the data and also to the devices. Proposed model allows the admin of the system to register the students with their images. So as the registered or unregistered student access the computer on the premises then based on the permission given to them, the system will shut down to prevent any data theft. On hardware theft like mouse and keyboard proposed model will raise an alert to inform the admin. This model is deployed using the face detection and recognition using the Deep convolution neural network.

Keywords: Convolution Neural network, Image Normalization, Theft Detection, Alert generation.

I. INTRODUCTION

Due to advancements in the technology, there can be video surveillance done on a particular area to keep it safe from intruders or thieves. This is highly useful to maintain the security of the items being safeguarded and it achieves by providing a form of the constant vigil on the target for any signs of malpractice. It is usually done in the case of shops where shoplifting is quite rampant. This technique can be readily used by the owner to nab the perpetrators and prevent a loss from occurring to his establishment.

Usually, surveillance with the help of a video is done by a CCTV camera which stands for a Closed-Circuit Television. Most of these Video surveillance techniques utilize the cameras to record theactivity in the premises and keep it stored for future viewing that can be done in case something is missing or a crime has occurred. But this is cumbersome as recording the video will take up a lot of memory in the hard disk and it would constantly be recorded onto the hard disk lower its life expectancy.

Due to the fact that the camera is constantly recording a video, it can degrade the quality of the hard disk over time, with bad sectors and other wear that happens on a Hard disk. To ameliorate this effect many owners do not keep recording all the time as it would suggest, but rather, they employ a technique to just capture footage when activated by an external stimulus. Therefore, as the act of theft occurs, it can be easier to identify the exact moment and also save valuable time searching through an entire days' worth of footage to identify the criminal.

Most of these, techniques, such as the selective recording of the footage can only be possible with the installation of additional hardware, such as laser trip wires and other sensors, such as motion detectors to determine the exact timing when there is an intrusion. These sensors make it easier to start recording only the essential aspects of the footage, thereby saving the hard disk and other energy expenditures.

The integration of such hardware can ensure that no time is wasted in the searching through the entire footage to gather the footage of the actual crime being performed. But this technique does not come with its demerits, such as the heavy cost of installation and maintenance of such features. Most of these sensors are highly sensitive, as they have to capture even the minutest movement in their surroundings, but unfortunately, that could mean that there can be a lot of false alarms that can occur even if an insect triggers one of the sensors.

Therefore, there needs to be a better implementation of surveillance that can be implemented to achieve a higher degree of accuracy without any major downsides.

This is achievable through the implementation of Image processing paradigm in the surveillance system. This is highly useful as it would be easily able to identify the theft at the right time by analyzing the footage in real-time.

Image Processing is an advanced technique that can process an image to get an enhanced image that can be used to isolate useful information from the image. The image can be a photograph or it can also be a frame in a video. The basic crux of image processing is the technique of signal processing which is at its core which analyses and extracts the information from the image. Therefore, an image processing technique can be trained to look out for potential attackers and thieves that can be identified from the footage. It also negates the use of sensors and other equipment to help reduce the cost of deployment.

This research paper dedicates section 2 for analysis of past work as literature survey, section 3 deeply elaborates the proposed technique and whereas section 4 evaluates the performance of the system and finally section 5 concludes the paper with traces of future enhancement.

II. LITERATURE SURVEY

M.Saad [1] explains that the distribution of electricity plays an important roleas it measures the consumption of users and generates the bill. In recent years, the electricity providerstarted using the conventional credit billing system. Later on, it resulted that this electrical metering was faulty as some severe problems were discovered and the electricity that was used generated a large bill and meter reading was not inappropriate due to this here was a large amount of profit and loss of power due to electricity theft.

S.Dupuis proposes a paper logic encryption technique that is used to protect ICs from the mask theft and from the unauthorized production of ICs[2]. To protect the ICs from the unauthorized users is to keep IC activated with the external keys. This encryption technique helps protect from theHardware being attacked by Trojan insertion. Just by imagining that the attacker will attack the hardware a Trojan is added to the signals with low controllability. This shows the quality of the encryption, which is essential to prevent an attacker from inserting a stealthy Hardware Trojan.

S.Nagpal introduces that in non-urbanparts of the country the theft in the farms are the most common thing but the farm's owners suffer from the loss in various ways. If an unauthorized person or animal enters the farm, they may steal the farm products or they can damage the crops on the farm. To provide a solution to this, the author has proposed the present paper where they implemented the wireless sensor in the network. The system is developed such thatit is very essential to monitor the boundaries of the farm to detect movement of unauthorized entries into the farm.These sensors continuously sense the movement in the farm through Radio- frequency transceiver and give an alert on the mobile if anything suspicious happens.[3]

T.Arafin[4] elaborates that the authors haveprovidedtheir solution on the hardware security problem to fight against the IC counterfeiting. They have provided the integration efforts deployability, and security matrices so it can help design the security measures for safeguarding the product supply to secure the IP theft. There is not much research made on this kind of theft detection the advantage for this kind of project is that they can be easily maintained by comparison of various techniques and the due cost of maintaining an anti-counterfeit program, lack of technological advancement for testing design and system integrity during runtime, cost of recycling and regulated disposal, cost of maintaining the database of failed and replaced parts, compliance with regulations, and an overall apathy towards counterfeiting.

V.Jyothi aimsto identify the malicious energy theft that had occurred in the intrusion detection system asthe only solution for it is an integrated intrusion detection system. Most of the smart metering system uses the traditional analog in the smart metering system.Recently there has been development of an advanced metering infrastructure available as a crucial element of a smart grid and they have replaced with the traditional one. In the present paper the AMIDS intrusion detection they have used sensors for the consumption data from the smart meter to more accurately to detect the energy. The results of the paper show accurate information about fusion and triggering alerts.[5]

D.Maiproposes a system in this paper as it already generates analert to the owner if someone has tried to steal their motorbike. This technique is based on human activity recognition and object detection by using cameras[6]. They have analyzed the activity of thieves captured by the cameras being used for detecting theft. Then the system will generate an alert and activity sequence of the thieves and send it to the user.

S.Sahoo elaborates thatthieves finddifferent ways to steal power and other power resources from the grid. In the proposed methodology a temperature dependent predictive model has used data from the distribution transformer to detect electricity used, by utilizing the smart meter[7]. The resulted has been model tested on different sites to find different ways ofpower theft. This model is one of best techniques when compared to the previous research which was done for the electrical theft detection which can be used for the real-world application.

K.Mandavillestates thatin recent years use of devicessuch as laptops, mobile, phones as increased and simultaneously there also complaints of these things beingstolen. According to an FBI survey 1 in every 10 laptops purchased will be robbed within the 12 months and out of that only 3 percent will be returned. The system has developed a new technique;an automatic method detector to find the stolen items by using the clustered network[8]. In this technique, the stolen things are searched on the basis of the logging information within the network activity and it should be found in very less amount of time if it is processed in a single system.

P.Sreedevi explains that Humans are highly possessive of their belongings and due to this they need the access control security system in recent time. There are various types of security provided one of it is a security called as face authentication. In the proposed methodology as the owners of the car are always in fear of having their vehicles stolen from a common parking lot or from outside their home. Image processing is used for the authentication process if any driver tries to access the vehicle their system will capture an image of the driver and check whether the driver is authenticated or not if not it will generate the alert.The system result is technologically system is simple, accurate and maintainable.[9]

M. Tariq expresses that in recent years there has been vast growth made in the field of the electrical sector there is an evolution of the electricity grid and this intelligence of decentralized generation has materialized in the form of a distributed power grid called as the microgrid. This microgrid is one of the small-scalegrids is used in distributed generation and in distributed storage [10]. In this paper wireless sensor network is engaged with the temperature sensor (RTS) nodes, and it is used in MG distribution network to measure the line resistance. Thus, the experiments detect 100% accuracy without knowing the distribution network

R.Punmiya[11] elaborates on Smart grid energy theft identification of gradient boosting theft detector (GBTD). Gradient boosting theft detector (GBTD) has basically three types of latestgradient boosting classifiers (GBCs): an extreme gradient boosting (XGBoost), categorical boosting (CatBoost), and light gradient boosting method (LightGBM). By using the stochastic features like standard deviation, mean, minimum, and maximum value of daily electricity usage a false positive rate is generated.Thus, the proposed method is beneficial for commercial use.

S.Shammi explains thatevery car owner always has the fear of the vehicles being stolen from the parking lot or from outside of the house. To secure the car or the bike there are some security measures taken into consideration by using the images and video processing. They provide the best solution by giving the idea of CCTV to secure the car from the theft. Due to CCTV cameras, there is a decrease in the percent of the car getting stolen but it has one drawback that the system is non-automated human monitoring of vehicles and can have human errors or lapses due to human fatigue.Thus, edge detection method is used as the proposed methodology for the prevention of vehicle theft detection.[12]

M.Nabil[13] Electric theft results in the loss in financial losses for several countries thus to avoid this the authors have implemented a general RNN-based electricity theft detector as the Modern smart grids rely on advanced metering infrastructure (AMI) networks for monitoring and billing purposes. These experiments are quite susceptible and may suffer from cyber-attacks. Therefore, the proposed RNN-based detector achieves a detection rate of up to 93%.The proposed data is more robust against attacks as it does not depend on customer data.

III PROPOSED METHDOLOGY

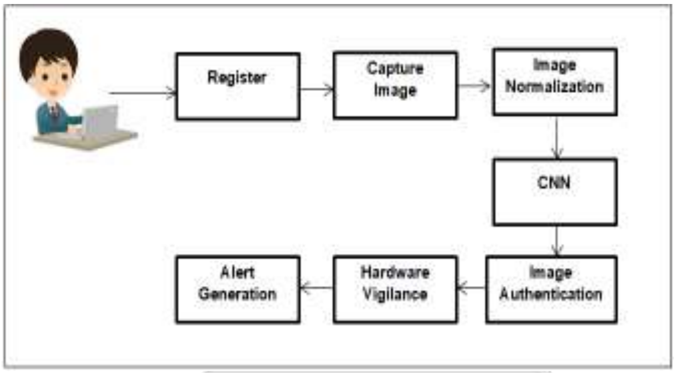


Figure 1: Proposed Methodology System Overview

The proposed methodology for hardware and software theft from the laboratory is depicted in the figure 1. The steps that involve in the methodology is described in the below mentioned steps.

Step 1: User registration and Image storage - This is the initial step of the proposed model, where Lab admin registers all the students along with their images. All the user attributes are stored in the database, whereas the user image is captured through the Java Media Files (JMF) API to store in a specific directory with the user name as the image file name.

Step 2: Image normalization- Once the student is registered and they access the computer, then his/ her current image is captured to authenticate the image. Authentication process involves the image normalization as the first step. Here based on the best image which is being authenticated properly for the available amount of light is considered as the model image.

Now all other images that need to be authenticated are normalized according to the model image so that the faces are getting authenticated properly. So in the process of normalization initially the model image is subjected to estimate its mean of RGB color channel. The obtained mean RGB color channels are set to identify the difference between the mean of the RGB color channel of the current images. The evaluated difference is applied to the all the values of the RGB of each and every pixel. Then the values of the RGB channels are normalized if they cross more than 255 or less than 0. By doing this the current image will get the same light effect as of the model image, that eventually helps to authenticate the current face more properly using Convolution neural network. This can be denoted by the equation 1 and 2 below.

$$\mu = \frac{(\sum_{i=1}^{n} RGBi)}{n} \qquad \_\_\_\_\_(1)$$

Where
µ - Mean of the RGB
RGB_i - RGB of instance pixel
n - Number of pixels in the image

$$\int_{i=0}^{n} RGBi + (\mu m - \mu f) \qquad \_\_\_\_\_\_\_\_\_\_\_(2)$$

Where
μ_m - Mean of the RGB of model image
μ_f - Mean of the RGB of current image
RGB_i - RGB of instance pixel
n - Number of pixels in the image

Step 3: Convolution neural network - This the core part of the proposed model here face of the student is authenticated to check the access control allocated to him. The first step that involves in the authentication process is First Layer.

First Layer - Here in the first layer both the stored image and the current images are resized to a fix size. Then these images are converted into the gray scale images by averaging the RGB color channels to fix them again into the pixel. After this process the whole image is divided into the decided number of blocks to match the face.

Deep layer - Here in this process the every decided blocks of the both current image and stored images are evaluated for their average brightness. Then this brightness of each block is checked for their absolute difference. If the difference is less than the 25, then the block is said to have zero difference and count that block as matched one. This process is iteratively perform on all other blocks to get the count and check for the maximum number of the count. The stored image with maximum count is matched with the given image to authenticate the image. This process can be shown in the below mentioned algorithm 1.

Algorithm 1: Deep Layer for face Authentication

```
// Input: Sample face $S_I$, Stored face $ST_I$
// Output: Boolean FLAG =TRUE or FALSE
Function: faceAuthentication($S_I$, $ST_I$)
Step 0: Start
Step 1: FLAG=FALSE
Step 2:count=0
Step 3: BLOCKx= $S_I$ / 8
Step 4: BLOCKy= $S_I$ / 6
Step 5: for i=0 to 8
    Step 6: for i=0 to 6
        Step7:b1=averageBrightnessof($S_I$ „BLOCKxi, BLOCKyj )
        Step8: b2=averageBrightnessof($ST_I$ „BLOCKxi, BLOCKyj )
        Step 9: Diff=0
        Step 10: k=| b1-b2|
        Step 11: if ( k<=25) THEN
            Step 12: Diff=0
            Step 13: count++
        Step 14: ELSE
            Step 15:DIFF=k
    Step 16: End for
Step 17: End for
Step 18: if ( count==48)
    Step 19: FLAG=TRUE
Step 20: return FLAG
Step 21: Stop
```

Step 4: Hardware Theft and Alert generation- Once the face is checked for the authentication. If the face is not authenticated, then it means some unknown person is intruded the computer. So the proposed model shut down the computer immediately. On the other hand, if the face is authenticated, then it is checked for the access control from the admin. If the access control is "yes" then the system allows the user to use USB storage devices. If the access control is "no" then system waits till the student uses the USB storage devices. As the unauthorized student uses the USB device, then model inform the admin and shut down the system immediately. The other hardware theft is managed like unplugging the mouse using the port listening mechanism. In this case also system immediately raises voice alert in the laboratory to take proper action.

IV RESULT AND DISCUSSIONS

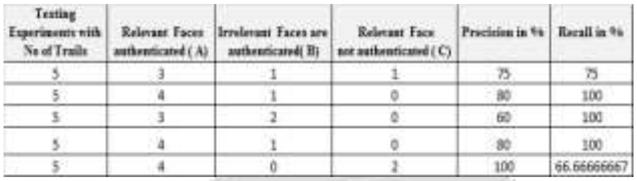
Face authentication technique elaborated in this paper has been successfully implemented with various equipment such as a D-Link Wireless double antenna router for managing the Local Area Network. There are some machines used for the deployment of this technique, all of which feature a Core i5 as their CPU with 6GB of physical memory. All of the client machines are equipped with a camera for capturing the student's Face for authentication. The methodology was coded in the Java programming language on Netbeans IDE and the database responsibilities were handled by Mysql.

The proposed technique was extensively tested to ensure optimum performance and efficiency. The affectivity of the system has been measured in one of the best parameters, Precision and Recall. This Experiment with Precision and Recall is elaborated below.

A = The number of relevant face are authenticated.
B= The number of irrelevant face authenticated.
C=The number of relevant faces not authenticated.

So precision can be given as

Precision = (A / (A+ B)) *100
Recall = (A / (A+ C)) *100



Testing Experiments with No of Trails	Relevant Faces authenticated (A)	Irrelevant Faces are authenticated(B)	Relevant Face not authenticated (C)	Precision in %	Recall in %
5	3	1	1	75	75
5	4	1	0	80	100
5	3	2	0	60	100
5	4	1	0	80	100
5	4	0	2	100	66.66666667

Table 1: Precision and Recall Experiment details

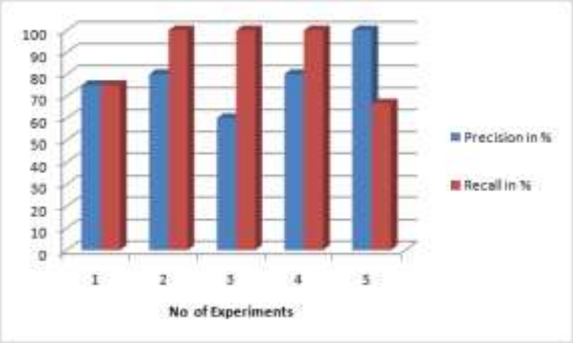


Figure 2: Precision and Recall Comparison

The table and graph plotted above depicting the scores obtained from the Precision and Recall. The presented technique has visibly achieved very high scores which are in the range of 80% Recall and 88% Precision for the successful authentication via biometric Face Recognition. The obtained precision and recall are evaluated under very constrained environment of the camera of 1.3 mega pixel only. So this is a good achievement in face recognition technique in the very first attempt of using CNN.

V CONCLUSION AND FUTURESCOPE

The model of hardware and software theft detection is deployed in the college laboratory for the theft of some software via USB storage device through injection technique. Whereas hardware thefts of some devices like the mouse and other USB devices are detected and alarm are raised using the port listening techniques. The alarms are raised and access is controlled over the authentication of the student who are using the computers in the college lab. The facial authentication scheme is carried out using the convolution neural network. The obtained accuracy of precision and recall are estimated at around 80% and 88%, which are pretty good in the constrained environment of 1 .3 mega pixel camera of the laptop.

In the future this system can be deployed in real time CC TV cameras and enable the admin to monitor all the camera vides via his interactive mobile application.

REFERENCES

[1]Muhammad SaadMuhammad Faraz Tariq, Amna Nawaz, Muhammad Yasir Jamal, “Theft Detection Based GSM Prepaid Electricity System”, IEEE 3rd International Conference on Control Science and Systems Engineering, 2017.

[2]Sophie Dupuis, Papa-Sidi Ba, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, “A Novel Hardware Logic Encryption Technique or thwarting Illegal Overproduction and Hardware Trojans”,IEEE 20th International On-Line Testing Symposium (IOLTS), 2014.

[3]Shobhit Kumar NagpalP. Manojkumar, “Hardware Implementation of Intruder Recognition in a Farm through Wireless Sensor Network”,International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 2016.

[4]Md Tanvir ArafinAndrew StanleyPraveen Sharma, “Hardware-Based Anti-Counterfeiting Techniques for Safeguarding Supply Chain Integrity”,IEEE International Symposium on Circuits and Systems (ISCAS), 2017.

[5]Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier, and Saman Zonouz,” A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructures”,IEEE Journal on Selected Areas in Communications, Vol. 31, No. 7, July 2013.

[6]Dung Mai and Kiem Hoang, “Motorbike Theft Detection Based on Object Detection and Human Activity Recognition”,International Conference on Control, Automation and Information Sciences (ICCAIS), 2013.

[7]Sanujit Sahoo,Daniel Nikovski,Toru Muso and Kaoru Tsuru, “Electricity Theft Detection Using Smart Meter Data”,IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2015.

[8]Kartik Mandaville, Saurabh Suman, Varun Thacker, Ashwath Rao B, “Theft Detection of Computers using MAC address by Map-Reduce Programming Model on a Cluster”, International Conference on Recent Advances in Computing and Software Systems, 2012.

[9] Pazhampilly Sreedevi, Sarath S Nair, “Image Processing Based Real Time Vehicle Theft Detection andPrevention System”,International Conference on Process Automation, Control and Computing, 2011.

[10]Muhammad Tariq and H. Vincent Poor, “Real Time Electricity Theft Detection in Microgrids through Wireless Sensor Network”,IEEE Sensors, 2016.
[11]Rajiv Punmiya and Sangho Choe, “Energy theft detection using gradient boosting theft detector with feature engineering-based preprocessing”, IEEE Transactions on Smart Grid, 2019.

[12]Sayma Shammi, Sayeed Islam, Hafiz Abdur Rahman, Hasan U. Zaman, “An Automated Way of Vehicle Theft Detection in Parking Facilities by Identifying Moving Vehicles in CCTV Video Stream”,International Conference on Communication, Computing and Internet of Things (IC3IoT), 2018.

[13]Mahmoud Nabil, Muhammad Ismaily, Mohamed Mahmoud, Mostafa Shahiny, Khalid Qaraqey, andErchin Serpedin, “Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-parameters”, 24th International Conference on Pattern Recognition, 2018.

****