1-2022

The Privacy Leakage of IP Camera Systems

Lee R. Castro
Montclair State University

Abstract

For in-home security, intelligent operations like top individual recognition and minimizing losses due to home break-ins, emergencies, and fraud are keys to success. This application integrates the closed-circuit television (CCTV) camera and the deep learning algorithms used to process these images. Automated intrusion detection alerts, real-time fire alerts, smart checkout, and potentially fraudulent point of sale (POS) transactions are its main features. Dynamic intrusion with machine learning is a software program in which the price of certain products changes over time through an algorithm that considers a variety of pricing variables. The face locator is a part of the algorithm that locates and detects motion by using the image search function. The system collects all available product locations from the live videos from multiple cameras. This is a helpful feature for finding misplaced products and detecting POS user fraud. This intrusion detection system (IDS) records POS transaction details on the screen as an overlay on video images to reduce home break-ins. To improve the ease and speed of transaction searches, the faces of individuals are used to search for disputed cases. Smart Checkout System (SCS) utilizes a self-service kiosk where users can generate bills by showing products to the linked camera. SCS uses Google vision technology to identify products. Motion detector and queue detection will detect long queues at the checkout counter in real-time and open new lanes to speed up the transaction, improve the experience, and reduce the number of abandoned purchases. Face recognition premium and alerts can also be provided.

MONTCLAIR STATE UNIVERSITY

The Privacy Leakage of IP Camera Systems

by

Lee R. Castro

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

January 2022

College of Science and Mathematics

Department of Computer Science

Thesis Committee:

[redacted]

Dr. Jiacheng Shang

Thesis Sponsor

[redacted]

Dr. Bharath K. Samanthula

Committee Member

[redacted]

Dr. Li Dawei

Committee Member

THE PRIVACY LEAKAGE OF IP CAMERA SYSTEMS

A THESIS

Submitted in partial fulfillment of the requirements

For the degree of Master of Science

by

Lee R. Castro

Montclair State University

Montclair, NJ

2022

Table of Contents

Abstract 1
Introduction 6
Aim and objectives 7
Research Problem 8
Motivation 11
Dissertation Report Outline 13
Methodology 13
  Hardware Requirement 14
  Software Requirement 14
System Design 15
Results 16
  Mean 18
  Standard Deviation 19
  Variance 20
Conclusion 21
Recommendations 22
References 24

Table 1: Show the mean score of the motion and no-motion 18
Table 2: Shows a table of the Standard variance between motion and no-motion 19
Table 3: Show the variance of the motion and no-motion 20

Figure 1: Shows a graph of the mean attack defense 18
Figure 2: A graph of the standard deviation between motion and no-motion 19
Figure 3: Shows a graph of the variance attack defense 20

Introduction

Intelligent operations like top facial recognition and minimizing losses due to shoplifting, emergencies, and fraud are keys to success in the retail industry. This application integrates the CCTV camera and the deep learning algorithms used to process these images. Automated intrusion detection alerts, real-time fire alerts, smart checkout, and potentially fraudulent point of sale (POS) transactions are its main features (Kocher and Kumar 9731-63). IP camera security is meant to protect the user's data handling and use. Most IP Cameras have generic software that does the least by protecting the cameras from hackers, misuse of data, or disabling. This experiment was justified by how the entropy of the data analyzed can be processed to predict whether there is an intruder in the house or not, going by the size of data packets transmitted.

The problem was determining a method to capture the camera packets and noticing if there was someone present in the home or not. I have used Wireshark, a network protocol analyzer, to fetch and analyze the network packets. Wireshark can capture packets when the camera is both online and offline. IP cameras are cameras that transmit and receive data via Internet Protocol. These cameras can send packets and alerts, which can trigger the alarm system automatically. The cameras can also notify a user through applications when any unusual activity is happening.

Areas where IP cameras can be used are commercial properties, industrial spaces, and home security systems. A manufacturer can use this experiment to produce more intelligent IP Cameras with updated sensory features for alerting a user if there is an intrusion in their absence when they are connected to the internet. Modern cameras have evolved to be so discreet that their presence is unnoticeable and can work wirelessly (Ortiz et al.).

IP cameras are used in surveillance by business owners and homeowners to monitor theft, burglary, and employee behavior while at work. This helps the users gather evidence in case something happens; in our case, this experiment will demonstrate how a data generating module can be used to notify the owner or capture videos for investigation purposes. The advancement of the hardware technology complements IP technology by capturing high-resolution footage with fewer network demands using wireless cameras and the manufacturer's software. This technology can be important in maintaining the integrity of premises. Our experiment leverages the ability of IP cameras to communicate directly to the network like any other network device. The cameras come installed with applications that make it easier to connect them to the internet; users have the options of installing decentralized or centralized cameras. The transmitted data in motion packets via inbuilt or installed protocols can output user information via the packet-based network.

Aim and Objectives

This report aims to explore the motion of objects and analyze the sensing systems with respect to the design and the user. The development methodology for probable object detection with tracing systems as well as the techniques used to define, analyze, and measure velocities and trajectories when the location of the moving sceneries of the "Sensing" Systems changes to identify items in the user's surroundings.

The following are the central objectives described in this report:

i. Detailed study of "moving Scenery" of items in the context of "real-time" Kinematical data in the vicinity of the user using "Sensing" Systems.

ii. The project's application potential for the corresponding "Open-Source Software" Python as a design and development tool.

iii. The project's applicability in a real-world setting.

The project's main goal is to improve the security and ease for the individuals with the help of operations like top facial recognition and minimize losses due to shoplifting. The application can also be used for checkout automation, trust, queue detection, reducing the use of the workforce, and increasing efficiency. This application integrates the CCTV camera and the deep learning algorithms used to process these images. Automated intrusion detection alerts, real-time fire alerts, smart checkout, and potentially fraudulent point of sale (POS) transactions are its main features (Kocher and Kumar 9731-63). The prices of certain products can be changed over time through a dynamic pricing algorithm that considers a variety of pricing variables. All these will automate the running of a retail shop. Self-checkout system, detection of misplaced objects, dynamic pricing according to the market rate analysis, etc. are the main highlights of this application that will help increase the efficiency of retail shop's running and decrease the workforce. This will be more convenient for the owners

Research Problem

We are exploring IP camera security vulnerabilities and analytical potential by applying meaning to the data transmitted over to a network analysis tool from an IP camera. It uses a data-generating function that demonstrates the difference between the packet activity in scenarios where there is motion and no motion to enhance the language. The experiment deduced that the data size is more in an in-motion state than in a no-motion state.

This experiment is an example of how motion information can be transmitted and analyzed using time and spatial coordinates. By exploring the nature of the waves of the Wireshark packets, the user can tell if there is an uninvited intruder just by predicting the entropy from the graph. There are various properties of the digital signal transmitted that can help this experiment attain the narrow objective of telling whether there is someone at home or not.

The packet information carries motion vectors, acceleration rates of the moved object velocities of the packets, and packet time. With this information stored in a database and connected to a remote network device like a phone or an alarm system, the user can receive notifications. This is the most remarkable aspect of IP camera systems. When the Wireshark packets are captured, the wave is observed while the zoom camera is on. The locks with higher entropy can be hard to predict, but as the programmer, you can use these properties to determine the program's output.

Entropy is the measure of randomness of the transmitted bits. By using statistical models, a program can measure the properties of the packets. Some of the most used characteristics of entropy, include unpredictability, uniformity in bit distribution, and absence of patterns. The lack of patterns implies both unpredictability and uniformity. Their unpredictability does not mean uniformity and their uniformity does not, in turn, guarantee the measure of solid non-computability of the transmitted sequence.

Real-time movement in front of the Zoom camera is captured as network packets and analyzed as digital signals. This experiment can be applied to machine learning applications intelligently to use the data sets. The default status of the camera in this experiment is on, but the shutter is off when picking no-motion data.

In this experiment, we will not go to the extent of telling if the threat is human or not. The experiment is a module to detect events or a rapid notification data-integrated systems component. Surveillance systems have evolved from the traditional analog signal to the digital signal. This has seen new paradigms of security issues. Packet-switched systems have dynamic topologies compared to the latter. This is both a blessing and a curse. The more the surface covered by IP-based camera systems, the more the exposure to attackers on the internet. The attacks can occur to your internal network via other devices.

Despite the new problems, the need for IP camera systems in the market today is enormous. The world has adopted the internet of things and there is a tremendous demand for connectivity via intelligent technologies. We will explore the use of IP camera as a security device by using motion information.

The motion information will be sent to the user interface as network packets. These are basic units of fragmented information transmitted via a network link. The camera will pick the video as a sequence of packets sent to a Network Interface Card, which displays it in a waveform (Ma et al. 1701-54). The waveform can be computed based on the specimen 20 boxes in the motion state and the no-motion state. These packets can be encoded with special ordinates, timestamps, location, device type, etc.

Network protocols determine the ports and maintain a well-functioning transmission. The packets are captured in the graphical user interface (GUI) of the Wireshark program (Wireshark). Data waveforms are then analyzed using three mathematical operations: mean, variance, and standard deviation. This data is plotted as graphs and the data observed shows that low entropy is collected in a motion state compared to a no-motion state.

The data is compiled as packets with context descriptions. This experiment emphasizes the quantity or size of data rather than the quality of the data. The data can only be interpreted to detect movements but cannot reveal what type is captured. The program does the capturing in waveforms by synthesizing the traffic characteristics. This data can help us study the environment where the IP cameras have been placed to observe and identify motion when the owner is not in the background, for example, at home or in business premises.

The dataset was well-computed using the PyCharm program and entropy values of the network packet traffic, which can be visually observed in the Wireshark panel as behavior shape graphs or entropy graphs with timestamps for measuring the data size.

Wireshark is a protocol analyzer or a traffic generator tool to help programmers collect predefined parameters with identifiers appendages on transmitted packets to reveal how a network performs. Background-related works that resemble this thesis were carried on smart-home sensor cameras using stochastic and heuristic graphs. This can enable real-time surveillance by classifying the network traffic as either a motion or a no-motion state. This is a valuable feature for an event-detection camera.

We used machine-learning functions, and the network packets to detect abnormal traffic visually. Network traffic characterization is the central thesis problem of this experiment. Using mathematical models of mean calculation, we can plot graphs of heterogeneous cameras and decide whether the traffic has any anomaly. The device classification framework helps us train the protocol analyzer to automatically predict using the entropy graphs generated by the python program.

Motivation

Anomaly-based intrusion detection by factoring traffic descriptors. Anomaly detection works by defining the empirical measure for the deviation from a no-motion state. In analyzing the graphs, we use the traffic descriptors to describe different features of the data collected. By using plotted behavior shape graphs and measuring the divergence to detect abnormalities, we can advance and use association vectors to differentiate anomalous flows from suspicious flows No-motion behavior doesn't show network data on the traffic protocol panel; the motion state is a recurrent time bin and is measured and compared by the normal state of the camera with the shutter off.

This experiment aims to demonstrate the working of machine-learning Intrusion Detection Systems and represent anomalies as signatures. In this phase, we assume misuse detection, which attaches types to network packets. This classifier has low entropy; hence, there is enough room to predict if a change occurs or when an anomaly is in the current time bin (Ahmim et al. 208-25).

In contrast to anomaly detection, the outlook is to define a standard network profile and the abnormal states by using the measure of deviation, mean, or variance from the normal status. After determining the degree as a vector variable, it can generate a statistical model, for example, the graphs as per the 20 network packets in motion and no-motion states. Machine learning systems can also process the variable. Modern Internet Protocol cameras are embedded within Intrusion Detection Systems. These IDSs come installed with sophisticated add-ons, that can be processed further by deep learning, feature engineering, and network traffic grouping.

Since our experiment's input is network traffic, network-based IDSs are ideal for this experiment. This experiment can develop a feature engineered to notify the user when the degree of deviation is attributed to the detection method.

There are two machine-learning algorithms commonly applied to the IDS, supervised and unsupervised systems. Supervised systems use signatures to classify data; this makes data classification time-consuming but more thorough than unsupervised learning systems that use calculated feature information to train the IDS. Let me highlight one learning model, the K-Nearest Neighbour (KNN). KNN parametrizes a class of behavior and calculates the hypothetic probability of the sample data. For example, the bin belongs to a particular class in the current time. Thus, the classification is based on the top-k proximity to neighbors (Sivasamy et al.).

About the system architecture, the first module parsed with subsequent time-bins. Each file contains a list of keys observable and associable with the number of flows transmitted by the IP address of the network camera. The data is processed and then passed to the module responsible for statistical modelling. Using 2D graphs, we can compare the current sketches and the sketches from the references. The degree of variance between the mean and the actual average profile can determine whether there is an anomaly or not.

The architecture of the technology factors in the topology and the components. The elements relate in ubiquitous ways that expose the IP cameras to vulnerable attacks. A good example is how the cameras use public channels of communication, giving attackers access points.

The quantity of data received is a calculated mean of the changes in the network packets received. By analyzing the wave using the models we have highlighted above, one can observe the movement captured by the IP camera or sensor. The acceleration of movements is received as motion vectors. IP cameras, magnetic devices, and motion sensors can use this experiment as a reference. The data packets are simply data sets embedded in sequences and can be changed to predict a programmed parameter. With further attributes added to the graphs like spatial coordinates, the meaning of the data can be broader, and that includes improving a user's interaction by making the data more readable.

Dissertation Report Outline

The dissertation of the given project has been completed by outlining the introduction, pointing out the significance and motivations behind the project and the subject, outlining the backdrop of the problems, and aims and objectives explored in the project in a real-world setting. Also, the report depicts the corresponding literature review carried out in the context of the research problem, the background and relevant literature associated with the given subject to its best interest and elucidates different perspectives and lines of thought associated with the topic. Following that, the project's approach has elaborated on the implemented measures, the accompanying analyses and procedures, and the pertinent findings and outcomes. Finally, there is the conclusion section that reveals the scope and limit of the project.

Methodology

The experiment used a small dataset instead of a complex one because in the past, complex systems have shown an increase in false alarm rates than in smaller datasets. Frequency analysis technique have been used as intrusion detection algorithms.

Hardware Requirement

Processor	Intel i7 8th Gen
RAM	8 GB DDR4
Hard Disk	512 GB SSD
Display Size	15''LED Monitor
Screen Resolution	1920*1080 Pixels
Keyboard	Wireless Enabled Keyboard (Recommended: Logitech)
Keyboard Mouse	Wireless Enabled Mouse (Recommended: Logitech)
MONITOR:	LED Monitor
Camera:	8 Megapixel Full HD 1.8f lens
Dedicated Graphics Card:	Nvidia Geforce GTX 1050 4GB DDR5

iPhone 12 5G speed A14 Bionic chip featuring Super-Retina XDR display with a 6.1-inch edge-to-edge OLED display

Software Requirement

Operating System: Windows (10)

Programming Language: Python

IDE: Open CV

Front-End: Python Django

Back-End: MongoDB

System Design

System design reduces an entire system to its basics by studying the various operations performed and their relationships within the system and the requirements of the various operations success. One aspect of the design is defining the system's boundaries and determining whether the candidate system should consider other related systems. A system can be defined as an orderly grouping of interdependent components that can be simple or complex.

The idea of the system design has been most practical and necessary in computerizing the interrelationships and integration of operations, especially when using computers. Thus, it is a way of thinking about organizations and their problems. An organization consists of several interrelated and interlocking components.

The most creative and challenging phase of the system life cycle is the system design. The term design refers a final system and the process by which it is developed. It refers to the technical specifications applied in implementing the candidate system. It also includes the construction of programs and program testing.

The first step in the system design is to determine how the output is produced and in what format. Samples of the output and the inputs are also presented. In the second step, input data and master files are to be designed to meet the requirement of the proposed output. The processing phase includes the system's objectives and complete documentation.

Finally, detailed system justification and an estimate of the impact of the candidate system on the user and organization are documented and evaluated by management as a step implementation. The final report prior to the implementation phase includes a procedure flow chart, record layouts, and a workable plan for implementing the KDMS system.

System design has two phases:

Logical

Physical

The logical design reviews the present physical system, prepares the input and the output, and prepares a logical design walk-through. We must decide how to log the required entries and how we should process the user data. Also, we must present the data in an informative and appealing format. This design also involves the methodology to store, modify, and retrieve data from the database as per the requirement. The physical design maps out the details of the physical system, plans the system implementation, and devises a test and implementation plan as well as new hardware and software.

We must decide how and where to store the input data and how to process it so as to present it to the user in an easy, informative, and attractive manner. A major step in the designing is the preparation of input and output reports in a form that's acceptable to the user. In this step, a data entry operator can feed the relevant details asked by the system for a particular task as input.

Results

The main motivation and objective of this system is to provide a solution to reduce the inconvenience of finding a unique diet for the user and enabling a user-friendly interface. Systematic handling of the schedules in such a way is key to increasing its manageability and competence.

This experiment does not focus on contexts specific to the nature of the object being captured by the IP camera. However, it identifies the traceability of the object or data packets transmitted as a feature of machine learning. The data packets come with references to guide the receiving protocol on interpreting the data. Wrapping these data packets in a protocol, for example, the Session Initiation Protocol which controls and terminates a session involving two-time bins, can be helpful for the network packets traffic descriptors that suit the statistical model to be generated by the traffic tool. It is a simple experiment and does not utilize all complex detection methods; mainly, misuse-detection is demonstrated here (Bozionek et al.).

Mean

motion	No-motion
1168.811	1191.163
1163.606	1201.954
1164.207	1200.948
1170.943	1197.673
1165.424	1200.34
1162.584	1201.113
1166.618	1196.808
1167.512	1197.926
1162.195	1202.666
1169.058	1202.168
1162.195	1202.185
1166.189	1202.218
1162.661	1202.881
1163.89	1204.335
1163.635	1203.147
1160.165	1201.828
1164.617	1206.947
1170.298	1218.5
1163.735	1202.736
1163.316	1205.366

Table 1: Show the mean score of the motion and no-motion

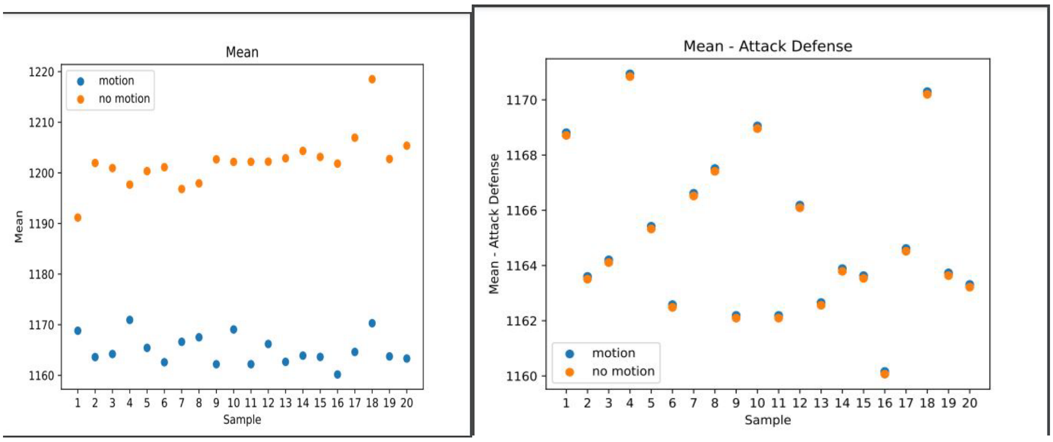

Figure 1: (a) shows the graph of the mean between motion and no-motion.) (b) Shows a graph of the mean attack defense

Standard Deviation

motion	No- motion
139.9037	83.99331
143.3254	64.80622
142.2689	64.36674
133.8969	64.47009
141.9154	66.11246
142.4413	63.52951
139.7985	65.29485
143.9124	62.33829
144.4087	63.21792
137.8882	63.73919
144.4087	61.32955
142.5834	64.44398
142.1255	61.26935
142.0681	61.8148
141.0062	62.24672
142.0588	61.49628
143.1291	58.30157
55.49954	40.41349
141.5414	60.24284
141.2445	61.26941

Table 2: Shows a table the Standard variance between motion and no-motion

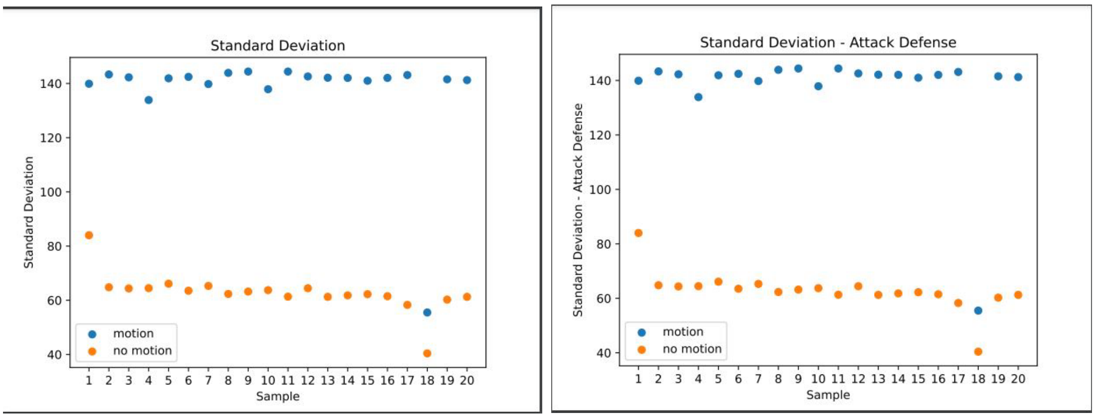

Figure 2: (a) shows a graph of the standard deviation between motion and no-motion (b))shows the standard deviation of the attack defense

Variance

motion	No-motion
19573.05	7054.876
20542.18	4199.846
20240.44	4143.077
17928.37	4156.393
20139.98	4370.857
20289.53	4035.998
19543.61	4263.418
20710.78	3886.062
20853.88	3996.506
19013.17	4062.685
20853.88	3761.314
20330.02	4153.026
20199.64	3753.933
20183.34	3821.07
19882.75	3874.654
20180.71	3781.793
20485.94	3399.073
3080.199	1633.25
20033.97	3629.2
19950.02	3753.941

Table 3: Show the variance of the motion and no-motion

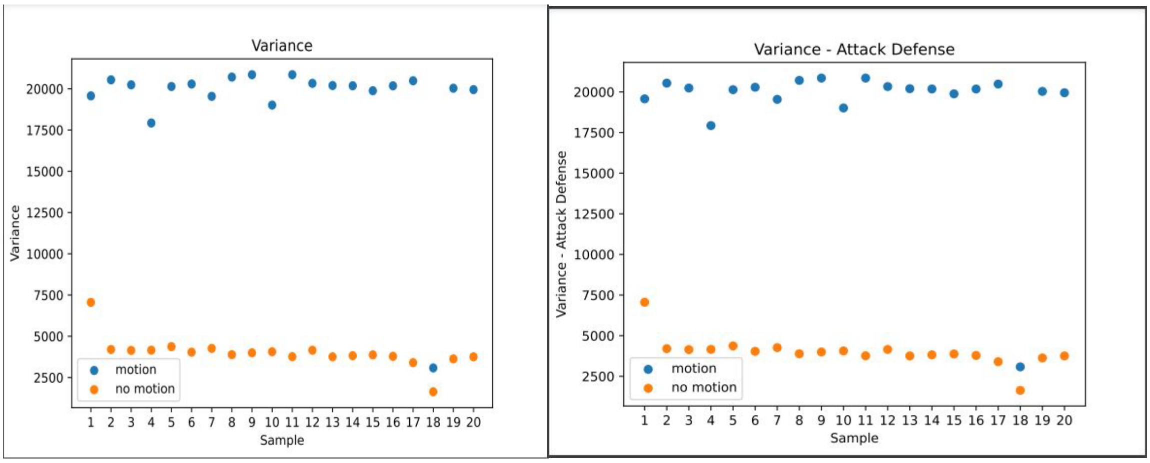

Figure 3: (a) shows the variance between the motion and no-motion (b) Shows a graph of the variance attack defense

Network packets remain incomplete unless parsed with additional header and application data. The header contains structured IP addresses, ports, and protocols fields. Some of the reasons I chose to use packets is because of their effectiveness in detecting U2L and R2L network hacking (Ortiz et al.). Packets have the ability to encode IPs and timestamps, thereby storing the data sources. The packets can be matched with packet patterns in real-time without caching.

This experiment tests algorithms based on statistical models. In IDS systems, false-positive rates in machine learning approaches are due to the poor relationships between features that are not well revised. Statistical equations calculate the deviation in the current time bin from default profiles. Datasets can train the IDS algorithm to tolerate deviations within an acceptable range. Statistical models can explicitly achieve noise handling.

Hotelling's multivariate statistical technique, is the concept this experiment is trying to mimic as a correlation of variables, using a variance matrix of the control model adopted. A null hypothesis is a conditioner to the descriptors; when the traffic in the current time bin shows minor deviation, the process controller doesn't output any anomaly. In an alternative hypothesis, the current traffic is an anomaly, but the deviation is acceptable, as the degree of deviation is an indicator. Hoteling has been used to track an object's scalar and spatial coordinates. The test can differentiate moving and stationary objects; however, it has challenges in processes with complex correlations, such as mean shift anomalies and counter regressions.

Conclusion

The identification method detects any object in the image with outlined rectangular boxes, then calculates each packet object and places its tag with these methods and algorithms through the deep learning machines (Kocher and Kumar 9731-63). The object was identified through the process of training datasets. Thousands of images were taken for each object to improve the accuracy. Then, the object in the image was outlined and labeled to be identified during real-time detection. Upon the completion of training of datasets, each object was identified with proper labeling. Hence, more research was conducted on object detection and more improvement were made to create a better algorithm. With this retailer can quickly gain insight into transactions, interests, and hotspots. When it comes to efficiency, kiosks offer the following:

- Reduced wait times compared to using cash registers. Customers can walk into the store, order, and pay without waiting in line.
- Reduced labor costs as one member of staff can overlook several self-checkout kiosks.

As the products are usually still handed out by employees or picked up by accessing digital lockers, the risk of theft is minimized with this solution. This system is ahead of others but less advanced than other options when it comes to transaction speed. Perceived control, reliability, ease of use, and enjoyment are as optimal as they can be for customers using this system. Next to online pre-ordering and checkout, kiosks are one of the most convenient self-checkout options for retailers selling meals and should also be considered for other types of products and stores.

Recommendations

This technology can be applied in various network device scenarios, for example, smart appliances, smart thermostats, motion lights, IP cameras, and much more innovative technology. When the camera is off, the behavior shape graph shows a smaller data quantity than when the camera is on. It can be concluded that the entropy decreases when the camera is on. This is because the camera receives a particular packet type. The functionalities and generated data are different for many devices. Some of the purposes of the camera surveillance system depend on user specifications such as for enforcement at the location where intrusion detection occurs, monitoring the home or work premise remotely, forensics on providing evidence in court proceedings, etc.

A drawback of this thesis problem/application is its inability to mask the statistical models to protect the system's integrity from attackers. Hackers can infiltrate the traffic pattern by scanning the waveforms with more extensive data and muting the descriptors.

This can keep the shutter off even when there is motion in front of the camera. Some of the prominent attacks include Denial of Service, which makes legitimate users unable to access the system. Volumetric attacks on the traffic generate network clogging, which crashes the systems denying service to the legitimate user. This provides scope for further research and experimental approaches to tackle the vulnerability.

If there is access from a foreign port or protocol. Machine-learning responses can be fed into the dataset to process the output to camouflage the back-end input, or layer the output to indicate data quantized that is opposite to the observed traffic if access is from a foreign port or protocol. The experiment has demonstrated the ability of Python algorithms to analyze camera motion packets intelligently to predict an anomaly in the observed timestamp against the established standard traffic profile.

References

Ahmim, Ahmed., et al. “A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-based Models.” *In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS),* 29–31 May 2019, pp. 208-25.

Bozionek, Bruno et al. *METHOD FOR CAPTURING AND TRANSMITTING MOTION DATA.* 5 Nov. 2015.

Kocher, Geeta., and Gulshan Kumar. “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: Recent Developments and Challenges.” *Soft Computing*, vol. 25, no. 15, 2021, pp. 9731-63.

Ma, Tao., et al. “A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks.” *Sensors*, vol. 16, 2016, pp. 1701-54.

Ortiz, Julio, et al. “About IP Cameras.” *Network Optix*, 1 Oct. 2020, https://www.networkoptix.com/2019/08/06/about-ip-cameras. Accessed 9 Oct. 2021.

Sivasamy, Avalappampatty, and Bose Sundan. “A Dynamic Intrusion Detection System Based on Multivariate Hotelling's T2 Statistics Approach for Network Environments.” *The Scientific World Journal*, 2015. doi.org/10.1155/2015/850153.

Wireshark (2020) *Wireshark · Go Deep.* 24 Jan. 2021, https://www.wireshark.org. Accessed 25 Nov. 2021.