

# A STUDY ON AI BASED SURVILLANCE CAMERA

<sup>1</sup>Chowdhary Kshitij Singh, <sup>2</sup>Dr. Neetu Sharma

<sup>1</sup>M.Tech Scholar, Department of C.F.I.S, G.I.T.A.M, Kablana, Jhajjar, MDU, Rohtak, Haryana

<sup>2</sup>HOD, Department of C.F.I.S & C.S.E, G.I.T.A.M, Kablana, Jhajjar, MDU, Rohtak, Haryana

**Abstract :** Since the time immemorial, security has been an important concern for humans. There has been a progressive development in this sector with growing technological inventions facilitating human efforts in surveillance to go down from solely to partly giving a sigh of relief. However studies show that humans continuing to watch a single video screen for about more than quarter an hour may lose approximately ninety percent of their ability to maintain their attention levels in order to spot significant events happening in the video. In this scenario, Artificial Intelligence could turn out to be a rescuer as it provides a solution to the limitations faced by humans in providing quality surveillance by continuously monitoring the live video footage. This remarkable leap in video surveillance for security using AI is a boon for humans round the globe. AI for video surveillance uses software programs to analyze the images captured by surveillance cameras so as to recognize objects, vehicles, activities or humans. The software can be programmed for various purposes like defining the restricted areas within the camera's purview, imposing restrictions for the time of the day for which the property is being protected.

**Index Terms - Artificial Intelligence, Camera, Image processing, IOT.**

## I. INTRODUCTION

AI for video surveillance uses software programs to analyze the images captured by surveillance cameras so as to recognize objects, vehicles, activities or humans. The software can be programmed for various purposes like defining the restricted areas within the camera's purview (such as a fenced space, restricting entry only to a parking lot and not to the sidewalk or street outside the parking lot) and imposing restrictions for the time of the day (such as off business hours) for which the property is being protected. Whenever someone or something breaks any of the rules (such as restricted entry in a particular area for a particular time period of the day) defined by the algorithm, an alarm is triggered setting an alert.

The Internet of things (IOT) is used to send the alert on mobile or mail in case a trespasser is detected breaking any of the rules of the algorithm (like nobody is allowed to enter a particular area during a specific period of the day). The A.I. programs used to execute such tasks make use of machine vision. Machine Vision is a technology and a methodology that provides analysis for image based automation. It consists of a chain of algorithms (or mathematical steps) which are executed in a sequence as if a patterned questionnaire is used to compare the image of the object visible on the camera with the repository of thousands of reference images of humans in varied angles and postures and movements as well.

A.I. works by questioning itself whether the observed entity showcases movement similar to the ones stored in reference images repository, if the size is same i.e. height relative to the width, whether it has two arms on either side of the body and two legs, if the speed of the movement is similar and if the alignment is vertical rather than being horizontal. The very feature A.I. to simultaneously maintain surveillance of numerous cameras makes it multitasking. A.I. also proves its superiority over human abilities by giving the best results even in challenging situations such as rains or extra light in case of glare. It also has an upper hand in anticipating situations like an object or a person from a distance away.

A.I. types for security can be classified into following two categories:

### 1.1 Rule-based AI

Rule based A.I. demands the programmer to define rules for each and every thing for which the device is expected to send alert as per the requirement of the user. This type of A.I. is mostly used for security purposes, for instance in surveillance cameras. Here, the hard-drive containing the program can either be situated inside the camera itself or else it can be located altogether in a different device where the camera's output serves as an input to this device.

### 1.2 Non-rule based

Non-rule based A.I. is a completely self-learning model which doesn't require any prior input programming by the programmer. This type of A.I. learns by observing the behavioral patterns of people, orientation and behavior of objects, machines, changes in nearby surroundings or environment, etc. based on various characteristics like size and shape, speed of movement, color, alignments, orientation (both vertically and horizontally) and many more. The visual data obtained by A.I. systems is standardized by classifying or tagging the objects and the patterns of those objects being observed. Thus, continuously amending the definition and meaning of what is considered as normal behavior or average behavior for the objects being observed. This way of learning facilitates systems

to keenly observe the patterns and makes them capable enough to catch hold of any anomalies or events where objects break the estimated patterns. In such situations, an alert is sent to the respective device.

Artificial Intelligence combined with IOT turns out to be a more efficient surveillance system as it helps the user to view the live footage of his property remotely. Also user can set his own rules against which he would be alerted if any of it is violated. User could also receive images of the activity being performed and the person performing the activity.

## II. PROBLEM FORMULATION

Continuously monitoring of the live footage on screen by humans for about twenty to thirty minutes lowers their attention levels such that the detection of objects or any changes in the environment seems less likely, this is termed as vigilance decrement. When a single individual is burdened with the responsibility to keep a check over two or more monitors simultaneously, the concentration is further divided reducing the productivity. And it clearly surpasses human ability when tens of cameras are to be observed at a time. Generally it becomes boring to watch the footages of empty hallways and buildings, storage areas, shops during off working hours, parking lots, thus hampering the attention levels of the scrutinizer. Such limitations of human abilities to deal with critical tasks demanding a great amount of sustained vigilance and long attention spans to keenly observe live events happening on the monitor has made a room for artificial intelligence in this arena which could help eliminating these loopholes and serving the purpose in a better way.

With hundreds of camera footages flashing up on a wall monitor, several computer screens used to scrutinize multiple video footages of cameras (placed in different areas) by splitting the screen and swapping every few minutes between different sets of cameras (installations done in various parts of the same property), accounts to enormous tedium to scrutinizers. The burgeoning demand of these video cameras for surveillance has a vast spectrum of customers ranging from shopping complexes, malls, showrooms, parking lots, residential societies in order to ensure security of residents, schools and offices to facilities that need higher levels of security like nuclear plants, data centers, places dealing with confidential data storage. The challenges and past experiences in area of video surveillance have shown that the systems involving operators (humans) to scrutiny the live coverage are not that much efficient and need technological intervention to upgrade them.

Initially when the concept of video surveillance systems was introduced, it was thought of as an evidence generating system which could of some help in forensics to identify suspects and culprits after occurrence of the incidents. There were several loopholes identified such as the ones with wide angle views of cameras installed in vast outdoor areas could not produce video with sufficient resolution. Thus, it becomes difficult to draw out conclusions from such videos. In these scenarios it becomes challenging to clearly identify the interloper as the image resolution is either very bad or the image is too small to be identified on monitor.

A user travelling to out of station were not able to know about the mis-happening/incident at the real time. Whenever he will come back then only he may able to know. So he should be informed during the incident happening so that he can do the needful for prevention.

Video surveillance surely acts as a solid proof to take the necessary action for any ambiguous event or crime. These days, forensic investigators and the police department, both are highly dependent on digital CCTV camera recordings to solve cases. First, they locate the evidence in a video tape and then, convict the criminals.

However, with the increasing number of cameras and home security systems, the amount of video created is also multiplying. Just consider a simple example. Reviewing a single tape of 2 hour duration to catch an employee who stole from the inventory is comparatively easier than reviewing same 2 hour duration tape from 15 cameras. We sure should increase the surveillance cameras to increase the safety, but then it also increases the amount of redundant tape being generated. This makes the process of finding the required data extremely time-consuming and impractical.

## III. PROBLEM SOLUTION

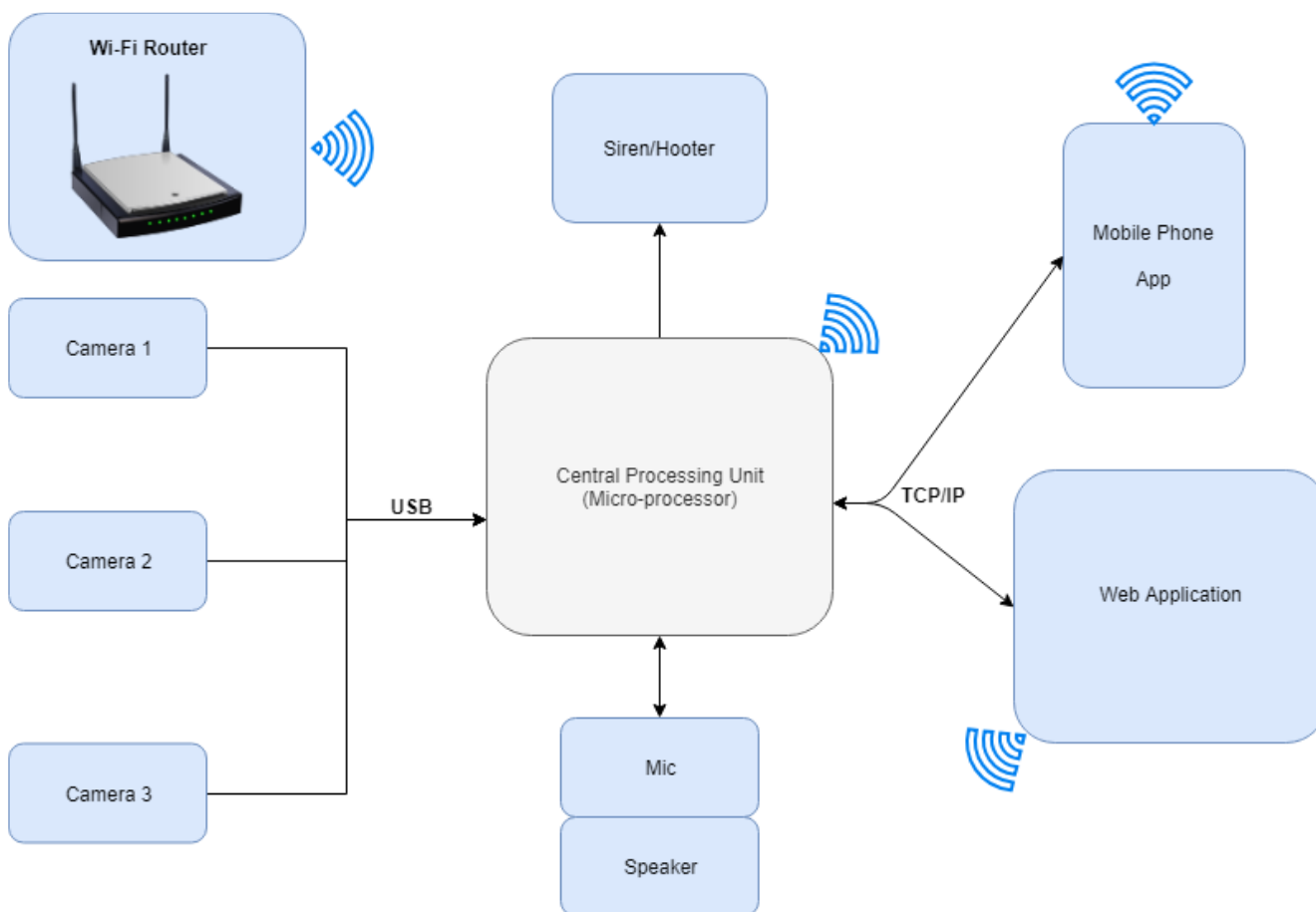
One of the best approach is to sort the data as per what the security keeper want to see like face, license plate number or the characteristics of the vehicles, machines such as color, type or the direction in which the body is moving. On the basis of these characteristics, the security footage can be sorted and indexed. The below model is the one of the best solution for this problem.

In this model all the surveillance systems are integrated at one centralized location so that security professionals can set rules, users, alerts, permissions and troubleshoot all the systems without physically touching them. In this way, the robust 'intelligent search' functions speed up not only the search of evidence, but all the operations of an enterprise.

There should be a complete security system running with artificial intelligence based analytics. There is no need of security guard to view the continuous footage of the camera. The camera will automatically trigger a siren (alert) and send the alert notification on the mobile app as well as email and web app if any suspicious activity get detected.

The Security system must have mentioned analytics:

- a) Color Detection.
- b) Motion Detection.
- c) Intrusion detection.
- d) Line tripping detection.
- e) Camera tempering detection.
- f) Face Detection & Recognition.
- g) Vehicle Number Plate Detection & Recognition.



**Figure 1:** AI Based Security Camera model.

The alert for the above analytics can be shared with the user on his mobile /web app with random click of the activity happen. The siren can also be triggered for the same.

Above mentioned approach uses the similar concept as that of Internet search engine's similar data. This procedure facilitates the surveillance personnel to quickly review the 'similar data' instead of manually searching through several hours of raw data. When you search for the particular query, then the images and videos related to that particular query are displayed. This procedure transforms raw data into rich informative content and reduce the amount of time needed to review the surveillance tape to the very large extent.

#### IV. RESULTS AND CONCLUSION

In it's short existence, AI has increased understanding of the nature of intelligence and provided an impressive array of application in a wide range of areas. It has sharpened understanding of human reasoning, and of the nature of intelligence in general. At the same time, it has revealed the complexity of modeling human reasoning providing new areas and rich challenges for the future. Using AI in the Surveillance system is the best option to reduce the human effort in watching continuous to live video. The A.I. learns itself by observing the day to day behavior of the peoples, vehicles, machines and it also learn from various characteristics like speed , size , color, groups and orientation.

So using Artificial intelligence with IOT for camera will be a better option for security and surveillance system. In short the artificial intelligence is the future of surveillance system.

#### V. ACKNOWLEDGMENT

This research conducted to meet the current challenges that are being faced to improve the security in Surveillance system. We have used IOT and Artificial intelligence for security automation. I would like to thank Dr. Neetu Sharma who supported me during this journey.

#### REFERENCES

- [1] The Appropriate and Effective Use of Security Technologies By Green, Mary W.
- [2] Visual sustained attention By Nuechterlein, K.H., Parasuraman, R., & Jiang, Q.
- [3] How effective is human video surveillance performance By Sulman, N.; Sanocki, T.; Kasturi, R.
- [4] The Evolution of Video Analytics, Security Sales & Integration magazine By Gruber, Illy.
- [5] Internet of Medical Things: Gatouillat, Arthur; Badr, Youakim; Massot, Bertrand; Sejdic, Ervin.

