International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

xx

COPY RIGHT

IJIEMR Transactions, online available on 31th May 2024. Link
https://www.ijiemr.org/downloads/Volume-13/ISSUE-5

10.48047/IJIEMR/V13/ISSUE 05/59

TITLE: Image Detection And Processing For Wireless Surveillance Camera Using Cloud Heritage Technique And Network Security

Volume 13, ISSUE 05, Pages: 546-551

Paper Authors **Somyadeep, Dr. Rishi Kumar Sharma , Deepak Saini**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Image Detection And Processing For Wireless Surveillance Camera Using Cloud Heritage Technique And Network Security

1st Somyadeep.
Research Scholar (B.Tech CSE)
Quantum University
Roorkee(UK), India
email somyadeep7217@gmail.com

2nd Dr. Rishi Kumar Sharma
Associate Professor (CSE)
Quantum University
Roorkee(UK), India
rishi.rishi1526@gmail.com

2rd Deepak Saini
Research Scholar (M.Tech CSE)
Quantum University
Roorkee(UK), India
sainideepak1323@gmail.com

Abstract—This work presents a comprehensive approach to enhancing the capabilities of wireless surveillance cameras by leveraging cloud heritage techniques and robust network security protocols. The primary objective is to find and improve real-time image detection and analysis for security purposes. The proposed system integrates a cloud heritage technique, allowing for the efficient storage, retrieval, and processing of image data in a cloud-based environment. This ensures scalability and accessibility, enabling seamless integration with existing surveillance infrastructure. The efficacy of this integrated approach is evaluated through extensive experiments, encompassing various scenarios and environments. The results demonstrate significant improvements in image detection accuracy, response time, and overall system reliability. This research contributes to the advancement of cloud-based surveillance technology by providing a scalable, secure, and efficient solution for image detection. The integration of cloud heritage techniques and network security measures showcases a promising avenue for future developments in the field of surveillance systems. This modern era requires modern and robust technologies so is the heritage cloud technique which has a very efficient role in network security.

Index Terms—Image detection, surveillance system, risk man-agement, cloud heritage technique

I. Introduction

Image detection for wireless surveillance cameras using cloud heritage techniques and network security is a cutting-edge approach revolutionizing the field of video monitoring and security. This innovative system leverages the power of cloud computing to process and analyse real-time imagery cap-tured by wireless cameras. By offloading computational tasks to remote servers, enables the cameras to function efficiently even with limited onboard processing capabilities. Network security plays a pivotal role in safeguarding the integrity and confidentiality of data transmitted between the wireless cameras and the cloud servers. Robust encryption protocols and secure communication channels are implemented to thwart unauthorized access and data breaches. Additionally, stringent authentication mechanisms and intrusion detection systems fortify the system against cyber threats, ensuring uninterrupted operation even in the face of sophisticated attacks. Deep Learning Algorithms, Feature Extraction, Object Detection and Localization, Anomaly Detection, Cloud Computing and Parallel Processing are some of the techniques used in Image detection for wireless surveillance cameras. The cloud heritage technique employs a distributed network of servers with high computational powers, allowing for rapid image recognition, object tracking, and anomaly detection. This translates to swift response times and enhanced situational awareness, crucial for timely intervention in security incidents. Moreover, the cloud heritage technique facilitates seamless integration, creating a cohesive ecosystem for comprehensive surveillance. Intelligent crime systems, terrorist attacks and increasing security-related problems have alarmed each and every nation and organization of the globe. The manual analysis process consists of a number of limitations it is costly, prone to errors, labour intensive, limited human resources, and sometimes failure of human resources to monitor continuous signals. Due to time con-straints, lack of resources, and technological advancement of criminal attacks, it is very difficult to provide 24x7 monitoring, resulting in knocking the opportunity of smart and intelligent-based wireless camera systems.

II. IMAGE DETECTION FOR WIRELESS SURVEILLANCE CAMERA.

For image detection, it requires an image loaded first. Then the following techniques and steps are used subsequently. 1. Clicking image:- The wireless surveillance camera clicks a still image or a series of frames from its field of view. 2. Pre-processing: - The captured image may undergo preprocessing to enhance its quality or reduce noise. During preprocessing resizing, noise reduction, and colour normalization is done.

3. Feature Extraction: - Distinctive features are extracted from the image according to our requirements. It can include edges, corners, textures, or other visual cues that help in distinguishing objects. 4. Feature Representation: - Extracted features are often represented in a format suitable for processing, such as vectors or matrices. 5. Object Detection:- Using algorithms like edge detection or color-based segmentation, the system identifies regions of interest within the image that may contain objects. 6. Object Recognition or Classification: - Once objects are detected, they are classified into predefined categories. This step can involve comparing extracted features to a database of known objects. 7. Post-Processing:- Additional processing may be applied to refine the results, remove false positives, or perform tasks like object tracking. 8. Alert or Action Triggering:- If a specific object or event of interest is detected (e.g., a person, a vehicle, or a specific behaviour), the system may trigger an alert or take a predefined action. 9. Feedback or Reporting: - The results of the image detection process may be stored, displayed, or communicated to a central monitoring system or user interface.

III. IMAGE PROCESSING FOR WIRELESS SURVEILLANCE CAMERA.

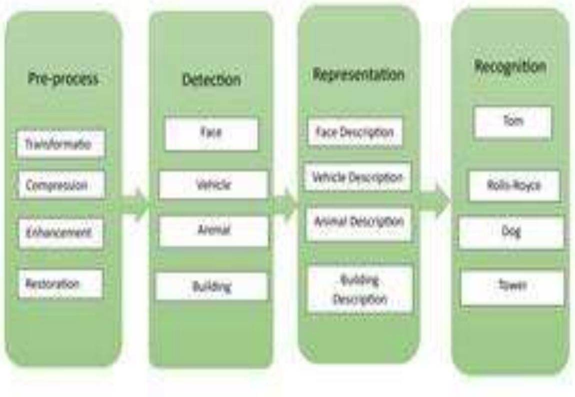

Figure briefly illustrates the workflow it, which consists of four phases, i.e., pre-process, object detection, representation, and recognition. To improve its quality and make the subsequent procedure easier, the raw image data will be processed, compressed, enhanced, restored, and so on in the g 1 phase. The detection step will involve the use of matching models, such as face, vehicle, animal, and building models, to detect and extract specific objects involved. These items will be described as a set of features during the representation phase. Ultimately, these things will be categorized as particular people, vehicles, animals, or structures during the recognition phase. Generally, when implementing the intelligent surveillance system, all four of the aforementioned phases are taken into consideration.
To be more precise, they are all installed on cloud-side servers or edge side devices.

Figure briefly illustrates the workflow it, which consists of four phases, i.e., pre-process, object detection, representation, and recognition. To improve its quality and make the subsequent procedure easier, the raw image data will be processed, compressed, enhanced, restored, and so on in the g 1 phase. The detection step will involve the use of matching models, such as face, vehicle, animal, and building models, to detect and extract specific objects involved. These items will be described as a set of features during the representation phase. Ultimately, these things will be categorized as particular people, vehicles, animals, or structures during the recognition phase. Generally, when implementing the intelligent surveillance system, all four of the aforementioned phases are taken into consideration.
To be more precise, they are all installed on cloud-side servers or edge side devices.

IV. CLOUD HERITAGE TECHNIQUE AND NETWORK SECURITY

To secure the images and data, the tool is designed into two stages. First, a new monitoring scheme is built to keep the privacy of data. Second, the checking process that plays a big role for saving users' privacy and highly secure places that use surveillance cameras is facilitated. This developed tool runs under certain circumstances and is intended to function when it is attached to the complete system, which we call a model. This model consists of a default Gateway (G), an IP Surveillance Camera, both having static IP addresses, and a trusted PC. G works as a monitoring unit that watches all network traffic using Wireshark. It is connected to the backup server (BS). Every period of time (t), the BS checks G and sends the capture files to the BS. G and BS are run on the same network. Thus, The BS delivers the capture files to the BS and checks G once every time interval (t). The networks used by G and BS are the same. Therefore, in order to address security concerns, we copy all capture files to BS, which has a log file that contains a record of every transferred data (date, size, etc.).

, if BS does not receive any copy this indicates for attack. The gateway of the surveillance camera is set to G. The network communicates with the IP camera and G. The IP camera traffic passes only through G and it can read, capture, and analyse. The destination of this traffic is the trusted PC. The specifications of the IP camera. The trusted PCs are the only devices allowed to have legal access to the camera. Trusted PCs also are allowed to connect to each other (authorized access). And if it has any glitch or any kind of vulnerability at any part then it will alert the system that there is any attack on the cameras. 1 The video equipment. In this manner, the network is kept safe and secure on the cloud.

Fig. 1. Image processing

V. PROBLEMS RELATED TO WIRELESS SURVEILLANCE CAMERAS

Image processing is a form of processing with input as an image such as a photograph or video frame and output can be characteristics or parameters related to the image that we use according to our requirements. 1. One of the most crucial features of today's intelligent security robots is image processing for object recognition. It makes these things visible and makes them applicable.

.

5.1 Basic problems Camera Footage can be Noisy- Noisy CCTV footage is generally occurs due to electrical or RF interference. Video can be choppy- If a real-time video from your CCTV camera appears choppy or suffers from visible tearing, it usually indicates a network problem.

Video footage from IP cameras will appear choppy if the network doesn't have the bandwidth required to carry it. Analogue video signals usually don't get choppy on their own. If there's a connectivity problem, it will manifest through flickering, noise or blackouts. However, the video output of NVR or network-connected DVR boxes can become choppy due to a slow network, regardless of its source.

Camera System Resolution or the Video Stream- A 720p or 960H camera may not capture clear images or videos. If we are using a 4-megapixel (1440p super HD) security camera, make sure the resolution or the video stream is set to 2560x1440 or at least 1920x1080 so that we can take clear images for observation.

Latest Firmware- It should be regularly checked for new firmware to fix bugs, including troubleshooting the camera picture issues like CCTV cameras not showing images, flick-ering problems and basic day-to-day problems. And this is the most important part of any wireless device. Because most of the attacks on the system are due to the loopholes and bugs in the system. 5.2 Storage Problem

a. High Storage Requirements: High-resolution images and continuous recording can lead to massive storage demands, necessitating robust and scalable storage solutions. So it is necessary that we should efficient software so that these data can be compressed and can be stored efficiently.

b. Cost Constraints: Acquiring and maintaining large-scale storage systems can be costly, especially for organizations with tight budgets. Cost is also a big factor for different clients it should be designed accordingly.

c. Data Retention Policies: Determining how long to retain images can be a challenge. Legal and regulatory requirements, as well as practical considerations, must be balanced.

d. Redundancy and Backups: Ensuring redundancy and reliable backup systems is crucial to prevent data loss due to hardware failures or other unforeseen circumstances. Backup is always an important part of wireless camera systems.

e. Data Access and Retrieval Speed: Quickly retrieving specific images for analysis or evidence can be a critical requirement, and storage systems need to support rapid access.

5.3 Security Problem

a. Unauthorized Access: Protecting against unauthorized access to the network or the surveillance feed is paramount. Weak passwords or improper access controls can lead to breaches.

b. Encryption: Ensuring that data transmitted between cam-eras and storage systems is encrypted safeguards against interception and tampering.

c. Vulnerabilities in Network Infrastructure: Weaknesses in routers, switches, or other networking equipment can be exploited, potentially compromising the security of the surveil-lance system.

d. Denial of Service (DoS) Attacks: DoS attacks can flood a network, making it unavailable for legitimate users. This can disrupt surveillance operations.

e. Physical Security: While not directly related to network security, the physical security of network equipment is crucial. Unauthorized access to network hardware can compromise the entire system.f. Monitoring and Intrusion Detection: Implementing effec-tive monitoring and intrusion detection systems helps iden-tify and respond to suspicious activities or potential security breaches.

The application of the cloud heritage technique offers a promising solution to address the challenges associated with image detection for wireless surveillance cameras, particularly in terms of storage and network security. This innovative approach leverages the power of cloud computing, allowing for efficient data management and enhanced security measures. One of the notable advantages of deploying the cloud heritage technique is the elimination of digital footprints. Unlike traditional storage solutions, where data leaves traces on local devices or servers, the cloud heritage technique operates in a manner that leaves no discernible trace of the data's presence. This significantly enhances privacy and security, making it harder for unauthorized parties to access or tamper with sensitive information. Additionally, the seamless retrieval of data is a hallmark of this technique. With the vast computational cloud resources, image data can be accessed swiftly and efficiently, enabling rapid response times in surveillance scenarios. This quick retrieval ensures that critical information is readily available when needed, enhancing the effectiveness of security measures. Furthermore, the cloud heritage technique incorporates robust encryption and security protocols, providing a fortified barrier against cyber threats. Data transmitted between cameras and the cloud is shielded from unauthorized access, ensuring the integrity and confidentiality of sensitive information.

CONCLUSION

The integration of cloud heritage techniques with network security measures represents a significant advancement in the realm of wireless surveillance camera systems. This approach not only addresses the challenges related to storage and network security, but also introduces a level of privacy and data protection that surpasses conventional methods. By harnessing the computational capabilities of cloud resources, real-time image processing and analysis become both efficient and effective, even for cameras with limited onboard processing capabilities. The elimination of digital footprints further forti-fies privacy, making unauthorized access exceedingly difficult. Swift data retrieval ensures timely responses to security inci-dents, enhancing overall situational awareness. Additionally, the implementation of robust encryption and access controls safeguards the integrity and confidentiality of transmitted data, fortifying the system against cyber threats. As intelligent crime and security concerns continue to evolve, the cloud heritage technique, coupled with stringent network security measures, stands at the forefront of modern surveillance technology, providing a comprehensive and intelligent solution for safe-guarding assets and environments.

REFERENCES

[2] K. Aggarwal and R. 0. Duda, Eds., “Special issue On digital filtering and image processing,” IEEE .]H. C. Andrews, Computer Techniques in Image Processing. New York: Academic, 1970.ns. Circuits Syst., vol. CAS-2 pp. 161-304,1975.

[3] CTV British Columbia (2011) Riot report has Vancouver mulling more CCTV cameras. 2 September, http://www.ctvbc.ctv.ca (accessed September 2011).

[4]]H. C. Andrews and L. H. Enloe, Fjds., ”Special issue on digital picture processing,” Proc. IEEE, vol. 60, pp. 766-898, July 1972.

[5] https://www.simplilearn.com/image-processing-article