INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Model for the flow of CCTV footage Supervised Machine Learning rundown Streaming and Storage with the use of third-party auditing in the cloud

Bincy Joseph
bincy.j1989@gmail.com
A J Institute of Engineering and Technology, Mangalore, Karnataka

Sharon C D'Souza
sharon.gonsalv@gmail.com
A J Institute of Engineering and Technology, Mangalore, Karnataka

ABSTRACT

Video summaries help to convert long videos into short compact series for easy storage. Most of the CCTV footages are daily event capturing series and need to extract unusual events from these footages. And sometimes these compact footages need to be stored maintaining its integrity and security in some cases. After extracting the unusual events and cut shorting the daily CCTV footage it needs to be streamed wisely to review the same. The reviewing needs to be online or remotely from any corner of the world. As of now, we don't have a proper means of what to do with these CCTV footages. And how effectively and wisely we can store the footage securely. Here in this paper, we discuss a flow model for summarizing, extracting unusual events, streaming, and storage. With these methods, the final product would be more content bearing, storage compact, and secure.

Keywords— *Video summarization, Intelligent video surveillance, Supervised machine learning, Third-party auditing*

1. INTRODUCTION

Time and storage are the most important aspect of today's technology. All techniques and methods point to how fast and accurately technology works. More work in less time is the slogan for all the techies in this era. Crime rate and physical assault and accidents are increasing day-by-day so due to which CCTV is installed at all premises. These CCTV footages need to be reviewed on a daily basis or sometimes after many years of storage of the same. So just fixing CCTV cameras and deleting the data captured is of no use. After capturing the daily video in CCTV, it needs to be summarized, streamed and stored properly and securely. This turns out to be the procedure on a daily basis. Rather than just storing it somewhere, it is more important to store it securely from extruders.

Nowadays analyzing the CCTV footage on a quick review of a daily basis and storing it in a very compact form securely for later use is required everywhere. Due to the increasing unusual behaviors and police cases, the CCTV cameras are used everywhere in schools, colleges, offices, etc. as proof in case of any issues, this needs to be stored. But then the storage is another issue as to where to store these chunks of data and how effectively we can do that. A whole lot of daily captured chunks of data cannot be stored as such. We need a way to cut short these videos and make it as compact as possible. When we sought large chunks of video into small chunks, we need to take care of one more aspect in CCTV footages that is the unusual events. Without giving necessary weight to unusual events these compact chunks of CCTV footage do not have any meanings. So unusual event detection is the most important thing in storing the CCTV footage.

One way to keep an eye on this overflowing video is to summarize the content and develop intelligent video surveillance using machine learning. Video summary should concisely, briefly present the video along with unusual happening in CCTV footages. So once if the CCTV footage is obtained in the model then it is the continuous process of detecting unusual events and summarizing the video based on important key frames, streaming it and storing it securely at someplace. These unusual event detections vary differently according to the type of CCTV footage. So, [1] there are a variety of methods for the unusual event detection based on the type of CCTV footage.

A company or a corporate office where at the end of the day an employee or the owner itself might review the CCTV footage. At this point of time, that person cannot glance through all of the CCTV footage as a full session of streaming. What he wants to know are just the unusual events that have recorded. So, these unusual events and summarized video of the full footage needs to be streamed within less time. [2] a Whole lot of chunk needs to be reduced into a flash of events within a span of time. After reducing and streaming these compact chunks on a daily basis needs to be stored somewhere retaining its integrity. And reviewing needs to be anytime even after storage of data. And to check whether the contents are as it is or to verify whether the content is unaltered, we need a public auditing scheme on a periodic basis. So that the user need not worry about the data stored.

2. METHODOLOGY

The general architecture of the proposed model is shown in figure 1. To build compact storage of CCTV footage to be

stored in cloud computing using third-party auditing we need to check for the unusual event first then summarize and go for daily streaming in less time and finally store. Third-party auditing is to extract CCTV footage on-demand securely from storage so that the user needs not to worry about the storage retrieval and extraction on their own risk instead they can lend it to third-party.

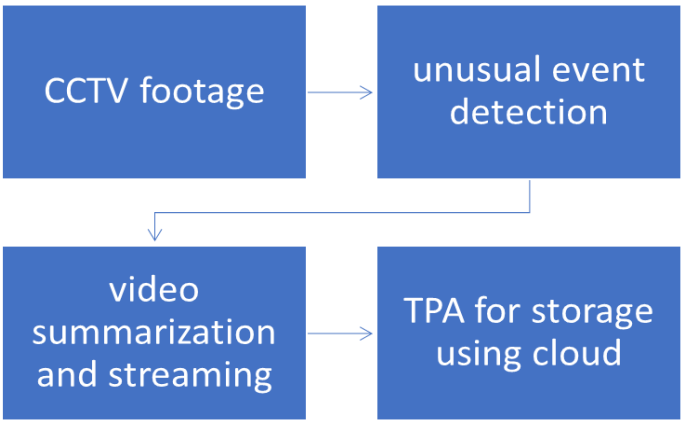

Fig. 1: Architecture of proposed model

Our proposed model consists of procedures as shown in general architecture and are:

(a) Unusual event detection
(b) Video summarization
(c) Streaming
(d) Storage

(a) UNUSUAL EVENT DETECTION

Supervised learning is a method under machine learning to train the system to give a pattern on usual event detection so that the system can be able to identify the unusual event in CCTV footage [1]. The most common anomaly detection algorithms outline anomalies in footages. Most common anomaly detection algorithms that can be used in the model are K-Means, One-Class support vector machines, Auto encoders.

And then for more advanced video formats According to Hu et al. [3] initially find the gradient among two local regions. Then construct a histogram of oriented contextual gradient (HOCG) descriptor for detecting unusual events in video surveillance. Without using complicated modelling techniques histogram of oriented contextual gradient (HOCG) can be used instead of a pixel-based histogram of oriented gradient (HOG) descriptors. As proposed by Hu et al. histogram of oriented contextual gradient (HOCG) is a better approach to be used in the detection of unusual events in our methodology.

(b) VIDEO SUMMARIZATION

At the end of the day in the corporate world if at all the daily CCTV footage has to be monitored then we obviously need a summarization technique. So that, user can manage the time to review the footage. Out of many video summarization techniques, going for summarization along with indexing will help to store the footage in order to help retrieval of data on demand.

Indexing and summarization produce data in a compact form for ease of retrieval. Automatic content summarization and indexing have attracted the new era. Multimedia uses several kinds of formats e.g. video+audio+text so we need multimodal analysis techniques for analyzing. Key frame-based representation gives a condensed form of representation.

An approach for summarization by Ji et al. present in [4] is a depiction of detected moving objects with respect to trajectories. For that first, the video sequence needs to be segmented based on a difference in leading-edge pixels detected in equal time separated frames (difference of 10 frames taken). Considering the last frame for video representation corresponding object trajectories are computed. Key frames are used for even more compact representation. Along with summarization object identification is required for indexing as mentioned in [5]. Observation of specific objects can be the indexes for CCTV footages and different indexing methods like B-Tree, B*Tree, B+ Trees can be used.

(c) STREAMING

Video streaming is necessary when you need to download and check for something in the footage. Or even you can stream online directly from the cloud storage provider. Now here comes the problem of how effectively it can be streamed. Without causing any delays if the video can be streamed then that is the better approach. For the streaming of the video third-party assistance is necessary to effectively glance through the video. Having the indexing technique from the summarization procedure the index would help the user to search for in the storage chunks of videos and streaming it. [11] Public and private key generated and handed between the user and the third-party auditor can be used any time to review the footage required. Reviewing can be done anytime anywhere without fully downloading the contents into one's own personal computer. The cloud storage using the third party helps the online review of CCTV footage. The keyframes collected and the unusual events in the footage in the videos can be fetched together for the reviewal process. Time for reviewing and place of ease for the user is the added advantage in this model.

(d) STORAGE

For secure storage of these daily CCTV footage rendering it to a third-party is a good approach in the cloud. Indexing helps in searching the particular dated or event-based video CCTV footage. The storage is secure because the third-party will never learn about the contents of the CCTV footage. There are different systems and security models [6],[8],[9],[10] for ensuring the security of remotely stored data. But they do not secure user data from third-party. Public auditability is required for more secure data verification. Furthermore, the user does not want his data to be leaked to these external parties [7] who does the public auditing process. For that purpose, encryption and decryption algorithms using public and private keys can be used. The user need not worry about storage capacity access and retrieval.

Third-party does the auditing for secure storage by helping out using private and public keys [11]. Storing data on a daily basis on one's own system is not feasible and better approach is using cloud storage with third-party auditing. Cloud providers 'pay as you use' policy. You pay for what and how much you have used. And need not worry about the memory capacity to be extended on demand. So that user need not worry about integrity, the security of the data content.

3. CONCLUSIONS AND FUTURE WORK

This paper presents a flow of video summarization, unusual event detection, effective streaming and storage using third-party auditing. We proposed possible effective ways in each of the flow. This routine procedure will help to store CCTV footages in order.

Future work will be viewed with the aspect of introducing more efficient ways and technologies for the flow of indexed storage of CCTV footage. Different technologies like Big-Data analytics, Deep learning, etc. can be merged into the proposed flow in this model.

4. REFERENCES

[1] Seemanthini. K, Akhila. S. Jain, Ashwin. M. Bharadwaj, Hema. B. M, & Meghana. P V, "A Survey on Unusual Event Detection in Videos". *Journal of Computer Science Engineering and Software Testing*, e-ISSN: 2581-6969, Volume 5, Issue 2, 2019.

[2] Ajmal, M., Ashraf, M. H., Shakir, M., Abbas, Y., & Shah, F. A. (2012, September). Video summarization: techniques and classification. In *International Conference on Computer Vision and Graphics* (pp. 1-13). Springer, Berlin, Heidelberg.

[3] Hu, X., Huang, Y., Duan, Q., Ci, W., Dai, J., & Yang, H. (2018), "Abnormal event detection in crowded scenes using histogram of oriented contextual gradient descriptor". *EURASIP Journal on Advances in Signal Processing*, %$, 2018.

[4] Z. Ji, Y. Su, R. Qian, and J. Ma, "Surveillance video summarization based on moving object detection and trajectory extraction," in Signal Processing Systems (ICSPS), 2010 2nd International Conference on, vol. 2, July 2010, pp. V2–250 –V2–253.

[5] W. Ding and G. Marchionini, "A study on video browsing strategies," University of Maryland, College Park, Tech. Rep. CLIS-TR-97-06, 1997. [Online]. Available: http://hcil2.cs.umd.edu/trs/97-11/97-11.html

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 598–609.

[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS'09, volume 5789 of LNCS*. Springer-Verlag, Sep. 2009, pp. 355–370.

[9] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 584–597.

[10] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. of Asiacrypt 2008*, vol. 5350, Dec 2008, pp. 90–107.

[11] Dr.Challa Narasimham. , Pachipala Yellamma., Data security in the cloud using rsa 4th ICCCNT - 13 July 4 - 6, 2013, Tiruchengode, India.

