Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.456 – 464

RESEARCH ARTICLE

DIGITAL FORENSICS SERVICE PLATFORM FOR INTERNET VIDEOS

N. Deepak[1], B. Arunkumar[2], Dr. T.V.P.Sundararajan[3]

[1,2]*PG scholar, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India – 638401.*

[1]deepakn.ae12@bitsathy.ac.in

[2]arunkumarb.ae12@bitsathy.ac.in

[3]*Professor, Bannari Amman Institute of Technology, Erode, Tamil Nadu, India -638401.*

suntvp@bitsathy.ac.in

***ABSTRACT*- Digital Forensics is an emerging technology, which is used to detect illegal content in videos. In this project, the main objective is to use the Content Delivery Network (CDN) based Resource Aware Scheduling (CRAS) algorithm to find the originality of the video. CDN transmits the packets from source to destination in the real-time approach. The sample video is given in terms of frames, where the frames are *i* frame, *b* frame, *p* frames respectively.**

CRAS algorithm schedules the tasks efficiently in the Digital Forensic Service Platform (DFSP) according to resource parameters such as delay and computational load. The proposed system decreases node traffic and improves the scalability.

***Keywords*- Digital Forensics, Fingerprint, Watermarking, Content access, video detection**

I. INTRODUCTION

As the number of videos distributed over the internet increases rapidly, there is a need to solve this problem. A recent study states that, 23.8% of the internet traffic is due to the illegal videos. So there is a need to develop the security for the internet videos. Digital forensics system helps to overcome this problem. Various techniques are used to find the illegal contents in the videos. Fingerprinting, Watermarking, Feature selection and comparison are some of the techniques. This paper mainly deals with the above mentioned techniques. The large amount of computation cost and communication cost are the major issues in the existing techniques. To solve the scalability and efficiency problems, we proposed some technique.

A novel large scale digital forensics service platform for internet videos is the advanced system proposed by Haoyin and Wen Hui[7]. In this work, the main task is to reduce the communication cost and scalability problems. CRAS algorithm used in this paper, detects the legality of the videos over the internet.

Applications of Digital Forensics:

Digital Forensics is commonly used in criminal law and private investigation. An unauthorized network intrusion can be found by this Digital Forensics system. Computer Forensics, Mobile device forensics, Network forensics, Database forensics, Forensic data analysis are all some of the fields where the digital forensics technique is used for monitor and detection purpose.

II. LITERATURE SURVEY

Sunil lee and ChangD.yoo [1] proposed Robust Video Fingerprinting Based on Affine Covariant Regions for detecting illegal contents in videos. In the existed method, they identified the video clip by using short feature vectors, which are all given as the fingerprints. In the proposed method, local fingerprints are extracted from the affine covariance region in each frame. The Maximally Stable Extremal Region(MSER) [2]is used for the detection of the affine covariant regions. The computational complexity of the MSER method is low.

The local fingerprints are extracted as follows, which is given in the block diagram. Figure1 shows clearly as how the local finger prints are extracted from the given video data. Detection of affine covariant regions and geometrical normalization along with the partition and overlapping plays major role in detecting the local fingerprints.

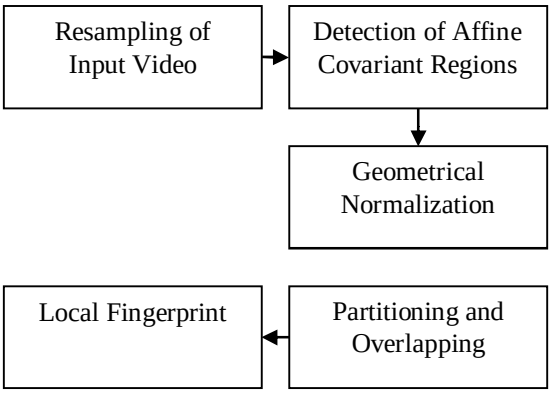

Fig.1: Extraction of local fingerprints.

In the proposed method, the detected regions are geometrically normalized and resized to the fixed size. And they are partitioned into the sub blocks which overlap each other. Matching of local finger prints and performance evaluation are the next two steps. Initially the local finger prints of the query video and original candidate videos are retrieved by searching on the Database of video clips. In this process we get the set of matched pairs. Also the performance can be evaluated by performing the above mentioned task for many videos and they are given as geometric and non-geometric distortions. Thus, the experimental result shows that the proposed method is performing very well against the geometric and non-geometric transformations like cropping, rotation etc.

Weihong Wang and HanyFarid,[3] proposed a paper on detecting duplicate videos under the title, Exposing Digital forensics in videos by detecting duplication. In this paper, they presented a computationally efficient technique for finding the tampering videos. Frame duplication and region duplication are used as main methods to find the illegal content. In the frame duplication method, an algorithm is used, in which video sequence length and various threshold values like spatial, temporal are used to detect the unwanted theme. In region duplication scheme, stationary camera is used and pair of frames are obtained. Further by using Phase correlation[4], the duplicated frames are found. In moving camera approach, the illegal content is obtained easily by the comparison of frames. Thus the result of this paper is given as follows. The first method detects the entire frames, which are all duplicate. These second technique finds only if a portion of frames are duplicated. And also the results shows that these algorithms can detect more duplications in high and low quality video. This techniques are producing good results when comparing to the existing techniques.

Maher elarbi, Chokri Benamarandhenri Nicolas presented a paper which described a blind video watermarking system invariant to geometrical attacks. The major problem in watermarking is recovery of watermark in the presence of geometric attacks like frameshift, cropping, etc,. Existed technique gives result based on the wavelet domain in comparison of neural networks and motion estimation[5]. This method also uses wavelet domain, in which watermark is added to the different shots of video. So this technique can give good efficiency than the existing method. An algorithm is used for watermarking the video content, for which the following block diagram is used.

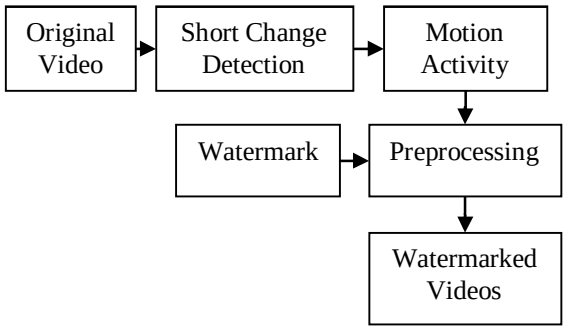

Fig.2: Watermarking Block diagram

In this process, initially the video is passed to the shot change detection then after the motion activity, pre processing the watermark, we get the watermarked video. The watermark is used for monitoring the video to find the legality of the particular video. Also the secret key is used to find the unauthorized videos. Here to find the performance of the scheme, some experiments are done, including shifting of frames, cropping, rotation attack, resize attack. From these tests, we can say that proposed method is finding the requirements perfectly.

Hua Zhong and Janbo Shi [5] proposed a method for Detecting unusual activity in video. In that paper ,they present a technique for detecting unusual activity in a videoset using some sample features. The video is divided into equal segments and classify extracted features and create a co-occurrence matrix. Model based approach, unsupervised approach and Feature selection approach is used in this technique. Initially image features are extracted from the video by detection and tracking process. Model based method is complex to find the result in the real time videos. And also have to select the features correctly to get the comparison results correctly. Video representation is given as video segmentation, image features and prototype features. To detect the unusual activity in the video new algorithm used. Unusual event detection algorithm is having the following steps. Initially the K-means algorithm is used. Then inter cluster similarity have been calculated. Finally by comparing this value with the total value can find the unwanted activity in the video set. To get the performance results, various tests are taken in various environments. From the tests can conclude that, this method make use of the simple features by automatically selecting the important feature signal. The results are efficient and stable.

Li Zhang, Bo Wu and Ram Nevatia[6] presented a paper on Pedestrian Detection in Infrared Images based on Local Shape Features. In which, the IR images is advantageous for many surveillance applications where the systems must operate around the clock and external illumination is not always available. The IR images are extended by using two feature classes and two classification models.

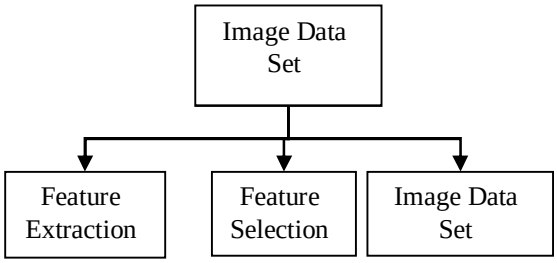

Fig.3: Outline For Dupli0acte image approach

The human detection approach consists of three stages as shown in fig. local feature extraction, feature selection and object classification. In feature extraction part, local spatial information of image is transformed into a feature space that is descriptive of the shape and appearance of the object but less sensitive to noise and other variations.

III. SYSTEM ARCHITECTURE

The Digital forensics service platform system contains the system architecture which is given in the fig4. Content access, Video detection, Resource management and Network monitoring module are all the basic blocks of the DFSP system.

A. Content Access (CA)

Content Access is placed in every CDN node, that is used to obtain video data from media sources. During this process, web crawler technology is used for web search to collect the data. This technology can scan through Internet pages to create an index of video data.

B. Video Detection (VD)

Video Detection is nothing but the number of servers grouped and distributed near the CDN nodes. VD is responsible for checking the video content to judge their legality. It contains Blacklist Database, Content Analysis Servers, and Searching and Matching Servers. Here the “Blacklist” Database is used to find the improper finger prints of improper videos and stores it. Content Analysis

Servers are used to analyze the video content. And fingerprints are extracted for the video. Searching and Matching Servers compare these finger prints with those pre-stored in "Blacklist" Database, and judging their originality.

C. Resource Management (RM)

RM controls and monitors the whole system. It is to schedule, coordinate, and manage all the resources and tasks. It have two main blocks. They are Network Monitoring module and Load Balancing module. Network monitoring module is in charge of monitoring all the nodes and media sources. And the Load Balancing module can control all the nodes and schedule different tasks based on the situation. To balance the load among multiple nodes, CDN-based Resource-Aware Scheduling algorithm is used.

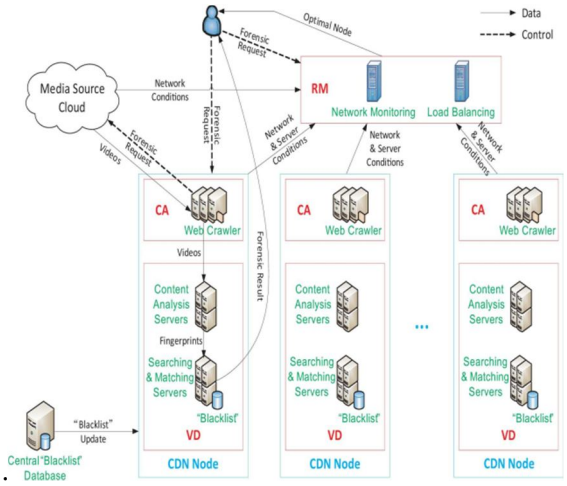

Fig.4: DFSP working flow

DFSP working flow is given in the above diagram. This fig 4 is given based on the reference paper [8]. Once a user requests to detect a media source. Then the request is first transferred to RM. Then RM processed and find an appropriate node for the media source. Finally the user request is then redirected to the selected node.

CA of the particular rnode obtains video data from the media source and then transfers them to VD. After that ,VD of the particular selected node analyzes the video content coming from the media source and extracts their fingerprints. These fingerprints are compared with those pre-stored in "Blacklist" Database. Finally, the legality of these videos, which is determined by the comparison result.

A Web crawler is an Internet technology that automatically browses the World Wide Web and indexing is done over here. A Web crawler may also be called as Web spider or an automatic indexer. Web search engines and some other sites use Web crawling or spidering software to update their web content.

D. Spatial Temporal Unit

For all key frames, frames before and after it are called as adjacent frames, as shown in the fig 5. Here we set 100ms between two adjacent frames. Key frame and its adjacent frames represent a short term of video that is with the key frame middle in it. We call this short video as a Spatial-Temporal Unit (STU), denoted as in the fig 5 [7].

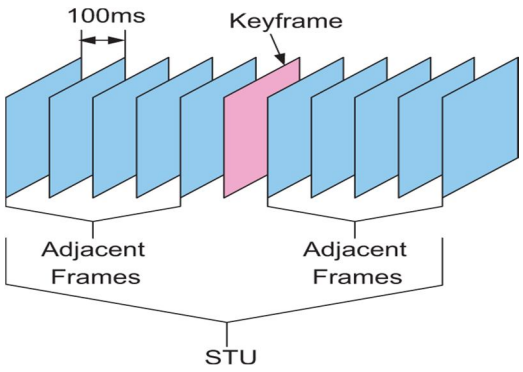

Fig.5: Key frame and its adjacent frames

In the field of video compression a video frame is compressed using different algorithms, centered mainly a round amount of data compression. These different algorithms for video frames are called picture types or frame types. The three major picture types used in the different video algorithms are,

I frame
B frame
P frame

I frames are the least compressible but does not require other video frames to decode. P frames can use data from previous I frames to decompress and are more compressible than I frames. B frames can use both previous and forward frames for data reference to get the highest amount of data compression.

E. Feature Extraction and Video Representation

Here the motion feature and global feature are used to represent an STU. It is known that within a short video clip, motion (including object, background, and camera motion) can be used to identify the content of video clip. First, we track the interesting points in each frame in an STU and get the motion direction of each interesting point. In practice, we use Kanade-Lucas- Tomasi (KLT*)* Tracker to track the trajectory. Second, we define nine directions of the trajectories. In addition to motion feature, we also use global feature in STU, including average color moment vector and average color histogram vector in HSV space, denoted by d_{cm} and d_{cm} respectively. As a result, we get the final feature vector of STU, denoted by

$$d^q = (d_{cm}, d_{cm}, d_{mot}) \qquad (1)$$

F Video Indexing And Matching

To speed up the process of video matching, we index videos using inverted file. Inverted file is an effective data structure in information retrieval system.

Let $tf_{t,d}$ be the inverse document frequency, which can be formulated as,

$$idf_t = \frac{N}{df_t} \qquad (2)$$

where N is the number of videos in the data set, and refers to how many videos contain word in the dataset. Then we assign a weight for each word in video as follows.

$$w_{t,d} = t.f_{t,d}.\ idf_t \quad (3)$$

Thus, video can be represented by $V(v_i) = [w_1, w_{2.....}w_i]\ |w|$,where |w| is the vocabulary size of video words codebook. Let Sim (v_i, v_j) be the similarity score v_i of video and video v_j, which is defined as,

$$Sim(v_i, v_j) = |V(v_i), V(v_j)| \quad (4)$$

Although v_i and v_j are long, given that they are sparse, by using inverted indexing structure, the computational complexity brought video matching is not very high. According to the query videos coming from the designated media sources are compared with those pre-stored in "Blacklist" Database.

IV. EXPERIMENTS AND RESULTS

For this work, ns2 simulator tool is used. Here the scalability, packet delivery ratio are shown as the result. Initially every node has been given in different colors, by proper color assignment. The original video is segmented into its equivalent frames. *i*frame, *b* frame and *p*frame are the basic types of frames.

To reduce the node traffic and time complexity, scheduling has been done. For scheduling, the files are configured for recording. After this assignment process, the packets are sent to the estimation from the source.

NUMBER OF NODES VS NUMBER OF TRANSMITTED PACKETS

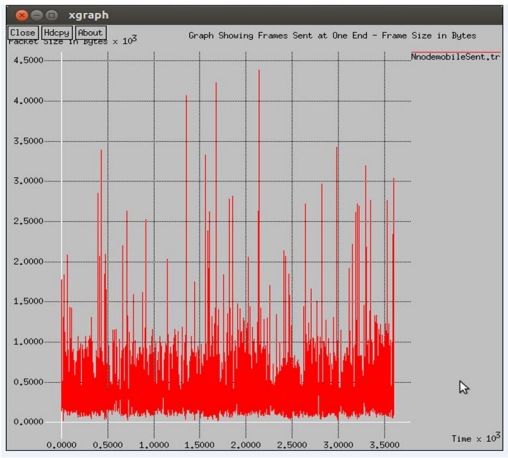

Fig.6: Number of Transmitted packets

Fig 6 shows that the number of transmitted packets among the nodes with respect to simulation time. The number of packets transmitted at the initial time is lesser than the number of packets transmitted at the final time. At the moderate time the packet transmitted is maximum. It is due to the traffic in the packet transmission between the nodes.

NUMBER OF NODES VS NUMBER OF RECEIVED PACKETS

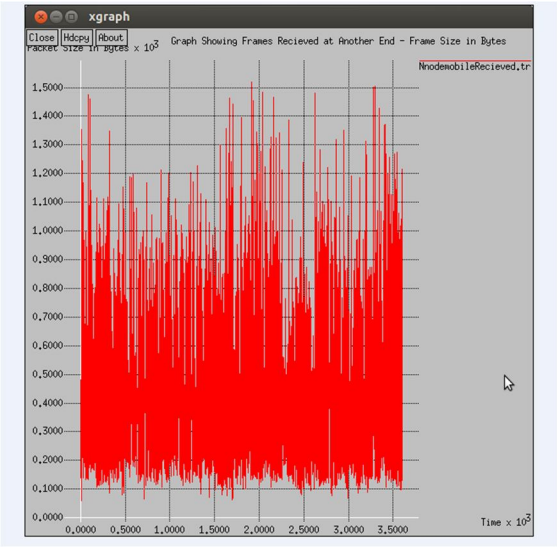

Fig.7: Number of received packets

Fig.7 shows the number of received packets. During transmission, some of the packets are dropped due to traffic. So there is loss of packets while receiving. The receiving rate of packets is same at both starting and ending time.

MEDIA SOURCES VS AVERAGE DETECTION TIME

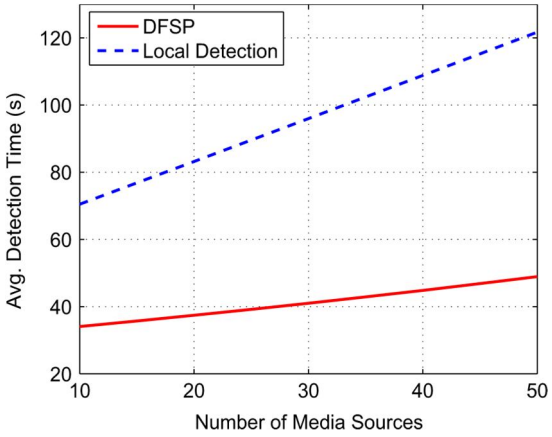

Fig.8 : Average detection time versus number of media sources.

Fig 8 shows the comparison of local detection and the DFSP system detection. The result is based on the number of media sources and detection time. From the fig.6 it is shown that, DFSP system is more efficient than the other approaches. In order to evaluate the scalability of the platform, in the third set of experiments, detection time is measured based on a variety of videos from ten arbitrary media sources. Fig.8 shows that the detection time with respect to the number of user queries. It can be observed from Fig.8 that the *DFSP* has a relatively stable detection time with the increasing number of user queries, which demonstrates better scalability. The average detection time is 35.2s. Despite the heavy demands on the video detection, the *DFSP* architecture is able to distribute the computation load among several nodes, which saves computation time significantly. Number of media sources are taken as 50to 100. It will help in getting good result.

TRANSMISSION OF PACKETS BETWEEN NODES

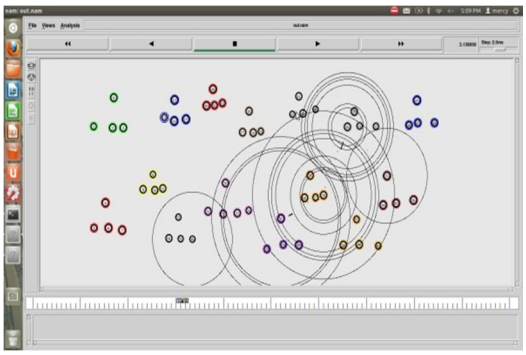

Fig.9: Transmission of packets between nodes

The fig 9 shows the transmission of packets among the nodes. Different color shows the different kind of nodes in the result. Green, yellow and red colors are used to represent the nodes. Green color represents the source node, yellow color represents the route node ,and red color represents the destination node.

V. CONCLUSION AND FUTURE WORK

In this paper the novel large-scale digital forensics service platform for the videos is proposed. More specifically, DFSP architecture is built upon CDN infrastructure. By taking advantage of CDN, distributed architecture has been constructed that has good scalability. Also a system is proposed to identify the number of packets transmitted and number of packets received.

The future work of this paper can be increasing the scalability by modifying the Content resource aware scheduling. And also, the delay factors and throughput also concerned in the future work.

REFERENCES

[1]Sunil Lee and Chang D.Yoo, "Robust Video Fingerprinting Based on Based Covariant Regions," in *proc. ICASSP'08, 2008,* pp. 1237-1240.

[2]J. Matas, O. Schum, M. Urban, and T. Pajdla, "Robust wide-baseline stereo from maximally stable ` extremal regions," in *Proc. Brit. Mach. Vision Conf.*, pp. 384-393,2002.

[3]W.Wang and H.Farid,"Exposing digital forensics video by detecting duplications,"in*Proc. ACM Workshop Multimedia and security*, Dallas, TX, Sep. 2007,pp.35-42.

[4]C. Kuglin and D. Hines. "The phase correlation image alignment method".in *IEEE International Conference On Cybernetics and Society*, pages 163–165, New York,September 1975.

[5]H.Zong, J.Shi and M. Visontai, "Detecting unusual activity in video",in*proc. IEEE Int. Conf. Computer and Pattern Recognition,2004,* vol, 2, pp II-819.

[6]L.Zhang, B.SWu and R.Nevatia, "Pedestrian detection in infrared images based on local shape features," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition,*2007, pp, 1-8.

[7]Hao Yin and Wen hui Hong li and ChaungLin,"A Novel Large Scale Platform for Internet Videos",in*IEEE Transactions on Multimedia,* VOL, 14, NO, FEB, 2012.

[8]M. Douze, A. Gaidon, H. Jegou, M. Marszalek, and C. Schmid,"INRIA-LEARs video copy detection system," in *Proc. TRECVID Workshop*, 2008.

[9]P. Xu, L. Xie, S. Chang, A. Divakaran, A. Vetro, and H. Sun, "Algorithms and system for segmentation and structure analysis in soccer video," in *Proc. IEEE ICME*, 2001, pp. 928–931.

[10]J. Gauch and A. Shivadas, "Identification of new commercials using repeated video sequence detection," in *Proc. IEEE Int. Conf. Image Processing*, 2006, vol. 3.

