Accepted Manuscript

RIMS: Real-time and intelligent monitoring system for live broadcast platform

Yangfan Li, Wei Ren, Tianqing Zhu, Yi Ren, Yue Qin, Wei Jie

PII: S0167-739X(18)30175-4
DOI: https://doi.org/10.1016/j.future.2018.04.012
Reference: FUTURE 4090

To appear in: *Future Generation Computer Systems*

Received date : 28 January 2018
Revised date : 20 March 2018
Accepted date : 4 April 2018

Please cite this article as: Y. Li, W. Ren, T. Zhu, Y. Ren, Y. Qin, W. Jie, RIMS: Real-time and intelligent monitoring system for live broadcast platform, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.04.012

RIMS: Real-time and Intelligent Monitoring System for Live Broadcast Platform

Yangfan Li[a,e], Wei Ren[a,b,e,*], Tianqing Zhu[c], Yi Ren[d], Yue Qin[a], Wei Jie[f]

[a]*School of Computer Science, China University of Geoscience, Wuhan, P.R. China*
[b]*Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences (Wuhan), Wuhan, P.R. China*
[c] *School of Information Technology Faculty of Science, Deakin University, Australia*
[d]*School of Computer Science, University of East Anglia, Norwich, UK*
[e]*Guizhou Provincial Key Laboratory of Public Big Data GuiZhou University, Guizhou, P.R. China*
[f]*School of Computing and Engineering, University of West London, UK*

Abstract

Personal live shows on Internet streaming platform currently is blooming as a popular application and attracting several millions of users. The content supervision of live streaming platform, in which hundreds of show rooms perform synchronously, is a major concern with the development of this new kind of service. Traditional image captures and realtime content analysis experience huge difficulties, such as processing delay, data overwhelming and analysis overhead. In this paper, we propose a new method to monitor real-time live stream and identify illegal live misbehavior intelligently based on state of perception and frame difference analysis. The proposed system makes use of several indicators of the chatting room status rather than analyzing images solely and directly. Three kinds of detecting techniques are adopted: self-adaptive threshold-based abnormal traffic detection, sensitive comments perception, and state evaluation. The proposed system captures the segmentation of video scenes by frame difference analysis, and pays more attention on the showing room that has large scene changes. We deploy our system to monitor a typical live platform called panda.tv, and the overall accuracy of three indicators reaches 90.1%. The application of this system can change current situation where the live platform supervision totally depends on manual review. The key techniques in this system can be widely

*Wei Ren,weirencs@cug.edu.cn

employed in many applications, such as live broadcast platform industries, video surveillance for state security, and the national security for counter-terrorism.

Keywords: Live Streaming Platform; Anomaly detection; Fuzzy Matching; Frame Difference Analysis; State Awareness

1. Introduction

The number of live streaming platforms and the audiences are both remarkably increasing[1, 2]recently. For example, Douyu, the biggest live streaming platform in China, announced that the number of active users per month reached to 1.5 billion. As early as 2015, another live streaming platform, Twitch said it had nearly 100 million visitors and 1.5 million broadcasters per month. Thousands of network anchors are playing games on that platform and have real-time communicate with their audience. A popular form of live video streaming involves charming ladies. They dance, yak, sing, engaging their audiences via mobile phones and personal computers. Visitors may pay for gifts provided by platforms and donate to performers; Performers can share the profit of gifts in proportion.

Live broadcast has attracted millions of audiences, and it also imposes great difficulties for realtime management and supervision. Its openness, elapse, and a large amount of online viewers may result in significant security risks[3, 4, 5]. For example, an illegal or un-properly broadcasting or comment will result in a serious impact or indications, especially when the number of participators in the room as large as tens of thousands. For example, in Jun. 2016, a well-known network anchor live shows drag racing, causing a car accident. Thousands of viewers have witnessed the incident. In Oct. 2016, a network anchor in douyu.tv live shows the process of taking off his clothes. Although the room was terminated by the administrator, it is almost half an hour later.

At present, the live streaming platform mainly takes manual review to identify illegal video. However, it is not easy to define a specific misbehavior, and there are too many patterns of illegal behaviors for checking by administrators. To reduce the workload, some companies try to use the machine-assisted identification. The main idea is straightforward by analyzing real-time video content. Some algorithms may have good performance in pornographic video recognition, however, there are hundreds of live streaming

videos simultaneously, and pornographic video is just the tip of the iceberg. Once one pattern is included, many other patterns occur. The accuracy of video analysis solely is unacceptable. Moreover, the network anchor in live streaming platform may make use of legal loophole, and only a few seconds of illegal broadcast is released for earning instant profit. Thus, the identification system may be cheated easily.

To fix above problems, this paper proposed a monitoring system that does not direct to analyze real-time video frames but focus on indirect factors or indicators. Our system makes use of three techniques: using self-adaptive threshold-based abnormal traffic detection to find the abnormal living room; monitoring the Danmaku (a realtime comment) between each live broadcast to discover sensitive words perception based on fuzzy matching; splitting the video stream into separate scenes and focusing on the room where scene changes. When we comprehensively evaluate above all indicators, the detection efficiency and accuracy will both be improved significantly, and especially, we don't need to capture and process each video streams. The proposed system can also discover new type of illegal patterns because the detection system is not solely based on image analysis.

The organization of the paper is as follows. The related work is described in Section 2. Section 3 describes some basic settings about monitoring of live video streaming platforms. In Section 4, we describe proposed system and key techniques. In Section 5, we conduct some experiments and evaluate the performance of the system. Finally, concluding remarks and possible future work are mentioned in Section 6.

2. Related Work

There are many ways to prevent illegal video at live streaming video platform like twitch.tv, douyu.tv and panda.tv. The most extensive study falls in image recognition. Felzenschwalb and Huttenlocher [6] proposed a graph-based EGBIS approach, which is a super pixel method. The segmentation of images often is input into the analysis system. The resulting segments are often called super pixels, which can be used for further analysis to compute certain information about objects in pictures and to recognize the content of videos. However, for realtime video content analysis, it is hard to find a proper algorithm to compute super pixel representations without decreasing the quality of the results. Jochen Steiner and Stefanie Zollmann introduced an incremental super pixels for real-time video analysis[7]. The basic idea of

the method is to divide the process of traditional EGBIS segmentation into smaller steps. They improved the segmentation methods that are based on finding minimum cuts in a graph. Some other systems analyze the real time motion to understand the semantic of video content. Yong Wang et al. [8] proposed a real time video motion analysis system. They use object detection, object tracking and camera motion understanding to get results. That system balances the computational complexity an analysis performance.

Aforementioned analysis systems target to analyze realtime video. They might have a good performance to some extent. However, live broadcasting platform is more complicated than tradition realtime video. The types of traditional video are relatively fixed, and the publisher usually is a specific organization. While as for live broadcasting platform, there are thousand kinds of living rooms that need to be analyzed at the same time. Everyone can broadcast a live show, as long as he has a computer or a mobile phone. Monitoring system may not be able to process new kinds of illegal videos and very likely miss some of them. For a live streaming platform, one time of missing may lead to serious social influences and damage the reputation of platform companies. Moreover, we argue that such image recognition based methods cannot be applied in realtime broadcast platform due to processing delay, and especially when there exist thousands of videos at the same time.

We observed that frame difference method is wildly used in background subtraction[9], Object Detection and tracking[10]. This method can accurately extract the main content of the image, and analysis the action of the content[11, 12]. This technique can be used for detecting sense changing within a manageable delay.

In live streaming video platform, every room has its own network traffics. Many methods for abnormal traffic detection are proposed [13, 14, 15, 16]. Zhengmin Xia et al. proposed a realtime and self-adaptive method for abnormal traffic detection based on self-similarity. It works well for abnormal traffic detection and unknown variants of attacks.

We will comprehensively adapt above methods in building our experimental system, focus on the indirected factors such as room status and parameters, instead of relying on image analysis solely. Our monitoring methods present following advantages - much faster detection (or shorter delay), more scalable, more general (in terms of video types), and more accurate.

3. Basic Settings

In this section, we briefly describe technical structures of the system. Fig.1 depicts the IPO model of the system.

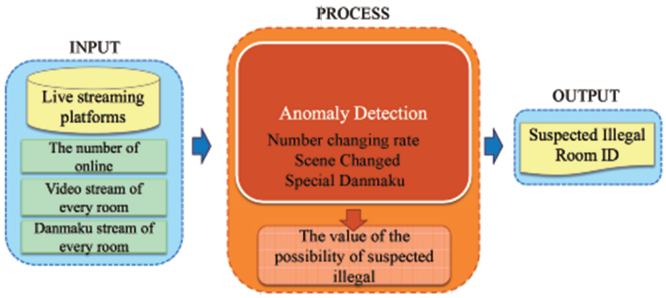

Figure 1: IPO(input process output) model of the system

3.1. Live video streaming cloud and Danmaku

Living broadcast platform cloud is an emerging cloud computing platform in mobile Internet. This cloud needs to support a large number of users for video broadcasting and browsing. As it is convenient for interacting by Danmaku between users and hosts, that is flying over the video image during broadcasting, it becomes a popular application in young generation users pervasively once it is released.

Danmaku is a realtime word displaying system that shows audience's feedback on current live video as multiple lines of moving comments overlaid on the screen. It is always used as a common component in live streaming platforms[17].

3.2. Abnormal traffic detection for show room

Abnormal traffic detection for a show room also imposes challenges, as the number of rooms may be thousands and the detection must be realtime. Although currently there exist a lot of methods to detect abnormal network traffics, most of them is not designed for multimedia traffics as well as not for realtime detection. Tailored design for live broadcast platform is required, in which self-adaptive threshold abnormal traffic detection is promising. We regard show rooms in the platform as a hub-based network, and traffic detection can be easily accomplished[18, 19].

3.3. Scenes segmentation

To find out which rooms have scene changed, computer image processing algorithms can be used for scene segmentation and variation detection. The non-differentiate scene usually presents the similar contents, and similar contents can be looked as one detection slot. Live steaming video is composed by many scenes, thus one scene is processed as an element unit. If we can determine that the previous scene is legal and the next scene changes slightly, we can consider that the next scene is also legitimate with high confidence. Put it in another way, we assume that most illegal scenes are always short in time, are jumped in dramatically for attracting instant influences, and can not be arranged in advance. Thus, our system focuses on the living rooms which present the obviously scene changing, which can greatly increment the processing speed and shorten the detecting delay.

3.4. Frame difference analysis method

When any person or object in a live scene moves, there is a noticeable difference between two adjacent frames[20]. Frame difference analysis is mainly used to detect adjacent frames of the image to capture the movement. The adjacent two frames will be compared, and a live showing room is suspected illegal when the computed difference is larger than a tuned threshold[21, 22, 23, 24]. The threshold can be determined and set by an experienced administrator of platforms, and it should be changed dynamically to approach the better false positives and false negatives[25].

Frame t subtracts frame t+1, and we can get a binary image D(u, v) , where u is the row of the pixel, v is the column of the pixel, and the function f is to get the gray value of frame t. D(u, v)is calculated as follows:

$$D(u,v) = \begin{cases} 1, |f_{t+1}(u,v) - f_t(u,v)| \geq T \\ 0, |f_{t+1}(u,v) - f_t(u,v)| < T \end{cases}$$

According to our experience we previously set the threshold as T. In the binary image, 0 represents that there exists no change in the adjacent frames, 1 represents that there exist changes. The flow chart of the frame difference analysis is shown in Fig. 2.

The advantage of proposed algorithm lies in that various image situations can be tackled by the adaptively setting parameter.

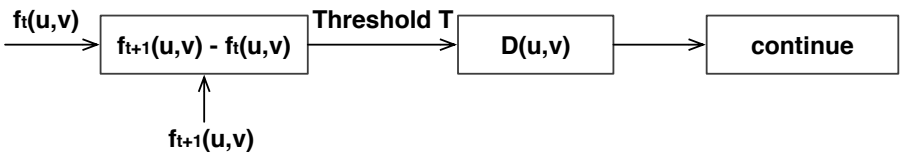

Figure 2: Frame difference analysis framework.

4. Proposed Scheme

Our proposed scheme consists of three primary modules to detect abnormal live show rooms, which constructs realtime monitor tools for platform administrators. The three modules of our system run independently, but the ultimate goal is the same to find suspected illegal rooms. The first module monitors the flow status of live room per unit time, and compares it with our pre-calculated thresholds to judge suspected situations. The second module captures Danmaku flows by connecting Danmaku servers, and then matches the Danmaku sensitive words with our pre-set Danmaku library. If the match succeeds, it will prompts suspected violations. The third module relies mainly on the screen shot from live stream for state sensing and analysis on frame difference, and the suspected illegal room is evaluated by the result of frame difference analysis. In this section, we will introduce above three primary modules. Fig. 3 depicts the architecture of proposed system.

4.1. Self-adaptive Threshold-based Abnormal Traffic Detection

The total number of viewers in the room is regarded as the major indictor of room traffic in this module. In order to implement the abnormal traffic detection by self-adaptive threshold, we conduct following technical steps as follows:

We use *jsoup*, a HTML parser based on Java, to parse out the number of live rooms and the number of entire online users accordingly from acquired html.

Subsequently, we record the total number of viewers (denoted as nov) in a live roomi (i is the room id) for each time segment (denoted as ts).

After that, the growth number per hour, denoted as K, is calculated by using linear regression equation. The formula for K is:

$$K = \frac{\sum_{i=1}^{n} ts_i * nov_i - n\overline{ts * nov}}{\sum_{i=1}^{n} ts_i^2 - n\overline{ts}^2}$$

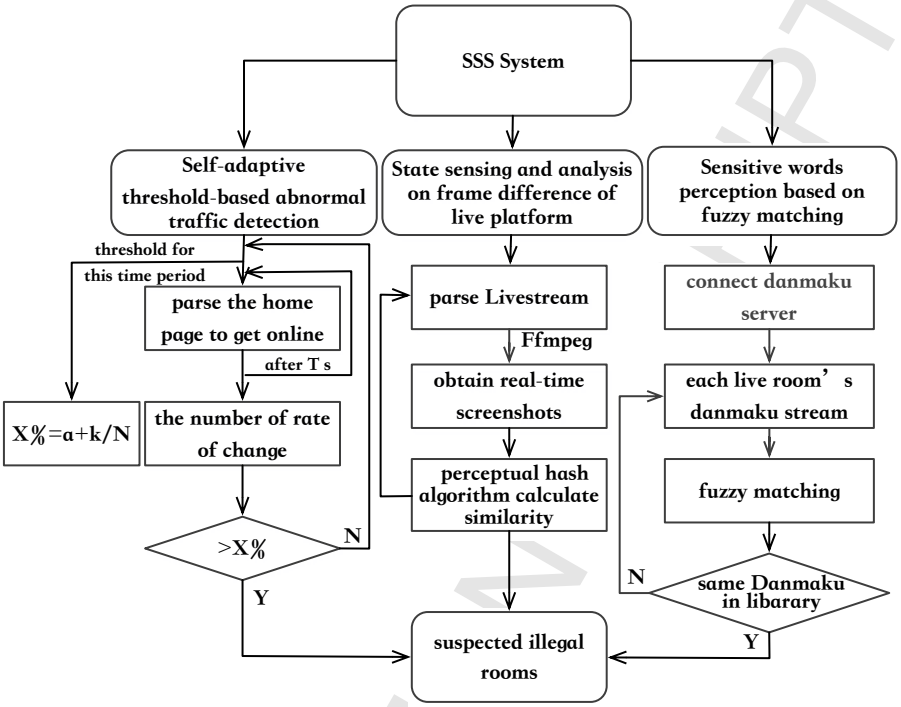

Figure 3: The architecture of the proposed system

n represents the total number of time segments.

Therefore, we define K/N (N is the number of online users at the beginning for this hour), which represents the growth rate of online user numbers in this hour.

We define $B = 1/N$, the number of growth rate $K * B$ regarded as an important parameter of adaptive threshold. Thus, we use $K * B + \Delta$ to calculate the threshold value ((our observation and experimental experiences convince the rationality of this threshold). The threshold is therefore calculated as follows: $X\% = K * B + \Delta$

If the actual growth rate of online user number is greater than this threshold, this room is regarded as an abnormal room with high confidence, and the number of this room will be displayed on the alter interface of our monitoring system.

We noticed that $K * B$ becomes larger when the number of the online users grows extremely fast during a given time slot. The threshold value can be tuned larger correspondingly. Thus, the actual growth rate of online user

number calculated by the system should be bigger for denoting an abnormal room.

On the contrary, if the number of online users grows slowly, or even declines, the threshold value should be set smaller accordingly. Subsequently, when the actual growth rate calculated by system is slightly greater, this room will be considered as abnormal. Hence, this adaptive threshold is reasonable to indicate suspicious live rooms.

In other words, the system tunes a threshold value related to the current time and room id, which is an acceptable rate and denoted as X, for each live room about online number per hour. The threshold is adaptive as realistic situations of each time may be differentiate, in order to avoid false positive and false negative jitters. Therefore, the threshold value should fall in an acceptable range of deviation. The adaptive algorithm for tuning of threshold value is given in Algorithm 1 as follows:

Algorithm 1: Self-adaptive threshold-based abnormal traffic detection

Input: current time , living platform's target url
Output: unusually $roomid_i$
Data:
$n \leftarrow$ living platform's room number
$K \leftarrow$ the rate of change of all people
$X \leftarrow threshold$

for $i \leftarrow 1$ **to** n **do**
  $xi \leftarrow$ the current number of people in the $Room_i$
  $yi \leftarrow$ the number of people in the $Room_i$ after t seconds
  $K = \frac{\sum_{i=1}^{n} x_i y_i - \overline{xy}}{\sum_{i=1}^{n} x_i^2 - n\overline{x}^2}$
  $X\% = a\% + KB$
  if $K > X$ **then**
    output unusual $roomid_i$
  else
    continue
  end
end

4.2. Sensitive Words Perception

This module is achieved by simulating multiple clients that can connect Danmaku servers to elicit Danmaku streams. As for the detection on sensitive messages in flying Danmaku, the traditional way only concentrates on sensitive words from huge amounts of Danmaku databases, which reduces detection efficiency. Thus, we first collect large amounts of sensitive words in the scope of anti-terrorism, heresy, pyramid selling, disunion and pornography, etc. Subsequently, we list some possible keywords based on the frequency of sensitive words for this room. To reduce the computation overhead, only fuzzy matching is conducted in analyzing of Danmaku. The system selects key words from Danmaku streams, and then match them with the words in a keyword table. Provided that it matches, the room number and the information of the Danmaku sender will be displayed on the alter screen of monitoring system.

We use a customized KMP algorithm to implement the sensitive Danmaku message fuzzy matching. KMP is a string-matching algorithm with high efficiency and agile implementation. Additionally, this algorithm costs the shortest time, compared with algorithms of the same type. KMP algorithm makes full use of the information contained in a specific pattern, and to obtain a prefix module by preprocessing this pattern. This algorithm performs more efficiently than traditional ones.

KMP algorithm to fuzzy match the information of Danmaku can find out similar words and phrases related to keywords (for example, the keyword is "shit". If there exist "sh.. it*, s... hit, shi... ttttttt" in the Danmaku stream that are similar to the key words, they will be identified.) Besides, it can also find out some representatives or typical keywords which are used by message senders who are incentive to avoid being detected. All of them can highly improve the efficiency and accuracy of detection. Also, the match method transforms Chinese characters to pinyin. Consequently, they can match with each other without being the same intonation. This match improves the traditional way, such as char-pattern matching and calling library, by exalting both matching speed and accuracy. The proposed method is given in Algorithm 2 and Algorithm 3 as follows:

4.3. State Sensing and Analysis on Frame Difference

This method is achieved through the following steps. First, we capture live video stream address from live URL, and then set a time interval T. After that, we call ffmpeg command to obtain screen-shots of the video within the

Algorithm 2: Sensitive words perception based on fuzzy matching

Input: living platform's target url
Output: unusually $roomid_i$
Data:
$X \leftarrow threshold$
$n \leftarrow$ living platform's room number
$K \leftarrow$ the rate of change of all people

```
build danmu library Including counter-terrorism,cults,etc.
for i ← 1 to n do
    danmu stream ←(get)— link danmu server
    if danmu string s1 is not NULL then
        string t1 ←(pinyin)— string s1
        if fuzzy-matching(t1) is TRUE then
            output unusual roomid_i
        else
            continue
        end
    else
        continue
    end
end
```

Algorithm 3: fuzzy-matching(t1) module

Input: *text*, *pattern*
Output: 0 or 1

```
1  j ← 0
2  k ← 0
3  for i ← 1 to n do
4  |   while j and p[j]!=t[i] do
5  |   |   j=f[j]
6  |   end
7  |   if p[j] == t[i] then
8  |   |   j++
9  |   end
10 |   if j==m then
11 |   |   k++
12 |   end
13 end
14 return k
```

same time interval. Subsequently, we name the screen-shots according to a special naming rules and save it to the local disk. We tailored design perception of hash perceptual [26, 27] algorithm to calculate similarity between consecutive screen-shots. When the live room id is altered when the similarity gaps is sufficiently large, the monitor system guides attentions to the live room with lower similarity. The low similarity implies that room state changes remarkably, and the supervisor will be notified to check the reason for the change.

The scene segmentation technique is depicted in Fig. 4.

The proposed system detects that scene changes in room 1 at time t1, and no changes at room 2 and room 3. At time t2, the scene of room 1 and room 2 changes; that of room 3 did not change. room 1 at t1 thus needs more attentions, likewise are room 1 and room 2 at t2. We divide the live stream scene via adjacent frame differences. Image perceptual hashing algorithm is implemented for state perception analysis onto frame difference, which relies on information processing theory from cognitive psychology. A mapping is created from multi-media data set to multi-media perception set, which satisfies the demand for perception security. The revised algorithm

calculates the similarity between consecutive image that feeds to perception hash algorithm, which has multiple advances such as robustness, discrimination, collision resistance and unidirectionality. The details are presented in Algorithm 4.

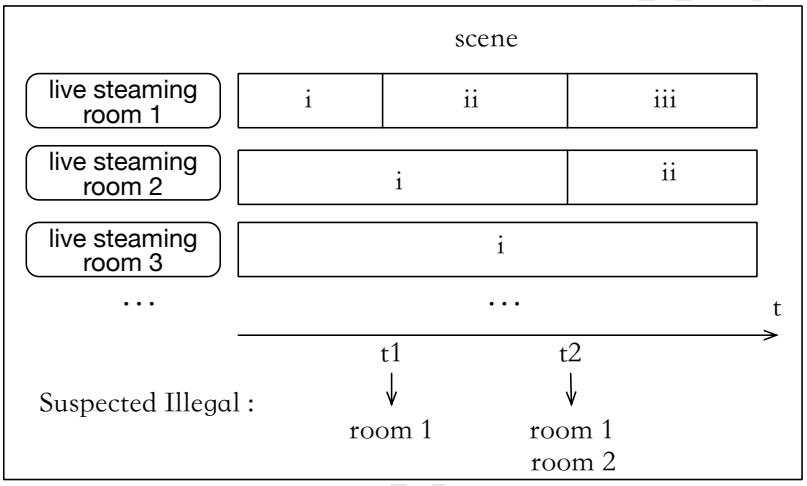

Figure 4: Traffic monitoring framework

We compute two-dimensional Discrete Cosine Transformation (DCT) in perceptual hashing algorithm[24, 28], Dto explore frequencies and amplitudes for approximating an image. Two-dimensional DCT is divided into positive and inverse transform, and major operations are listed as follows:
1.Positive transformation:

$$F(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{P-1}\sum_{y=0}^{Q-1} f(x,y)cos\frac{u\pi x + \frac{1}{2}u\pi}{P}cos\frac{v\pi y + \frac{1}{2}v\pi}{Q}$$

$$u \in [0, P-1], v \in [0, Q-1]$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{P}}, & u = 0 \\ \sqrt{\frac{2}{P}}, & u \neq 0 \end{cases} \quad \alpha(v) = \begin{cases} \sqrt{\frac{1}{Q}}, & v = 0 \\ \sqrt{\frac{2}{Q}}, & v \neq 0 \end{cases}$$

2.Inverse transformation:

$$f(x,y) = \sum_{x=0}^{P-1}\sum_{y=0}^{Q-1} \alpha(u)\alpha(v)F(u,v)cos\frac{u\pi x + \frac{1}{2}u\pi}{P}cos\frac{v\pi y + \frac{1}{2}v\pi}{Q}$$

Algorithm 4: State sensing and analysis on frame difference of live platform

Input: living platform's target url
Output: unusually $roomid_i$
Data:
$Y \leftarrow$ similarity threshold
$n \leftarrow$ living platform's room number

```
for i ← 1 to n do
    build ffmpeg command
    save 1.bat
    run 1.bat
    get roomid_t.bmp
    if roomid_t-1.bmp is exit then
        y ← calculate the similarity
        if y < Y then
            output unusual roomid_i
        else
            continue
        end
    else
        continue
    end
end
```

$$u \in [0, P-1], v \in [0, Q-1]$$

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{P}}, & u = 0 \\ \sqrt{\frac{2}{P}}, & u \neq 0 \end{cases} \quad \alpha(v) = \begin{cases} \sqrt{\frac{1}{Q}}, & v = 0 \\ \sqrt{\frac{2}{Q}}, & v \neq 0 \end{cases}$$

5. Experiment and Performance Evaluation

The system relies on the harmonic cooperation of three components - abnormal traffic detection, sensitive words perception based on fuzzy matching, and perception state analysis on frame difference. Accordingly, in order to show the efficiency of the system, we first test these three parts separately, and then conduct an overall study. We evaluate multiple performances in

real experiments. From Sept. 20 to Sept. 27th, we have tested more than 100 rooms in Panda.Tv for 7 days. We chose this live platform because it is one of the biggest live streaming platform in China, and we can easily get the detail information of the site. All the following experiments are conducted by Java over PC with Intel Core i5 wit 2.50GHz processor and 4GB memory.

1) Abnormal traffic detection.

It finds the suspected illegal rooms by the rate of traffic changes, which is reflected by the changing rate of viewer number in the room. Our experiment evaluates two folders: all rooms with abnormal traffic could be detected; how many detected rooms are really suspected illegal. The details are given in the following.

First, we test whether all rooms with abnormal traffics could be detected by the system. For each 10 minutes, our system fetches the number of viewers in each room, and calculates the changing rate of number in adjacent intervals for each room. The system records the results in a log file, including threshold, links of each room, on-line numbers of each room, and changing rate of viewer number in adjacent intervals for each room. The results are shown in Fig. 5. It is easy to check whether rooms with abnormal traffics can be detected by the system. As shown in the figure, our system will focus on room 352783 at 10 minutes, and room 13653 at 100 minutes.

Secondly, we check the rooms that are detected by the system to verify whether they are really suspected illegal. It can be done by opening windows of these rooms manually. During our experiments, there are 69 rooms with abnormal traffic detected by the system, and 32 of them are really suspected illegal. Observing from experiments, we find that if a room contains sensitive words, such as relating to pornography, the number of viewer will sharply increase, which influences on traffics. This again justifies that abnormal traffics can serve as a reference for the detection of suspected illegal rooms.

2) Sensitive words perception.

This part detects suspected illegal rooms via Danmaku. The sensitive words in Danmaku streams include following categories: terrorism, racial discrimination, religion, pornography, dirty words, and so on. If Danmaku contains sensitive words, the room might be suspected illegal. A library of sensitive words is constructed. In testing of this module, Danmaku of each room is monitored. If Danmaku in a room contains sensitive words, related records will be dumped in a log file. We then check that in these rooms how many are really suspected illegal. In detection, 102 rooms are found sensitive words, of which 45 are really suspected illegal rooms. In the experiments,

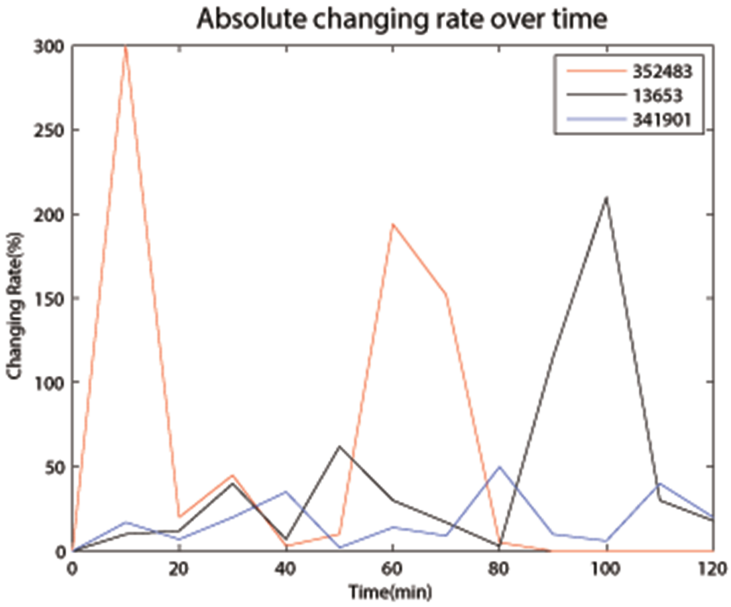

Figure 5: Log file for traffic monitoring results

we found that Danmaku is a indicator of interaction hotness between the viewers and the host. The number of Danmaku is related to contents and the number of viewers. Therefore, sensitive words can be used as a reference for suspected illegal rooms detection.

3) State of perception and analysis on live frame difference.

Frame difference can be applied to scene segmentation. By capturing moving objects in the same intervals, and analyzing the image sequence of adjacent frames, we can detect those rooms where the frame differences change rapidly once it is larger than the threshold. These rooms are very likely suspected illegal rooms, thus we could use it as an indictor.

To test this module, we capture screen-shots of each room in every 10 seconds and calculate the frame difference of adjacent intervals for each room. If the difference in the frame is above the threshold, our system will alter the room id. We take room 329279 in panda.tv as an example. This room is detected by abnormal traffic, and it is often recommended on the web site. The changes of frame difference are shown in Fig. 6. Fig. 7 presents the adjacent screen-shots of room 329279. The experiment result again justifies that state perception and analysis on frame difference can serve as an

indicator for suspected illegal room detection.

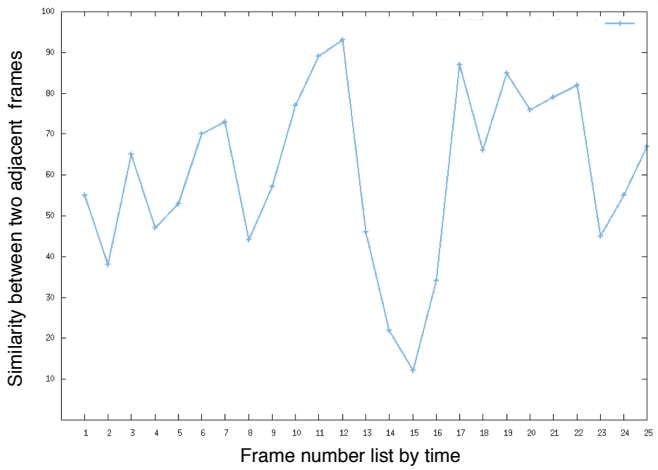

Figure 6: The changes of frame difference of Room 329279

Figure 7: The screen-shots of Room 329279 - 18 frames to 22 frames

4)comprehensive analysis

Based on the aforementioned three detection method, we detects live streaming rooms in Panda.tv. We select those suspected illegal rooms from output rooms by manual detection, then record data in Table 1 as follows:

Extensive experiment analysis shows that above three proposed methods are important indirect indicators for detecting suspected illegal rooms, and our system comprehensively considers them all for optimized efficiency and accuracy.

Table 1: Our system detection results(live streaming room in Panda.tv)

Detection Indicator	Output Room Number	Suspected Illegal Rooms	Accuracy
Abnormal traffic detection	69	22	31.8%
Sensitive words perception	102	45	44.1%
State of perception and analysis	257	76	29.6%
Union Three Indicator	43	39	90.1%

6. Conclusion and future works

In this paper, we proposed a realtime intelligent monitoring system for live video streaming platform based on indirect indicators such as state awareness and frame difference analysis. The proposed scheme includes abnormal traffic in terms of changing rate of room viewers, sensitive words filtering in Danmaku, and perception frame difference analysis. We test our system in real platform Panda.tv. We also record the number of suspected illegal live streaming, which is selected by manual detection (positive value). As a result, our system alerts 43 room id that detected by three indirect proposed factors, and 39 of them are really suspected illegal, and the integrated accuracy of the three modules reaches 90.1%. The experiments shows that our proposed methods are greatly reduces the working load of content managements of live streaming platforms, in which most of them rely on manually monitoring.

Acknowledgement

The research was financially supported by the Open Funding of Guizhou Provincial Key Laboratory of Public Big Data with No. 2017BDKFJJ006, National Science Foundation China 61502362, and Open Funding of Hubei Provincial Key Laboratory of Intelligent Geo-Information Processing with No. KLIGIP2016A05.

References

[1] J. Peng, S. Detchon, K.-K.R. Choo, H. Ashman, Astroturfing detection in social media: a binary n-gram-based approach, *Concurrency and Computation: Practice and Experience.29(17)(2016).*

[2] A. Heravi, D. Mani, K.-K.R. Choo, S. Mubarak, Making Decisions about Self-Disclosure in Online Social Networks, *In Proceedings of 50th Annual Hawaii International Conference on System Sciences. (2017).*

[3] D. Quick, K.-K.R. Choo, Pervasive social networking forensics:Intelligence and evidence from mobile device extracts, *Network and Computer Applications.86(2017)24-33.*

[4] C.-D. Orazio, K.-K.R. Choo, An adversary model to evaluate DRM protection of video contents on iOS devices, *Computers Security.56(2016)94-110.*

[5] S.A. Miraftabzadeh , P. Rad, K.-K.R Choo, M.A. Jamshidi, Privacy-Aware Architecture at the Edge for Autonomous Real-Time Identity Re-Identification in Crowds, *IEEE Internet of Things Journal.(2017).*

[6] P.F. Felzenszwalb, D.P. Huttenlocher, Efficient graph-based image segmentation, *International Journal of Computer Vision.47(2004)167-181.*

[7] J. Steiner, S. Zollmann, G. Reitmayr, Incremental superpixels for real-time video analysis[C], *Proceedings of the Computer Vision Winter Workshop.(2011).*

[8] Y. Wang, T. Zhang, D. Tretter, Real time motion analysis toward semantic understanding of video content, *Conference on Visual Communications and Image Processing.(2005).*

[9] P.Ramyaa, R.Rajeswarib, A Modified frame difference method using correlation coefficient for background subtraction, *Procedia Computer Science.93(2016)478-485.*

[10] S. Kamate, N. Yilmazer, Application of Object Detection and Tracking Techniques for Unmanned Aerial Vehicles, *Procedia Computer Science.61(2015)436-441.*

[11] G.-S. Sarma, V.-S. Kumar, S.Nizmi, Image Processing - A Gizmo for Video Content Extraction, *ARPN Journal of Systems and Software.(2011).*

[12] M. Jiang, J. Kong , H. Huo, Informative jointsbasedhuman-actionrecognition using skeletoncontexts, *Signal Processing: Image Communication.33(2015)29-40.*

[13] W. Xiong, H. Hua, N. Xiong, L.-T. Yang, W.-C. Peng, X.-F. Wang, Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications, *Information Sciences.258(2014)403-415.*

[14] V.-S.W. Eide, O.C. Granmo, F. Eliassen, Real-time video content analysis: QoS-aware application composition and parallel processing, *ACM Transactions on Multimedia Computing, Communications, and Applications.2(2)(2006)149-172.*

[15] M.S. Kim , H.J. Kong, S.C. Hong, A flow-based method for abnormal network traffic detection, *Network operations and management symposium.1(2004)599-612.*

[16] Z. Xia, S. Lu, J. Li, Real-Time and Self-adaptive Method for Abnormal Traffic Detection Based on Self-similarity, *International Conference on Web Information Systems and Mining. Springer Berlin Heidelberg.(2009)383-392.*

[17] Y. Chen, Q. Gao, P.-L.P.Rau, Watching a Movie Alone yet Together: Understanding Reasons for Watching Danmaku Videos, *International Journal of Human-omputer Interaction.(2017).*

[18] W. Ren, S. Huang, Y. Ren, K.-K.R. Choo, Lipisc: a lightweight and flexible method for privacy-aware intersection set computation, *APlos One.11(6)(2016).*

[19] W. Ren, R. Liu, M. Lei, K.-K.R. Choo, Segoac: a tree-based model for self-defined, proxy-enabled and group-oriented access control in mobile cloud computing, *Comput Stand Interfaces.54(2016)29-35.*

[20] X.-H. Jin, X. Hui, W. Yang, Q.-J. Liu, D. Zhao, S. Xu, Improved Moving Target Detection Technology, *Advanced Materials Research.(2014).*

[21] H. Liu, H. Kun, J.-L. Dai, R. Wang, H.-Y. Zheng, B. Zheng, Combining background subtraction and three-frame difference to detect moving object from underwater video, *OCEANS.(2016).*

[22] Y.-H. Miao, L.-Z. Wang, D.-S. Liu, Y. Ma, W.-F. Zhang, L.-J. Chen, A Web 2.0-based science gateway for massive remote sensing image processing, *Concurrency and Computation: Practice and Experience.27(9)(2015)2489-2501.*

[23] L.-Z. Wang, Y. Ma, J.-N. Yan, V. Chang, A.-Y. Zomaya, pipsCloud: High performance cloud computing for remote sensing big data management and processing, *Future Generation Computer Systems.78(2018)353-368.*

[24] L.-Z. Wang, W.-J. Song, P. Liu, Link the remote sensing big data to the image features via wavelet transformation, *Cluster Computing.19(2)(2016)793-810.*

[25] Y. Liu, Y. Zhao, M. Liu, L. Dong, Y. Wu, Research on the algorithm of infrared target detection based on the frame difference and background subtraction method, *Signal and Data Processing of Small Targets.(2015).*

[26] N. Saikia, P.-K. Bora , Perceptual hash function for scalable video[J]. International journal of information security, *Journal of Real-Time Image Processing13(1)(2014)81-93.*

[27] L. Weng, B. Preneel, A secure perceptual hash algorithm for image content authentication, *IFIP International Conference on Communications and Multimedia Security. Springer Berlin Heidelberg.(2011)108-121.*

[28] Q.-W. Zhang, W.-X. Du, L.-Q. Yuan, M. Li, Face Recognition Using Discrete Cosine Transform and Fuzzy Linear Discriminant Analysis, *Communications in Computer and Information Science.(2011).*

Yangfan Li is a student at School of Computer Science, China University of Geosciences, Wuhan. His research interests include information security and image processing.

Wei Ren currently is a Professor in School of Computer Science, China University of Geosciences (Wuhan), China. He was with Illinois Institute of Technology, USA in 2007 and 2008, School of Computer Science, University of Nevada Las Vegas, USA in 2006 and 2007, and Hong Kong University of Science and Technology, in 2004 and 2005. He obtained his Ph.D. degree in Computer Science from Huazhong University of Science and Technology, China. He published more than 70 refereed papers, 1 monograph, and 4 textbooks. He obtained 10 patents and 5 innovation awards. He is a senior member of China Computer Federation

Tianqing Zhu received her B.Eng. and M.Eng. degrees from Wuhan University, China, in 2000 and 2004, respectively, and a Ph.D. degree from Deakin University in Computer Science, Australia, in 2014. Dr. Tianqing Zhu is currently a continuing Teaching Scholar in the School of Information Technology, Deakin University, Australia. Her research interests include privacy preserving, data mining and network security. She has won the best student paper award in PAKDD 2014.

Yi Ren obtained his Ph.D. in Information Communication and Technology from the University of Agder, Norway in 2012. He was with the Department of Computer Science, National Chiao Tung University (NCTU), Hsinchu, Taiwan, as a Postdoctoral Fellow and an Assistant Research Fellow from 2012 to 2017. He is currently a Lecturer in the School of Computer Science at University of East Anglia (UEA), Norwich, U.K. His current research interests include security and performance analysis in wireless sensor networks, ad hoc, and mesh networks, LTE, and e-health security. He received the Best Paper Award in IEEE MDM 2012.

Yue Qin is a student at School of Computer Science, China University of Geosciences, Wuhan. Her research interests include mobile security and authentication of mobile devices.

Wei Jie has been active in a broad spectrum of areas in parallel and distributed computing, in particular, grid and cloud computing, computing security technologies, e-science and e-research. Dr Jie has been actively involved in professional services. He is the General Chair of the IEEE workshop on Security in e-Science and e-Research, and has served as Program Committee member for more than 40 international conferences and workshops. He has published approximately 50 papers in international journal and conferences and has edited three books.

This paper focus on the content security of live streaming platform. In this paper, we propose a new method to monitor real-time live stream and identify illegal live videos intelligently based on state of perception and frame difference analysis. The proposed system makes use of several indirect factors of the chatting room status rather than analyzing images directly. The application of this system can change the situation where the live platform supervision totally depends on manual review. This system can be widely employed in many areas, such as live broadcast platform companies, state security department, and the national security of counter-terrorism department.