Accurate Identification of Internet Video Traffic Using Byte Code Distribution Features

Yuxi Xie, Hanbo Deng, Lizhi Peng(✉), and Zhenxiang Chen

Shandong Provincial Key Laboratory of Network Based Intelligent Computing, University of Jinan, Jinan 250022, People's Republic of China
plz@ujn.edu.cn

Abstract. Video traffic, the most rapidly growing traffic type in Internet, is posing a serious challenge to Internet management. Different kinds of Internet video contents, including illegal and adult contents, make it necessary to manage different video traffic using different strategies. Unfortunately, there are few research work concerning Internet video traffic type identification. In this paper, we propose a new effective feature extraction method, namely byte code distribution (BCD), for Internet video traffic type identification. The BCD method first counts the times of each byte code value (0 to 255) from a video flow, and then computes the ratio between each count and the total byte count. Such that the 256 ratios are used as the features. Comparing with traditional packet-level features, the BCD features contain more video type information, and are able to make identification more accurately. To test the performance of our proposal, we collect a set of video traffic traces containing two typical video types, romance and action. We conduct a set of comparing experiments on the collected data. The results show that the BCD method can hit extremely high identification accuracies (higher than 99%), far higher than those of the traditional packet-level feature extracting methods. The empirical studies show that the BCD method is promising for Internet video traffic identification.

Keywords: Byte code distribution · Feature extraction
Video traffic identification · Machine learning

1 Introduction

Recent years, Internet has witnessed an explosion of video traffic. According to Cisco's report [1], 82% Internet traffic is generated by video applications. Rapidly emerged video contents greatly enhance Internet users experiences while impose heavy burden on Internet. At the same time, lots of abnormal videos, such as pornographic and violent videos, are widely spread on the Internet. Such videos carry high risks for both of the security and the mental health of Internet users. Therefore, how to effectively identify and manage Internet video

J. Vaidya and J. Li (Eds.): ICA3PP 2018, LNCS 11334, pp. 46–58, 2018.
https://doi.org/10.1007/978-3-030-05051-1_4

traffic has become an urgent problem to be resolved. Video content analysis is an important research topic in computer vision area [18]. Generally, such researches first extract key frames from the original videos. Then, global image features and local object features, such as image colors, textures, and shapes are extracted to identify the video contents [11]. Most video content analysis methods process static and complete data. That is to say, such methods analyze video contents using complete video or image data, leading to poor real-time processing ability. Additionally, on the Internet, real time video streams make it difficult to collect complete image or video data on network devices. Therefore, from the view point of engineering, it is infeasible to apply traditional video content analysis techniques to Internet video traffic identification. Internet traffic identification research provides a possible solution for this problem. In fact, observing the video stream packets on a network device, and extracting features on the packet level or the flow level, and identifying the video content types using these features, such a process is a typical traffic identification process. Unfortunately, as far as we know, there are so few researchers concern on this problem. Most research work related to Internet video traffic was carried out to identify whether a network flow is a video flow or not [4,10], but not the video traffic content type. Schuster et al. [17] made a preliminary attempt for Internet video traffic content type identification in 2017. They use the burst pattern, together with other traditional packet level features, e.g. packet length, and byte rate, to identify the video streams. Their experimental results show that both of the traditional packet level features and the burst pattern feature can hit accuracies higher than 90% for most cases. However, in this research, the video content level features were completely ignored, in contrast of the emphasis of the packet level features, resulting the low identification accuracies for some cases. Therefore, to explore more complex and effective features, and build accurate identification models is the feasible way for Internet video traffic identification.

To address this problem, in this paper, we set out to find content related Internet video traffic features, which can be applied to identify video traffic accurately. Such features should be extracted from video flows efficiently. Driven by this motivation, we make the following contributions in this paper:

- We first collect a set of video traffic data in a real campus network environment, which contain romance and action types. Different from the work in [17], we use the video content types as the instance labels. We consider romance and action videos in our study, as they are the most two representative Internet video types.
- A video content related feature extraction method, namely "Byte code distributions(BCD)", is proposed. We first extract the byte codes of each video flow, and then calculate the occurrence frequency of each code based on the observation of the flow. The observation can be the early section or any fraction of the video flow. Finally, all the byte code frequencies form a vector, that is the feature vector. BCD features can be efficiently extracted from video traffic data. Moreover, they contains more information of different video types than traditional packet level features do.

To test the performances of our proposal, a set of empirical studies are conducted. Three typical supervised learning algorithms are applied for the identification in our studies, they are C4.5 decision trees, support vector machine (SVM), and BP neural networks (BPNN). The experimental results show that video flow BCD features are extremely effective for the identification of the romance and action movies. Our method hits a high identification accuracy of 99.9%, significantly higher than those of using the traditional packet level features. Empirical studies show that our proposal is promising for Internet video content type identification.

The rest of the paper is organized as follows. In Sect. 2, we review the related work. Section 3 introduces our study framework. Section 4 gives the technical details of our data collection method and the data set. The feature extraction and identification methods are presented in Sect. 5. The experimental evaluation details, including the settings, the results, and the analysis are given in Sect. 6. Finally, we conclude the paper in Sect. 7.

2 Related Work

2.1 Network Traffic Identification

From the technical view point, network traffic identification methods fall into three categories: port-based identification, deep packet inspection (DPI), and machine learning (ML) based identification. Port-based identification, the most antique network traffic identification method, simply identifies the application layer protocol types by the source/destination port number of a TCP or UDP flow. DPI techniques are able to achieve extremely high identification accuracies under the conditions that the packet payloads can be inspected. However, these techniques have two fatal drawbacks: firstly, they cannot cope with encrypted traffic; secondly, these techniques are not able to be deployed in high-speed networks because of their high computation and storage costs.

Machine learning based methods, with fine generalization and intelligent capabilities, have become the dominant methods for traffic identification. Generally, ML-based methods extract traffic features from the packet level, flow level, or session level, and then use a set of labeled feature data to train a ML model. Finally, the trained ML model is applied to predict unknown traffic instances. Feature extraction is the basic and vital step for ML-based methods. Moore et al. [9] use 248 statistical features to describe the flow, such as the length of flow duration, packet arrival time interval and packet size, etc. Peng et al. [12] studied effectiveness of statistical features for early stage Internet traffic identification. By using statistical packet and flow level features, different machine learning techniques, including supervised machine learning [3,19], unsupervised machine learning [15], and semi-supervised machine learning [21] were widely applied for traffic identification.

Gong et al. [6] proposed an improved incremental SVM learning algorithm to identify P2P traffic. Preprocessed incremental data and trained SVM model are brought into incremental learning algorithm to obtain a new prediction model.

Qiao et al. [14] proposed a method using the time window to generate simple and effective features from the header of the network stream packets. Zhang et al. [22] introduced a new scheme of Robust statistical Traffic Classification (RTC) by combining random forest and k-means to address the problem of zero-day applications. Peng et al. [13] used IDGC model to identify imbalanced traffic.

The above methods about network traffic identification is identification of application type instead of the type of video. The granularity of recognition is coarser.

2.2 Video Content Identification

In fact, a lot of research work have been done to identify video content using computer vision techniques. However, most of these methods process static and complete data, which leads to poor real time processing ability. Yuan et al. [20] proposed a new method that using a hierarchical Support Vector Machines to distinguish the different video genres based on ten computable spatio-temporal features. Rasheed and Shah [16] put forward that through the visual disturbance feature and average shot length of every movie, the movie genre has been successfully classified. A transductive learning framework for robust video content analysis based on feature selection and ensemble classification was presented by Ewerth et al. [5]. Liu et al. [8] proposed a method that applying a (wavelet-based) analysis to extract the long and short range dependencies within the video traffic for generation of the robust and efficient traffic fingerprint. Chaisorn et al. [2] presented a hybrid signature along with a hierarchical filtering approach for similar content identification. Li et al. [7] proposed to extract robust video descriptor by training deep neural network to automatically capture the intrinsic visual characteristics of digital video.

In terms of video traffic recognition, a consistency-based feature analysis and selection method was presented by Dong et al. [4] to systematically find some new and effective features for video traffic classification. And a hierarchical k-Nearest Neighbor (KNN) classification algorithm is then developed based on the combinations of these statistical features. Mu et al. [10] studied a parallel network flow classification method based on Markov's model. These small amounts of research just identify the traffic generated by video applications in numerous network traffic. In terms of Internet video content recognition, the method presented by Israeli scholars have opened the door to identify the content and types of the video at the traffic level. A relatively good results have been obtained through the burst pattern feature of data packets and the methods of convolution neural network in their work. More specifically, the identified object is the title of the video.

3 Study Framework

The study framework of this paper contains three main stages: data collection, feature extraction, and classification.

Firstly, raw video traffic data is captured and stored in the server. Then a set of preprocessing steps, e.g. noise data filtering and TCP flow converging, are conducted on the raw data. As most Internet video streams are transmitted using the TCP protocol, we only consider TCP flows in our study. After the preprocessing operations, a processed original video traffic data set is generated.

At the second stage, a set of video traffic feature extraction studies are carried out. There are two main steps in this stage. First, three types of packet sampling operations are executed on the original video traffic data, including early stage sampling, fraction sampling, and regular interval sampling. The reason of applying sampling operations is easy to be understood: it makes non sense in real scenarios to extract feature data on a complete flow. Second, we extract BCD features as the video content features based on the sampled packets. The extracted feature data forms the feature data set, which can used for the training and testing of the machine learning models. In addition to the BCD features, we also extracted two traditional packet level features, packet size and packet inter-arrival time, for comparisons.

Finally, we applied three classical machine learning models, C4.5, SVM, and BPNN for the identification and validation of the extracted features. It should noticed that we do not care the machine learning models. Instead, we focus on the applying of these machine learning models on our video traffic data. That means we can choose the most effective learning model for the real video traffic identification problem according to the evaluation results.

4 Data Collection and Preprocessing

4.1 Data Collection

The data collection test bed is deployed in our campus network environment, which is shown in Fig. 1. We deployed seven user computers as the collection clients. Each client computer equips two Intel Pentium G620 CPUs, and runs Windows 7. We deploy the Wireshark packet capturing tool on the client computers to collect the raw video traffic data. The collected data are then sent to a centralized server, and preprocessed on the server.

In this study, two typical video content types are considered, romance and action. During October 2017 to March 2018, the users of the client computers visited Internet video sites and played the two types of videos from time to time. When a client computer was playing target videos, all other network applications were stopped to avoid generating non-video traffic, and the Wireshark tool was started for capturing. Many Internet videos begin with advertisement videos, which were manually skipped in our studies.

The Internet video sites we visited cover Youku, Tudou, iQIYI, Sohu video, and Tencent video. For each video site, we selected 100 romance movies and 100 action movies. The first 15 min of each movie were played and its packets were captured. Considering the storage limitation, we did not collect the complete video of each movie. In fact, we consider that the 15 min section is enough to contain the unique network characters of an Internet video. Table 1 shows the details of the collected video traffic data.

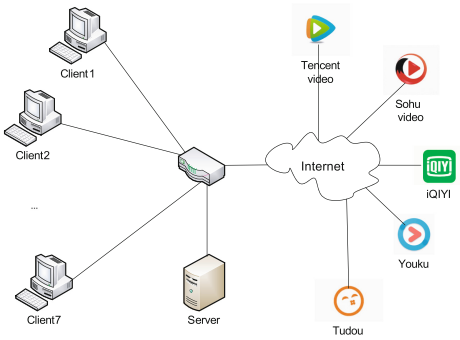

Fig. 1. The architecture of data collection

Table 1. Collected video traffic data

Video site	Video type	# instances	# bytes (GB)
Youku	Romance	100	2.3
	Action	100	5.1
Tudou	Romance	100	1.9
	Action	100	4.9
iQIYI	Romance	100	2.1
	Action	100	4.9
Sohu video	Romance	100	1.8
	Action	100	4.8
Tencent video	Romance	100	2.2
	Action	100	5.2

4.2 Data Preprocessing

The raw data is saved in standard .pcap format files. As most Internet video sites using the TCP protocol for video stream transmission, we first picked up all TCP packets in the preprocessing operations. Then all the packets were converged into distinguished TCP flows (connections). In some TCP flows, the SYN packet, or the FIN packet, or RST packet are missed, because we just captured the first 15 min of each movie instance. Therefore, we use the timeout strategy to determine the beginning and ending of the incomplete TCP flows. In addition, flows that contain less than 1000 packets were discarded. The underlying fact is that such "short" flows are usually generated by background applications, and should be filtered as noise data.

5 Feature Extraction

It is well known that feature extraction is vital for machine learning tasks, as the learning results greatly depend on the qualities of the extracted features.

In traffic identification researches, packet-level and flow-level features are widely used, such as packet size, packet inter-arrival time, up/down byte rate, up/down byte volume, etc. Such features perform well in general traffic identification tasks. However, for video traffic identification, traditional packet-level and flow-level features that are just statistical features at the network level, not at the content level obviously cannot reveal the differences of different video content types. On the other hand, as stated in Sect. 1, it is very hard to extract computer vision features from the living video streams on networks. They analyze and process the complete video file while we analyze and process the data packet. In comparison, our method is more convenient and real-time. Therefore, we propose fast video traffic feature extraction method using the BCD features of packet payloads, which will be introduced in details in Subsect. 5.1. We also use two basic packet-level features, packet size and packet inter-arrival time, in our study for comparison.

5.1 Byte Code Feature

It can be easily and intuitively concluded that each video content type has its unique scene style. For example, romance movies have smooth and mild scenes, in contrast with the violent and fast-paced scenes of action movies. Similarly, different video content types also have different patterns for the sound, the emotional expression, and so forth. When the videos are packed into network packets, and transmitted on the network, such different patterns can be mapped to the byte coding styles of the network packets. If we observe these packets on the network, and extract the features with right ways, we can identify different video types by finding their unique patterns.

Let's observe a fraction of a video flow, for example 2 min. Suppose there are n packets in this fraction, all the packets in this fraction form a sequence $P_1, P_2, ..., P_n$. The payload size of the ith packet is S_i. If we extract each byte of the packet, and get its values (varying from 0 to 255), then all the byte values can be illustrated as Table 2. If we sum up the byte values of each row in the table, then we get 256 counts $c_1^i, c_2^i, ..., c_{256}^i$ for the ith packet. We conduct the counting procedure on each packet of the packet sequence $P_1, P_2, ..., P_n$, and get a count matrix

Table 2. Byte values of the ith packet

	$Byte1$	$Byte2$	...	$ByteS_i$
0	0	0	...	1
1	1	0	...	0
⋮	⋮	⋮	⋮	⋮
255	0	1	...	0

$$C = \begin{bmatrix} c_1^1 & c_2^1 & ... & c_{256}^1 \\ c_1^2 & c_2^2 & ... & c_{256}^2 \\ \vdots & \vdots & \vdots & \vdots \\ c_1^n & c_2^n & ... & c_{256}^n \end{bmatrix} \tag{1}$$

Finally, we sum up each column of this matrix, and get 256 count numbers. Then compute the proportion of the jth count number as follows.

$$f_j = \frac{\sum_{i=1}^{n} c_j^i}{\sum_{k=1}^{256} \sum_{i=1}^{n} c_k^i}, \ j = 1, 2, ..., 256. \tag{2}$$

So we get a vector containing 256 components $F = \{f_1, f_2, ..., f_{256}\}$. That is the feature vector.

It can be observed these features show the distributions of the 256 byte codes in the video flow fraction. Such simple statistical features have two significant advantages. First, these features can be easily extracted with low computation and storage costs. Second, such features depend on the contents of the original videos to some extent. That is to say, they can show the patterns of the original videos.

5.2 Feature Extraction Algorithm

Algorithm 1 describes the feature extracting procedure. In which the input is the preprocessed data set D. That is to say, in D, we have filtered the noise data and all the flows have been converged as illustrated in Sect. 4. We go through the whole data set, and compute a feature vector F containing 256 components for each video flow. Therefore, a feature data set is formed, and each instance is a video flow instance. Finally, the video type labels, 0 for romance and 1 for action, are added to each instance. This feature data set can be used for the training and testing of the learning models, which will be introduced in the next section.

Algorithm 1. BCD features extraction

Input: Preprocessed data set D;
Output: Feature data set FD(BCD features data set);

```
for each flow FLOW_k in D do
    Initialize the count matrix C using zero elements;
    for each packet P_i in FLOW_k do
        for each byte b_j in P_i do
            c^i_{b_j} ++;
        end for
    end for
    Compute the feature vector F_k according to Eq. (2);
    Add the video type label of the flow y_k to the end of F_k;
end for
```

6 Experiments

6.1 Performance Measures

We use accuracy and f-measure as the performance measures in our empirical evaluations. Without lose of generality, we consider binary classification tasks. For such tasks, the accuracy *acc* can be defined as follows.

$$acc = (TP + TN)/(TP + TN + FP + FN) \tag{3}$$

Where, true positive (TP) is the number of the correctly classified positive instances, true negative (TN) is the number of the correctly classified negative instances, false positive (FP) is the number of the negative instances those be incorrectly classified as positive ones, false negative (FN) is the number of the positive instances those be incorrectly classified as negative ones. Precision p and recall r are two typical measures, which are defined as:

$$p = TP/(TP + FP) \tag{4}$$

$$r = TP/(TP + FN) \tag{5}$$

Both precision and recall are able to show the prediction performance of a learning model from different points. F-measure, the harmonic mean of precision and recall, is a complicated measure which is defined as follows.

$$F - measure = (2 * r * p)/(r + p) \tag{6}$$

6.2 Classifier Parameter Settings

Three classification algorithms are used to classify the feature data sets in our experiments. Including C4.5 decision trees, SVM and BPNN. Table 3 shows the parameter settings of the classifiers.

Table 3. Classifier parameter settings

C4.5	SVM	BPNN
confidenceFactor:0.25	kernel function:linear	Transfer function of ith layer
minNumObj:2	method:SMO	hidden layers:'tansig' 'logsig'
seed:1	polyorder:3	output layer:'purelin'
splitCriterion:IGR	rbf sigma:1	training function:'traingd'
		learning function:'learngdm'
		number of iterations:15000
		learning rate:0.01

6.3 Results and analysis

Table 4 shows the accuracies and f-measures the three classifiers got using BCD features.

Table 4. Comparison of experimental results

	Accuracy	F-measure
C4.5	0.9992	0.9992
SVM	0.9950	0.9950
BPNN	0.9942	0.9942

As can be seen from the results, all the three classifiers output extremely high values (higher than 99%) for both of accuracy and f-measure. These results strongly imply that the BCD features are really effective for video traffic type identification.

Comparisons Between Packet-Level Features and BCD Features. To further validate the effectiveness of the BCD features, we carry out a set of comparing experiments between the packet-level features and the BCD features. This time, we extract the packet sizes and IATs of the original video flow, and then use C4.5, SVM and BPNN for the identification. Finally, the results are compared with those of the BCD features, as Figs. 2 and 3 show. The significant differences between the results of the BCD features and the results of the two types of packet-level features can be easily observed. For both of accuracy and f-measure, all the three selected learning models output result values no more than 0.9, far lower than the high values of the BCD features. The comparison results strongly suggests the BCD features are far more effective than the traditional packet-level features in video traffic identification.

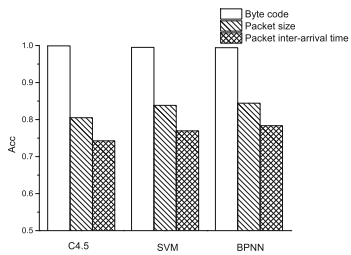

Fig. 2. Comparison results of accuracy

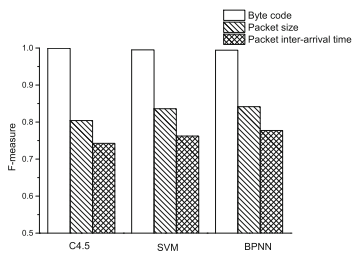

Fig. 3. Comparison results of F-measure

Identification Results of the Sampled Data. We use three packet sampling strategies to validate the real application effectiveness of the BCD features. First, we randomly select a 10 min fraction from each video flow for the feature extraction, and we call such strategy as the fraction sampling. For the second strategy, we select the packets in the first 2 s of each flow to extract the features, and we call it as early stage sampling. The third sampling method, namely regular interval sampling, selects the packets of each video flow every 3 s. We then extract the BCD features from the sampled video data, and put the feature data into C4.5, SVM and BPNN for identifications. Again, we use histograms to show the identification results, as shown in Figs. 4 and 5.

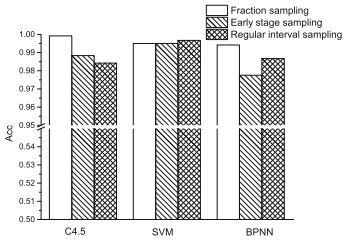

Fig. 4. Results of classification accuracy

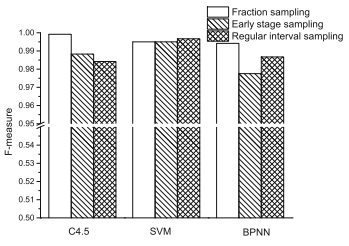

Fig. 5. Results of classification F-maesure

As can be seen from the results in Figs. 4 and 5, all the three packet sampling strategies can get high classification performance. Most of the result values of the three learning models are higher than 0.98. The differences between them are negligible. In other words, the two video types can be accurately identified using both the stream's early features and equal interval sampling features. Regarding these results, two conclusions can be drawn. First, the BCD features are proved to be effective for either the complete traffic data or the sampled data. Second, it is possible to accurately identify video content types in real network traffic environment.

7 Conclusions

We propose a new effective feature extraction method for Internet video traffic type identification in this paper, which computes the BCD of the packets of the target video traffic. Comparing with the traditional packet-level feature extraction methods, our proposal is able to get more accurate discrimination information of different video types. Consequently, our features work more effective than the traditional packet-level features for video traffic identifications. We conducted our proposal on a real collected video traffic data, using three classic machine learning algorithms. The experimental results provide empirical evidences that the BCD features are able to get extremely high identification performance, which are far higher than that of the traditional packet-level features. Our experimental results also show that the BCD features work well with

packet sampling techniques, which is important for high speed networks. However, we only investigated two typical types of videos: romance and action. In our future work, more video traffic types should be studied, and that will be a big challenge.

Acknowledgement. This research was partially supported by the National Natural Science Foundation of China under grant No. 61472164, No. 61573166, No. 61572230, and No. 61672262, the Doctoral Fund of University of Jinan under grant No. XBS1623, and No. XBS1523.

References

1. Baranyi, P.: Visual network index (VNI) complete prediction. https://www.cisco.com/c/zh_cn/solutions/service-provider/visual-networking-index-vni/index.html
2. Chaisorn, L., Fu, Z.: A hybrid approach for image/video content representation and identification. In: Industrial Electronics and Applications, pp. 966–971 (2012)
3. Dong, S., Li, R.: Traffic identification method based on multiple probabilistic neural network model. Neural Comput. Appl. **1**, 1–15 (2017)
4. Dong, Y.N., Zhao, J.J., Jin, J.: Novel feature selection and classification of internet video traffic based on a hierarchical scheme. Comput. Netw. **119**, 102–111 (2017)
5. Ewerth, R., Mühling, M., Freisleben, B.: Robust video content analysis via transductive learning. ACM Trans. Intell. Syst. Technol. (TIST) **3**(3), 41 (2012)
6. Gong, J., Wang, W., Wang, P., Sun, Z.: P2P traffic identification method based on an improvement incremental SVM learning algorithm. In: International Symposium on Wireless Personal Multimedia Communications, pp. 174–179 (2015)
7. Li, Y.N., Chen, X.P.: Robust and compact video descriptor learned by deep neural network. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 2162–2166 (2017)
8. Liu, Y., Sadeghi, A.R., Ghosal, D., Mukherjee, B.: Video streaming forensic-content identification with traffic snooping. Asian J. Agric. Rural Dev. **2**(10), 39–45 (2010)
9. Moore, A.W., Zuev, D.: Discriminators for Use in Flow-Based Classification. Intel Research, London (2005)
10. Mu, X., Wu, W.: A parallelized network traffic classification based on hidden markov model. In: International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 107–112 (2011)
11. Peng, L., Xue, Y., Wang, C.: Survey on recognition and filtering of network video content. Comput. Eng. Des. **10**, 048 (2008)
12. Peng, L., Yang, B., Chen, Y., Chen, Z.: Effectiveness of statistical features for early stage internet traffic identification. Int. J. Parallel Program. **44**(1), 181–197 (2016)
13. Peng, L., Zhang, H., Chen, Y., Yang, B.: Imbalanced traffic identification using an imbalanced data gravitation-based classification model. Comput. Commun. **102**(1), 177–189 (2017)
14. Qiao, M., Ma, Y., Bian, Y., Liu, J.: Real-time multi-application network traffic identification based on machine learning. In: International Symposium on Neural Networks, pp. 473–480 (2015)
15. Rao, Z., Niu, W., Zhang, X., Li, H.: Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Netw. Appl. **11**(3), 592–601 (2018)
16. Rasheed, Z., Shah, M.: Movie genre classification by exploiting audio-visual features of previews. In: Proceedings of the International Conference on Pattern Recognition, vol. 2, pp. 1086–1089 (2002)

17. Schuster, R., Shmatikov, V., Tromer, E.: Beauty and the burst: remote identification of encrypted video streams. In: Proceedings of the 26th USENIX Security Symposium, pp. 1357–1374 (2017)
18. Shinkar, T., Hanchate, D.B.: Video content identification using video signature: survey. Int. Res. J. Eng. Technol. (IRJET) **4**, 746–751 (2017)
19. Ye, Z., Wang, M., Wang, C., Xu, H.: P2P traffic identification using support vector machine and cuckoo search algorithm combined with particle swarm optimization algorithm. In: Zhang, S., Xu, K., Xu, M., Wu, J., Wu, C., Zhong, Y. (eds.) ICoC 2014. CCIS, vol. 502, pp. 118–132. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46826-5_10
20. Yuan, X., Lai, W., Mei, T., Hua, X.S., Wu, X.Q., Li, S.: Automatic video genre categorization using hierarchical SVM. In: IEEE International Conference on Image Processing, pp. 2905–2908 (2006)
21. Zhang, J., Chen, C., Xiang, Y., Zhou, W., Vasilakos, A.V.: An effective network traffic classification method with unknown flow detection. IEEE Trans. Netw. Serv. Manage. **10**(2), 133–147 (2013)
22. Zhang, J., Chen, X., Xiang, Y., Zhou, W., Wu, J.: Robust network traffic classification. IEEE/ACM Trans. Netw. **23**(4), 1257–1270 (2015)