TRAFFIC PATTERN-BASED CONTENT LEAKAGE DETECTION

[1] Chunarkar Nirosha
M.Tech(CSE)
SREE DATTHA INSTITUTE OF ENGINEERING & SCIENCES, Hyd

[2] L ROSHINI
Assistant professor
Computer Science Department
SREE DATTHA INSTITUTE OF ENGINEERING & SCIENCES, Hyd

ABSTRACT

For the reason of enhancing and demanding popularity of multimedia streaming applications and services in current days, in the case of trusted video delivery, in the case of reliable video-prevention of leaks, has become really important. While managing the privacy of the user, the conventional system has solved this problem by suggestive of ways of unsighted traffic across the network. This conventional system maintains a high detection accuracy while dealing with traffic variations in the network (for instance, network delay and packet loss), on the other hand, in their discovery presentation of the video The prominent change in the duration effects a lot to diminish. A novel material focuses on organization the problem present a discovery plan, which is sturdy in the video length variations. Differentiate the video of a diverse duration, we institute the same association between the anthology and the video compared to the duration of the videos. In that way, we also enhance the detection of the offered schemes even in the environment, in the length of the video. by the test, the effectiveness of our concerned scheme is predicted in the length of video length, delay change, and differences of packet loss.

KEYWORDS : Streaming content, leakage detection, traffic pattern, degree of similarity.

I. INTRODUCTION

Circulated computing is a territory of computer science that studies spread systems. A speckled scheme is a software organization in which mechanism situated on networked computers swap a few words and harmonize their procedures by fleeting messages. The mechanism corelate with each other in class to achieve a universal goal. There are many alternatives for the information fleeting method, together with RPC-like connectors and significance queues. Three important personalities of circulated systems are: concurrency of works, need of a universal clock, and independent stoppage of mechanism. A vital aim and dare of circulated systems is position precision. Examples of scattered systems diverge from SOA-based systems to extremely multiplayer online games to peer-to-peer applications.

A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.

Distributed computing also refers to the use of distributed systems to resolve computational problems. In distributed computing, a problem is divided into many tasks, each one is resolved by one or additional computers, which communicate with each other by message fleeting. The utterance circulated in words such as "circulated organization", "distributed programming", and "circulated algorithm" originally known as computer networks where being computers were actually circulated within some geographical section. The conditions are at the at hand time used in a much broad sense, even referring to personal processes that run on the same substantial computer and interrelate with each other by information passing. While there is no single definition of a circulated system, the following important properties are normally used:

1. There are some self-governing computational entities, each of which has its own confined memory.

2. The entities communicate with each other by message passing.

In this article, the computational objects are called computer or nodes.
A circulated system may have a general aim, such as solving a widespread computational trouble.] on the other hand, each computer may have its own user with individual requirements, and the function of the distributed system is to coordinate the use of shared property or provide contact services to the users.

Other typical properties of circulated systems comprise the following:

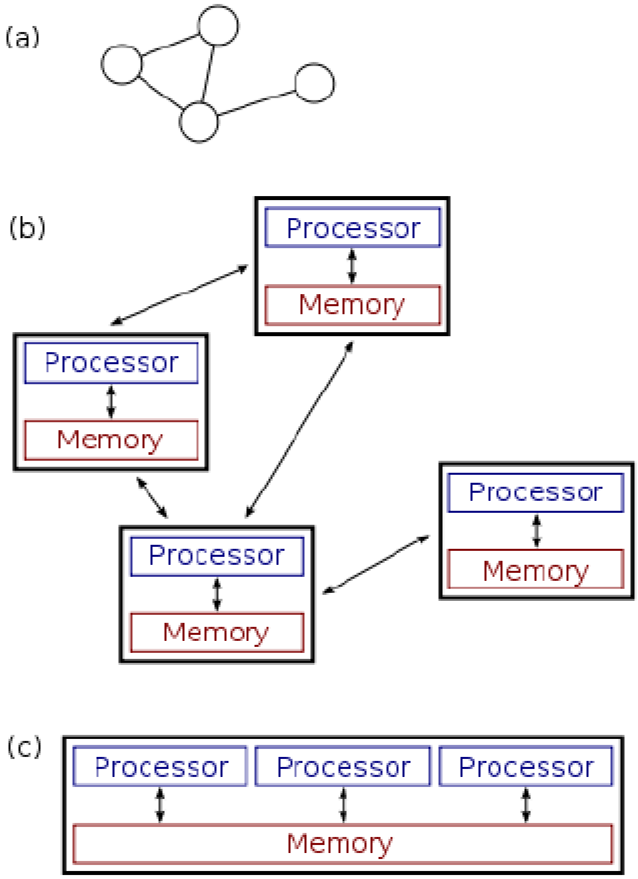
1. The system has to put up with failures in personage computers.

2. The organization of the system (network topology, network latency, quantity of computers) is not known in proceed, the system may contains of various sorts of computers and network associations and the system may alter throughout the execution of a circulated program.

3. Each computer has only a not enough, unfinished vision of the scheme. Each computer may identify only one part of the input.

Distributed systems are set of of networked computers, which have the same aim for their work. The expressions "coexisting computing", "corresponding computing", and "distributed computing" have a lot of overlie, and no clear difference exists between them. The same system may be distinguish both as "parallel" and "distributed"; the processors in a distinctive distributed system dart concurrently in parallel. Parallel computing may be seen as a particular definitely connected form of distributed computing, and distributed computing may be seen as a insecurely predetermined form of parallel computing. on the other hand, it is potential to generally classify contemporaneous systems as "parallel" or "distributed" using the following criteria:

In parallel computing, all processors may have access to a shared memory to exchange data among processors.In distributed computing, each processor has its personal personal memory (distributememory). Data is swapped by Paasing the message by the process.



The figure on the right illustrates the discrepancies between distributed and parallel systems. Figure (a) is a schematic view of a distinctive distributed system; as usual, the system is represented as a network topology in which each node is a computer and each line linking the nodes is a communication link. Figure (b) shows the same distributed system in more detail: each computer has its own local memory, and information can be swapped only by passing messages from one node to another by using the obtainable communication links. Figure (c) shows a parallel system in which each processor has a direct access to a shared memory.

The situation is further intricate by the traditional uses of the terms parallel and distributed algorithm that do not relatively match the above definitions of parallel and distributed systems; see the section Theoretical practicalities below for more detailed discussion. nonetheless, as a rule of thumb, high-performance parallel computation in a shared-memory multiprocessor uses parallel algorithms while the harmonization of a large-scale distributed system uses distributed algorithms.

II. EXISTING SYSTEM:

A central apprehension in video streaming forces is the safety of the bit stream from illegal use, doubling-up and distribution. One of the most accepted approaches to avoid unwanted contents contribution to unlawful users and/or to guard authors' copyrights is the digital rights administration (DRM) expertise. Most DRM techniques employ cryptographic or digital watermark methods. on the other hand, this category of approaches have no

noteworthy outcome on redeployment of contents, decrypted or restored at the user-side by formal yet spiteful users.

DISADVANTAGES OF EXISTING SYSTEM:

Moreover, redeployment is to be precise no longer complex by using peer-to-peer (P2P) streaming software. Hence, streaming traffic may be leaked to P2P networks.

III. PROPOSED SYSTEM

In this paper, we spotlight on the illicit reorganization of streaming inforation by an approved user to exterior networks. The active proposals observe information obtained at diverse nodes in the core of the streaming path. The retrieved data is used to create traffic patterns which come out as distinctive waveform per contented, just like a fingerprint.

ADVANTAGES OF PROPOSED SYSTEM:

1. These technologies develop the allotment of any type of data over the Internet.

2. The traffic pattern production method performed in predictable techbiques.

IV. IMPLEMENTATION

4.1 Video Leakage setting:

Based on the popularity of transforming delivery of movies, enhancement of P2P streaming software has achieved more Diligence. These technologies enhance the transformation of any type of detais over the Internet. First, a known user in a safe network taken streaming information from a content server. Then, with the use of a P2P streaming software, the regular yet spiteful user re transfer the streaming information to a non regular user unknown its network. These type of content-leakage is barely detected or Detained by watermarking and DRM-based methods.

4.2 Leakage Detection measures:

In particular the video streaming process, the variations of the quantity of traffic seems as a unique waveform related to the content. Thus by observing this knowledge retrieved at different nodes in the network, content-leakage can be detected. The topology composed of two main parts, namely the traffic pattern generation engine attach in each router, and the traffic pattern matching engine manipulated in the management server. Owing to the fact that, each router can find its traffic quantity and cause to traffic pattern. For the time being, the traffic pattern similar in pattern engine measures the state of fact between traffic patterns through a matching method, and based on certain measures, evaluate contents loss. The result is then similar in character to be the destination edge router to curb leaked traffic.

4.3 Pattern Generation:

We report the traffic pattern peer group procedures performed in technical operations. Traffic pattern peer group process is based on a either time slot-based algorithm or a packet size-based algorithm. Time slot-based algorithm is a direct solution to produce traffic patterns by summing the amount of traffic appearance for the time of a particular period of time, t. In case some packets are pending, they may be stored over the observant list, xi+1, instead of the primary list, xi. Therefore, hindrance and jitter of packets pull or twist out of shape the traffic pattern, and as a effect of an action, reduce the the quality or state of being correct in pattern matching. Moreover, time slot-based algorithm is influenced by packet detriment. Packet size-based algorithm describes a slot as the summation of quantity of arrival traffic until the statement of a specific packet size. This algorithm only makes use of the packet arrival way and packet size, since is robust to vary in environment such as delay and jitter. However, packet size-based algorithm shows no errors to packet loss else not missing of any information in the packet.

4.4 Pattern Matching:

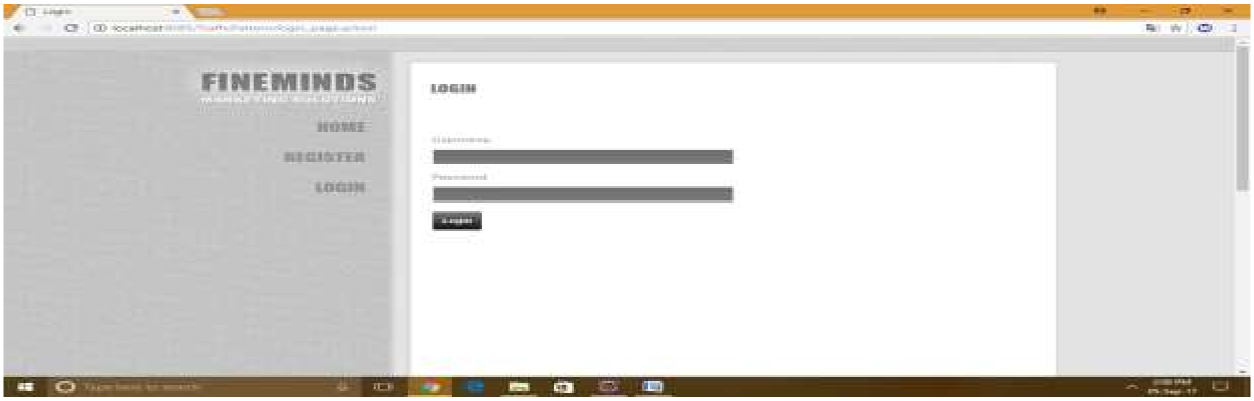
In pattern picture, the degree of state of fact is defined to be the similarity value between designs. The server-side traffic designs shows the precise traffic pattern. The basic techniques to account the similarity of traffic patterns called cross-correlation matching algorithm, composed of computing the cross-correlation coefficient, which is used as a metric of similarity between the changed traffic patterns. Before evaluating the similarity among the incomplete pattern XU and the server-side pattern YU.

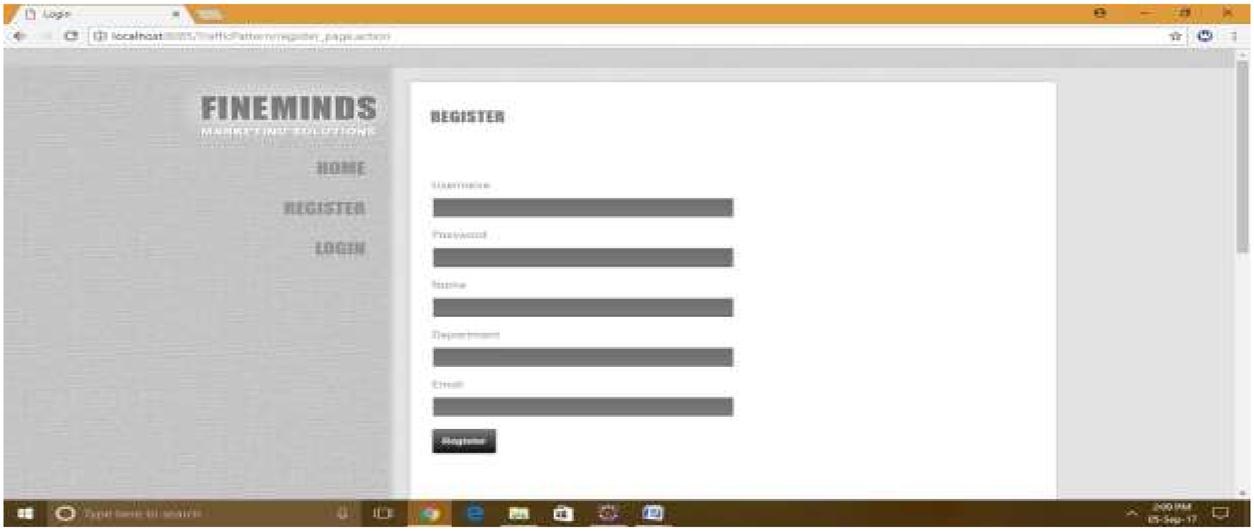
Another pattern matching algorithm is the dynamic programming (DP) matching based on the DP technique. DP matching utilizes the an amount of space between two compared patterns in U-dimensional vector space as based on lengths refers their significance of the significance of fact.

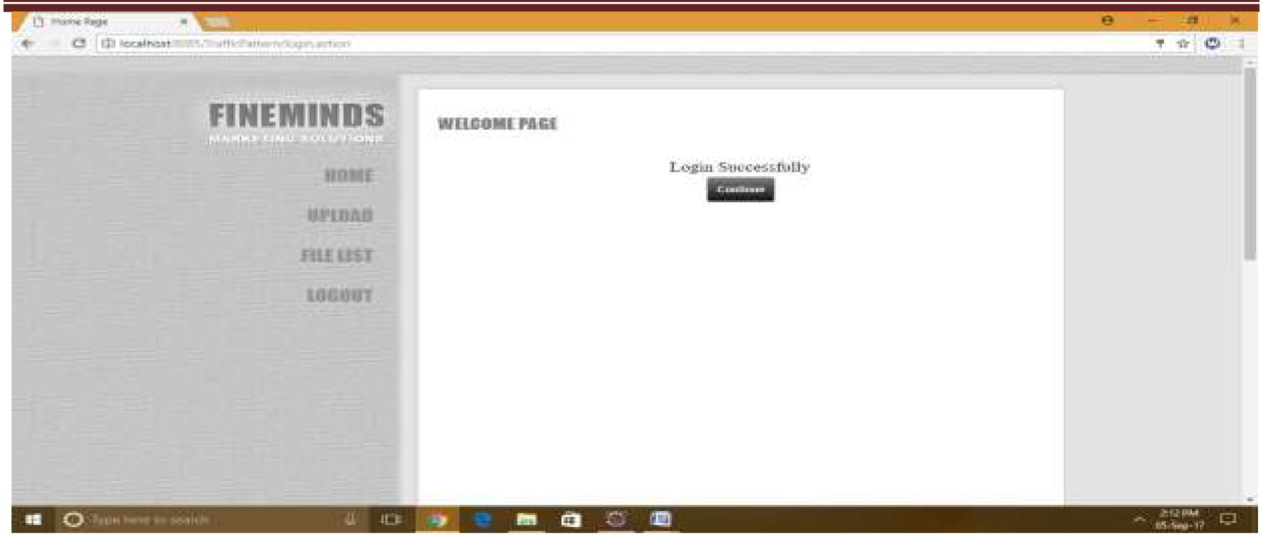
4.5 Leakage Detection Criterion:

The cross-correlation matching algorithm is implemented on both the traffic patterns generated through time slot-based algorithm and those generated through packet size-based algorithm. The similarity data taken from the matching of time list-based produced traffic designs are large quantity and low quantity and their transforming is taken to be basically distributed around zero, since the transformation of relation between coefficient measures of two random waveforms is minimum to a normal distribution. On the other hand, the DP matching algorithm is executed on traffic patterns produced by packet size-based algorithm. So taken into consideration of, a exact predefined measure is used as the conclusion entrance to packets. Whether or not patterns are matched is decided by taking in to consideration the distance measured through DP matching with the decision threshold, i.e., the distance minimum than the threshold shows that the compared traffic patterns are similar.

V. SCREENS

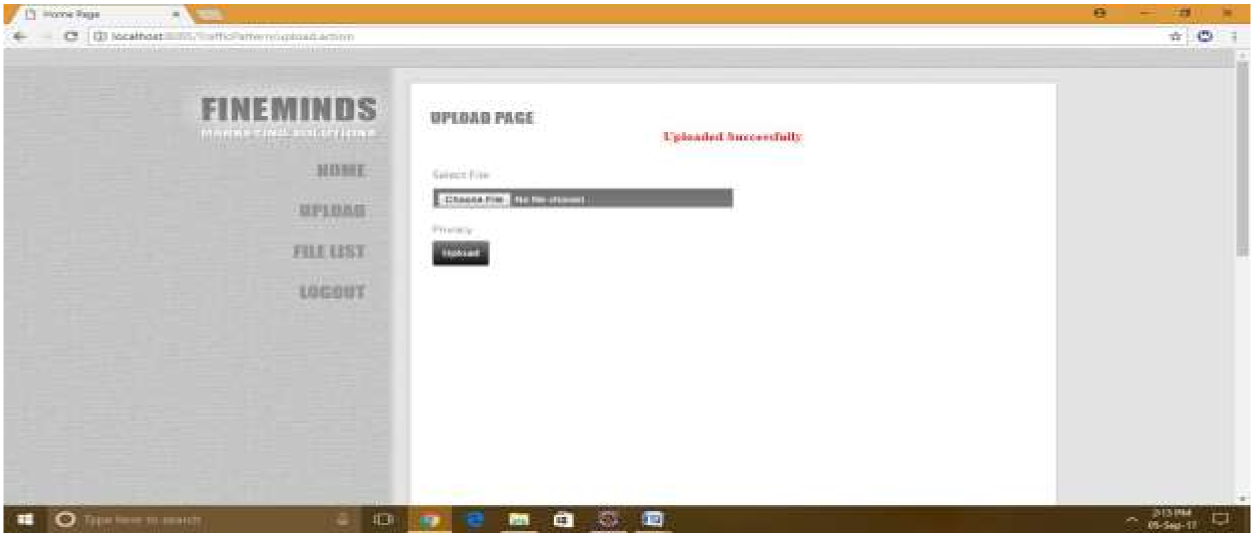






WELCOME PAGE

Login Successfully



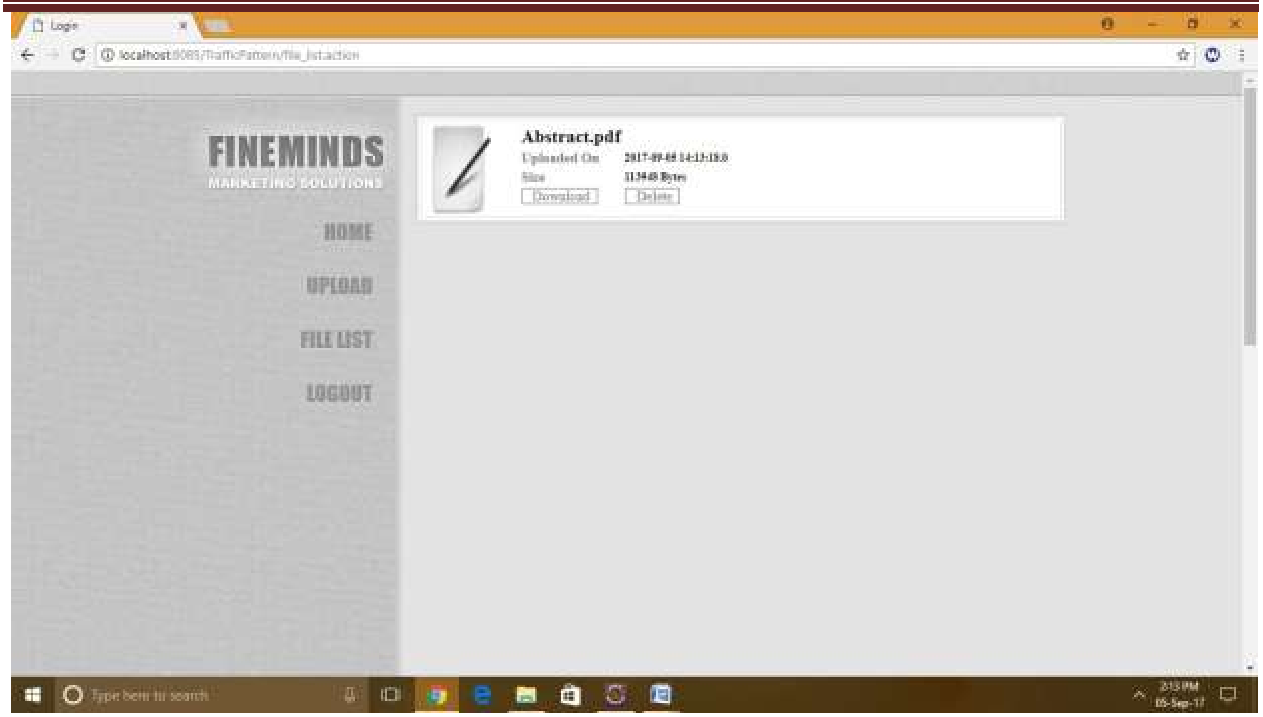
UPLOAD PAGE

Uploaded Successfully

Select File

Choose File No file chosen

Privacy



Abstract.pdf

Uploaded On 2017-09-05 14:13:19.0

Size 113448 Bytes

Download Delete

VI. CONCLUSION

The content leakage detection system build on the fact that each Transmit or receiving the content has a unrepeated traffic pattern is an advanced solution to curb unauthorized redistribution of contents by a regular, yet spiteful user. Though three typical conventional methods, namely, T-TRAT, P-TRAT, and DP-TRAT, show robustness to delay, jitter or packet loss, the detection performance diminish with considerable changes of video lengths. This paper used to solve these issues by introducing a dynamic leakage detection scheme. Moreover, in this paper, we peruse the performance of the proposed method under a real network environment with videos of different ranges. The proposed method allows flexible and precise transmit or receiving content leakage detection independent of the ranges of the streaming content, which increase secured and be sured content delivery.

REFERENCES

[1] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture," Proc. ACM SIGCOMM, pp. 55-67, Aug. 2001.

[2] Z. Yang, H. Ma, and J. Zhang, "A Dynamic Scalable Service Model for SIP-Based Video Conference," Proc. Ninth Int'l Conf. Computer Supported Cooperative Work in DE, pp. 594-599, May 2005.

[3] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture," Proc. ACM SIGCOMM, pp. 55-67, Aug. 2001.

[4] O. Adeyinka, "Analysis of IPSec VPNs Performance in a Multimedia Environment," Proc. Fourth Int'l Conf. Intelligent Environments, pp. 25-30, 2008.

[5] E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in Digital Video Content Protection," Proc. IEEE, vol. 93, no. 1, pp. 171-183, Jan. 2005.

[6] S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications," IEEE J. Selected Areas Comm., vol. 16, no. 4, pp. 573-586, May 1998.

[7] M. Barni and F. Bartolini, "Data Hiding for Fighting Piracy," IEEE Signal Processing Magazine, vol. 21, no. 2, pp. 28-39, Mar. 2004.

[8] K. Su, D. Kundur, and D. Hatzinakos, "Statistical Invisibility for Collusion-Resistant Digital Video Watermarking," IEEE Trans. Multimedia, vol. 7, no. 1, pp. 43-51, Feb. 2005.

[9] E. Diehl and T. Furon, "Watermark: Closing the Analog Hole," Proc. IEEE Int'l Conf. Consumer Electronics, pp. 52-53, 2003.

[10] Y. Liu, Y. Guo, and C. Liang, "A Survey on Peer-to-Peer Video Streaming Systems," Peer-to-Peer Networking and Applications, vol. 1, no. 1, pp. 18-28, Mar. 2008.

[11] E.D. Zwicky, S. Cooper, and D.B. Chapman, Building Internet Firewalls, second ed., O'Reilly and Assoc., 2000.

[12] M. Dobashi, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Traitor Tracing Technology of Streaming Contents Delivery Using Traffic Pattern in Wired/Wireless Environments," Proc. IEEE Global Telecomm. Conf., pp. 1-5, Nov./Dec. 2006.

[13] K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection Using Dynamic Traffic Pattern," IEICE Trans. Comm., vol. J19-B, no. 2, pp. 166-176, 2010.

[14] A. Asano, H. Nishiyama, and N. Kato, "The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection (Invited Paper)," Proc. Int'l Conf. Computer Comm. Networks (ICCCN '10), pp. 1-6, Aug. 2010.

[15] S. Amarasing and M. Lertwatechakul, "The Study of Streaming Traffic Behavior," KKU Eng. J., vol. 33, no. 5, pp. 541-553, Sept./ Oct. 2006.

[16] Y. Gotoh, K. Suzuki, T. Yoshihisa, H. Taniguchi, and M. Kanazawa, "Evaluation of P2P Streaming Systems for Webcast," Proc. Sixth Int'l Conf. Digital Information Management, pp. 343-350, Sept. 2011.

[17] R. Duda, P. Hart, and D. Stock, Pattern Classification, second ed. Wiley Interscience, 2000.