Tracing Illegal Redistributors of Streaming Contents using Traffic Patterns

K. Ramya
Department of Computer Science
Anna University of Technology, Coimbatore.
Hosur-635109, Tamilnadu, India

D. Ramya Dorai
Department of Computer Science
Anna University of Technology, Coimbatore.
Hosur-635109, Tamilnadu, India

Dr. M. Rajaram
Department of Electrical & Electronics
Anna University of Technology
Tirunelveli, Tamilnadu, India

ABSTRACT
The tracing scheme is using similarity of traffic pattern to trace the source of leaks when sensitive or proprietary data is made available to large set of parties. On the other hand we must implement digital rights management (DRM) to control content spreading and to avoid unintended content use. General tracing methods use either watermarking or cryptographic keys to protect the digitally protected content. In those methods, malicious users can interrupt tracing with illegal process at user side computers. To prevent all illegal process at user side, routers should analyze information embedded in to packets which is unrealistic. The proposed method is used to detect illegal content streaming by using only traffic patterns which are constructed from amount of traffic traversing routers.

General Terms
Variable Bit Rate(VBR) traffic, Streaming Content.

Keywords
Digital Rights Management (DRM), Streaming Content, Traffic Pattern.

1. INTRODUCTION
In recent years, the evolution of advanced wired and wireless access networks along with the rapid development of broadband Internet have allowed us to easily utilize real time video streaming applications and services via high-speed networks. YouTube [9] and MSN Video [10] are notable examples of such applications, which serve a huge population of users from all around the world with diverse contents, ranging from daily news feeds to entertainment feeds including music, videos, sports, and so forth, by using streaming transmission technologies. In addition, real-time video streaming communications such as web conference [1], [2] in intra-company networks or via Internet with Virtual Private Networks (VPNs) are being widely deployed in a large number of corporations as a powerful means of efficiently promoting business activities without additional costs. Indeed, these streaming technologies tend to be adopted more heavily by businesses in contrast with individual users. Since most of these data streams (particularly in businesses) contain confidential information, ensuring security to prevent illegal leakage of streamed contents is a crucial aspect.

One of the most popular approaches to prevent undesirable contents distribution to non-licensed users or to protect the author's copyrights is Digital Rights Management (DRM) technology. Traitor is one who is the illegal redistributors of streaming content to non legitimate user. Traitor tracing is technology which enable us to observe users contents streaming and to detect illegal streaming[7] and [11]. In general, traitor tracing systems embed copyright notices and server side information into contents, using the digital watermarking technology. Recently, the method which uses cryptographic keys is to detect illegal transfers of contents [15].

However, those methods depend on information embedded into contents, malicious users can interrupt tracing with illegal process at user side computers. To prevent all illegal processes at user side computers, routers should analyze information embedded into packets which is unrealistic because it needs very high computation.

Furthermore, observing information in packets may cause problems from the perspective of the protection of personal information. Therefore, we should examine the traitor tracing method which does not use embedded information.

Using Variable Bit Rate (VBR), the movies bit rate changes according to the change of scene. When these movies are delivered and played as contents by streaming, the changes of the amount of traffic will appear as a unique waveform on the contents. This server information base waveform can be related to user information which is independent of the movies contents. Therefore, by matching the waveform at the server side and the waveform at the user side, we can detect the reception of the contents. If there is a user who receives the contents without permission, we judge that this is an illegal reception.

The proposed method is used to detect an illegal streaming using only the amount of traffic which is observed in very short period of time (approximately 20[s]) from the routers located just before the users. This system can be operated with less processing time than packet analysis. Furthermore, it can prevent illegal processes of malicious users efficiently, because no process is needed at user side computers.

The rest of this paper is organized as follows. Section 2 surveys overview of DRM technologies, the conventional methods in traitor tracing, and research works on these technologies. Section 3 introduce the proposed illegal redistributors (Traitor) tracing system using traffic pattern. Section 4 deals with the consideration in traitor tracing system. Section 5 discussed the effective counter measures to achieve high performance even in complicated network environments and summarize the open issues.

2. RELATED WORK

2.1 Cryptographic Schemes

DRM technology consists of several technologies, such as encryption and access conditioning. The traitor-tracing technology is also one of the key technologies that constructs DRM systems, and is used to monitor the content usage and to confirm that a user appropriately uses contents. Traitor tracing schemes can be implemented by using cryptographic schemes or watermarking schemes. Any data that is to be available to some while it should not be available to others can obviously be protected by encryption. The data supplier may give authorized parties cryptographic keys allowing them to decrypt the data. This does not solve the problem above because it does not prevent one of those authorized to view the message (say, Alice) from transferring the streaming content to some unauthorized party (say, Bob). Once this is done then there are no (cryptographic) means to trace the source of the leak. We call all such unauthorized access to data piracy. The traitor or traitors is the (set of) authorized user(s) who allow other, non-authorized parties, to obtain the data. These non-authorized parties are called pirate users. The traitor tracing schemes of Chor et al. [4] adopt the following model: pirate decoders that allow access to the content may be manufactured but such decoders, if captured, must inherently contain identifying information that will allow the broadcaster to cut them off from future broadcasts. Additionally, the source of piracy can be detected and legal means can be taken. To do so, Chor et al. introduce a new form of cryptography that uses one encryption key and multiple distinct decryption keys, with the property that one cannot compute a new decryption key from a given set of keys. The traitor tracing schemes of [4], [5], and [6] approximate such a scheme. Two cost measures are to be considered when implementing such schemes: storage requirements at the user end and the necessary increase of bandwidth. The Achilles' heel of such traitor tracing schemes is their underlying assumption that pirates provide unauthorized subscribers with decoders capable of decoding the original broadcast. Such schemes would be ineffective if the pirate were simply to rebroadcast the original content using a pirate broadcast system. The traitor tracing schemes with cryptographic keys gives the decoder which is personalized by a unique allocation of decryption keys, once, before it is sold to a subscriber. Only when a pirate decoder is captured, the traitor tracing schemes activated in order to trace a legal decoder used in building the pirate unit.

2.2 Watermarking Schemes

Watermarking schemes were introduced and discussed by Boneh and Shaw in [6]. In their study they assumed that the content is watermarked once, prior to its broadcast. The schemes of [4] and [6] are static. To overcome this, dynamic model is introduced [5]. In general, the watermarking problem is to generate multiple versions of watermarked content so that, given a black market copy of that content, the watermarks embedded in that copy would lead to the identification of its source. A watermarking scheme for tracing traitors consists of two essential parts:

1. **Watermark distribution:** an algorithm that assigns each subscriber a watermarked copy of the content.
2. **Tracing and incrimination:** an algorithm that, given an illegal copy of the content, uses the watermarks embedded in it in order to trace back at least one of the traitors that participated in producing that copy.

A watermarking scheme is called *deterministic* if it traces and incriminates all traitors and no one else but the traitors. On the other hand, schemes in which there is a small chance of false incrimination are referred to as *probabilistic*.

The simplest tracing system using watermarking is considered as shown in Fig. 1. The following is the procedure adopted by this system.

1) The content provider embeds unique information1 into the content using digital watermarking, and produces copies of the content.

2) Each copy of the content is delivered to different users.

3) The user's application analyzes the content's data and reassembles the embedded information.

4) The user's application notifies that he or she is watching the content, according to the extracted information.

This shows the mechanism to verify whether or not the secondary content distributions exist and to find the runoff source of the secondary content. First, unique content $\mathbf{C_1}$ is delivered to user $\mathbf{U_1}$. Next $\mathbf{U_1}$**'** s application finds watermarked information $\mathbf{W_1}$ and notifies it to server **S**. When an unauthorized secondary content distribution is conducted

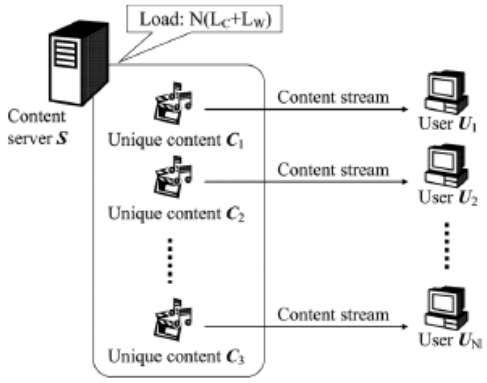

Figure.1. **Detection System Using Watermarking**

between $\mathbf{U_1}$ and $\mathbf{U_2}$, $\mathbf{W_1}$ is also found from $\mathbf{U_2}$'s content. Next, $\mathbf{U_2}$'s application notifies $\mathbf{W_1}$ to **S**. Finally, **S** finds duplicated $\mathbf{W_1}$ and concludes that the content is secondarily delivered from $\mathbf{U_1}$ to $\mathbf{U_2}$ indicated as a caution sign in Figure.1.

However, this traitor-tracing method has two issues. First, this method requires a large amount of computation to encode content and to embed watermarks, since each user receives an individual content. For instance, if the load of content encoding and watermarking are $\mathbf{L_C}$ and $\mathbf{L_W}$, respectively, the total load to deliver content which has traceability of traitors should be at least $\mathbf{N*(L_C + L_W)}$. Here, **N** is the number of content users. This is especially not realistic for real-time streaming systems. This is why a method to assist tracking traitors and to reduce the load is strongly needed.

Second, the watermark, which is a key technology of traitor tracing and is used to embed information into the host signal, is not without its shortcomings. Furthermore, there are known

attacks against watermarks, such as the removal attack, collusion attack, copy attack, closest-point attack, and sensitivity attack.

According to their work, general watermarks perform poorly against the benchmark that they proposed. Consequently, when the watermark is used over networks, it causes some problems because of unclear network environments and users. This is why traitor-tracing methods with watermarking require an additional technique to tighten the scope of application by narrowing down the list of users who may be traitors. Additionally, it is desirable to interoperate with a method to find suspicious content distributions without watermarking. In particular, we will consider detection of "illegal relay" by avoiding deciphering and decoding contents in watermarking. Towards this end, we envision a method to track the content stream using information about traffic amount observed at routers. Our method circumvents the need of decrypting and decoding the content, and this is the major contrast with respect to the watermarking technique. The proposed method can also be used with general traitor-tracing methods in order to enhance the security.

3. DETECTION SYSTEM USING TRAFFIC PATTERNS

In streaming contents delivery equipped with VBR encoding techniques, the content-dependent unique traffic volume allows us to detect the leakage of contents to the external networks by comparing traffic patterns observed at the network nodes close to the content server with those monitored at the egress node. Figure.2 shows the overall configuration of the proposed content leakage detection systems. In streaming contents delivery equipped with VBR encoding techniques, the content-dependent unique traffic volume allows us to detect the leakage of contents to the external networks by comparing traffic patterns observed at the network nodes close to the content server with those monitored at the egress node. Figure. 2 show the overall configuration of the proposed content leakage detection systems.

Figure.2 depicts the leakage detection process in a typical scenario whereby confidential content is being delivered from the server to the licensed yet malicious user, which re-distributes the content, via P2P streaming software, to an unlicensed user located in the external network. Each router observes its traffic volume and informs the management server by using Simple Network Management Protocol (SNMP) like mechanisms.

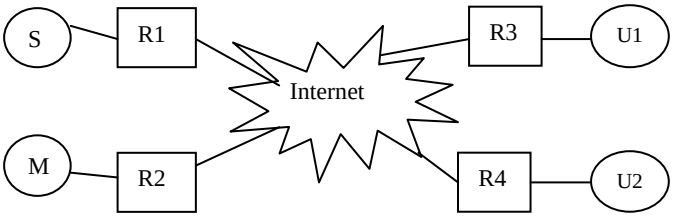

Figure.2. **Proposed Detection System**

The management server accordingly generates traffic patterns, and is able to detect content leakage by comparing these patterns.

3.1 Traffic Pattern

In animated contents (MPEG), the bit rate is automatically adjusted to the changes of the scene. Each content is considered to have its own characteristic feature just like fingerprint, therefore, the unique information of these contents appear in waveforms. This paper focuses on VBR traffic, which is typical type, used in contents delivery and calls these waveforms "Traffic pattern". Here, the each content is distributed independently of each streaming server.

The traffic pattern is generated by dividing traffic into some chunks of IP packets by following a division policy. There are three division policies

1) Time slot- based Traitor Tracing (T-TRAT)
2) Packet size- based Traitor Tracing (P-TRAT)
3) DP (Dynamic Programming) matched Traitor Tracing (DP-TRAT)

The division policy is unique to each conventional method. In T-TRAT, a chunk is composed of packets arriving during the same timeslot. On the other hand, packets, size of which is below a certain threshold, are used as delimiters to determine chunks in both P-TRAT and DP-TRAT approaches. The division policy does not depend on time. Therefore, it is robust against the packets delay.

Traffic pattern is defined as amount of traffic for one time slot, a certain period of time Δ t(s) and expressed for N dimension in the following expression.

$$X=(x1,x2,x3,\ldots,x_N)^t,\ T = N(\Delta t) \qquad (1)$$

Here, T(s) is the whole length of traffic pattern.

Similarity of traffic patterns between certain user side (Y_U) and a part of server-side pattern X_U and use a cross-correlation coefficient as a criterion to judge the similarity of traffic patterns. Calculate the cross-correlation coefficient R_{XY} using the following equation (2).

$$R_{XY} = \frac{(X'_U)^t\, Y'_U}{\sqrt{\|X'_U\|^2 \cdot \|X'_U\|^2}} \qquad (2)$$

Where $-1 < R_{XY} < 1$ and X'_U, Y'_U are the normalized traffic patterns when the *mean* = 0, and *variance* = 1.

$$\boldsymbol{X}'_{\boldsymbol{U}} = \begin{pmatrix} (x_1-\bar{x})/s_x \\ (x_2-\bar{x})/s_x \\ \vdots \\ (x_U-\bar{x})/s_x \end{pmatrix}, \boldsymbol{Y}'_{\boldsymbol{U}} = \begin{pmatrix} (y_1-\bar{y})/s_y \\ (y_2-\bar{y})/s_y \\ \vdots \\ (y_U-\bar{y})/s_y \end{pmatrix}$$

R_{XY} 's value would be near to 1, if two vectors were similar to each other.

3.2 Comparison of Traffic Pattern

Figure. 3. Overviews the traffic pattern matching process. Since the server-side traffic pattern, X_S, and edge router-side traffic pattern, Y_U, have different lengths in general, i.e., $U \leq S$, we employ a sliding window-based method. The size of the window is set to be equal to the length of the receiver side router pattern, U. The pattern matching procedure is repeatedly called($S - U + 1$)

times for different combinations of the edge router-side pattern and a piece of the server-side pattern, X_U, clipped from the original pattern, X_S, by the sliding window. If and only if even one of the matching results shows that the compared patterns are similar, we may conclude that there is a content leakage. The similarity criteria are different among conventional methods according to the adopted pattern matching algorithm. As described next, the cross-correlation matching coefficient is used in both T-TRAT and P-TRAT approaches. On the other hand, Dynamic Programming (DP) matching is employed in DP-TRAT. Next, the Transform Process in Figure.4 is conducted to prevent influences of burst errors in wireless environment. In the Transform Process, first, vector's elements whose values are equal or less than a certain threshold T_P are removed from the User-side pattern Y_U (U-dimension) and new User-side pattern Y_U (U - dimension) are constructed. For example, three elements are removed in Figure 4. Next, the same part of the Server-side pattern's elements as the User-side pattern is also removed and new Server-side pattern X_U (U-dimension) is constructed. In Figure 3, three corresponding elements are removed. After the Transform Process, cross correlation coefficient R_{XY} is calculated with Equation (2).

After these, sliding the window from left to right is done by one slot and the whole server-side pattern is scanned. We repeat the extraction of pattern X_U (U-dimension) from server-side pattern X_S (S-dimension), the Transform Process and also calculate the cross-correlation coefficient.

Error Losses elements as the User-side pattern is also removed and new Server-side pattern X_U (U - dimension) is constructed. In Figure 4, three corresponding elements are removed. After the Transform Process, cross correlation coefficient R_{XY} is calculated with Equation.

After these, sliding the window from left to right is done by one slot and the whole server-side pattern is scanned. We repeat the extraction of pattern X_U (U-dimension) from server-side pattern X_U (S-dimension), the Transform Process and also calculate the cross-correlation coefficient. If whole server-side pattern X_S had S-dimension and user-side pattern Y_U had U-dimension, the number of the calculation would be S-U+1 time.

If a large value exists in cross-correlation coefficient graph, it means that a certain user-side pattern is similar to the part of the server-side pattern and such a pattern is called a "matched pattern". In this case, the user is considered to be receiving contents.

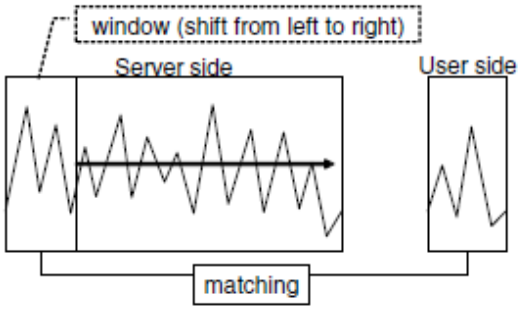

Figure. 3. **Traffic Pattern matching Mechanisms**

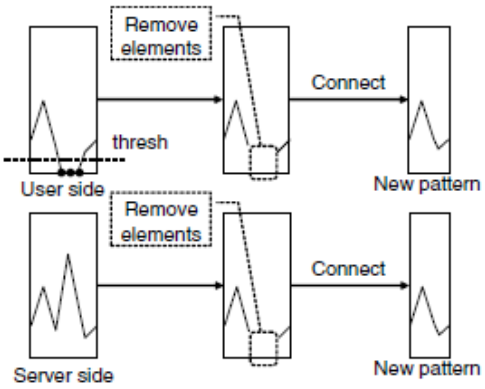

Figure. 4. **Traffic Pattern in Wireless Environment and Measure against Burst error**

3.3 Dynamic Determination of Discrimination Threshold

Compared to wired environment, in wireless environment, packet losses occur more frequently due to random errors and burst errors. This causes user-side traffic patterns to be impaired and the overall value of the cross-correlation coefficient to be decreased. Thus, the detection would be almost impossible, if we set the discrimination threshold value to be fixed, for example T_R = 0.9 (the value that is generally considered to be high correlation). For this reason, we introduce a method to dynamically determine the discrimination threshold value T_R from the statistical tendency of the cross correlation coefficient. In this way, we can flexibly cope with the network state. Most parts of $S - U + 1$ cross-correlation coefficients have small values, whose distribution is considered to be the normal distribution[16], since the distribution of cross-correlation coefficients of two different waveforms is approximated to the normal distribution. However, the cross-correlation coefficient of two patterns similar to each other has a large value compared to most other values and such a large value is called as an "outlier". The part which should be detected is one part among $S-U$ +1 parts and such a part is statistically considered as an outlier. The mathematical way of detecting outlier is based on the mean and variance is as follows. Let μR be the mean and σR be the variance of cross-correlation coefficient, the discrimination threshold value T_R is defined as

$$T_R = \min(\mu R + 4\sigma R,\ 1.0) \qquad (3)$$

According to the Chebyshev's inequality, the probability that the data are equal or greater than the threshold value T_R is about 6[%]. As a result, the coefficient greater than T_R calculated from equation (3) is regarded as one outlier. Figure.5 shows the proposed determination algorithm which can be applied in both wired and wireless environments. Therefore, without taking into account which environment users belong to, we can detect an illegal streaming by using this algorithm.

Figure.5 shows the proposed determination algorithm which can be applied in both wired and wireless environments. Therefore, without taking into account which environment users belong to, we can detect an illegal streaming by using this algorithm.

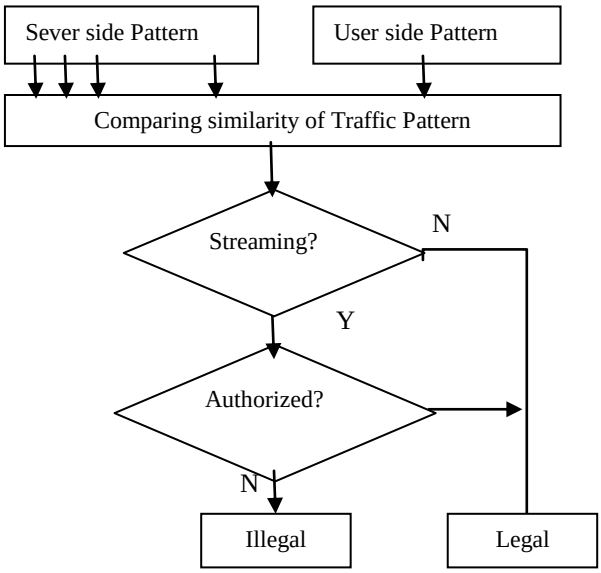

Figure.5. **Algorithm of Discrimination**

4. CONSIDERATION

4.1 Delay

The main problem in real-time delivery of movies is the delay due to the huge size of data. The traffic pattern in this case becomes the parallel displacement of the traffic pattern when there is no delay. However, even if there is a difference in detecting position, the characteristic of waveform would not be impaired. Therefore, delay should have small impact on our detection system.

4.2 Background Traffic

In general, there are not only contents traffic on the network, but also many other applications traffic and other users' traffic. However, to some extent, it is possible to extract the contents traffic from other users' one, using IP address information and packet type.

5. DISCUSSION

The performance of illegal re-distributor tracing systems is dominated by both employed traffic pattern generation and matching algorithms. Two features have been demonstrated in the work of Matsuda *et al.* [17]. First, the adaptation of packet size-based traffic pattern generator, instead of the time slot based one used in T-TRAT, enables P-TRAT to achieve robustness to packet delay jitter. Second, the employment of DP matching as a pattern matching technique permits DP-TRAT to remove the effect of packet losses. In addition, their work provides us with significant results on the relations between such algorithms, and the robustness to packet reordering and encryption. However, the key concern in adopting both time slots based and packet size-based traffic generators consisted in the issue of packet reordering, which may have a significant impact upon the performances of all the conventional methods. Indeed, in these conventional approaches, considerable performance degradations were noticed in network settings with the high packet reordering rate equal to seven percent whereby playing the streaming contents becomes almost impossible. This implies that the traffic pattern changes are not significant when the packet reordering rate is not high regardless of the equipped traffic pattern generators. However, high packet reordering rates is not uncommon in environments with multiple paths existing between the observation points . This, still, remains an open issue. Packet size distribution based traffic pattern generation is considered as a potential solution which may be robust to packet reordering.

In contrast to the packet reordering issue, the performance degradation due to packet encryption is the most difficult problem. As potential solutions to cope with the performance degradation due to packet encryption, we here indicate two different directions. The first one is the enhancement of the proposed method by introducing an intelligent algorithm being able to estimate the additional packet header size for encryption with high accuracy even with the occurrence of fragmentation. In this approach, the performance enhancement is dominated by the accuracy of the equipped estimation algorithm, i.e., not depending on the traffic pattern generation and matching algorithms, that is derived from the fact that the proposed method achieves almost perfect performance without fragmentation. The second one is the clean state approach based on a new traffic pattern generation scheme, i.e., generating traffic patterns without counting small packets at both observation points so as not to be affected by fragmented packets. It can be either time slot based or packet size-based, or based on other new schemes. In such approaches, we may additionally need to develop a new traffic pattern matching mechanism to counter-act the difference between compared traffic patterns arising from the additional traffic volume due to packet encryption. It is supposed that introducing additional components allows us to detect content leakages in various environments. However, one of the distinct advantages of traffic pattern-based illegal re-distributor tracing approach lies in its light processing load. Therefore, we are required to devise a new technology by taking into consideration its practical use in real networks.

6. REFERENCES

[1] Y. Chu, S. G. Rao, S. Seshan and H. Zhang, "Enabling conferencing applications on the Internet using an overlay multicast architecture," in Proc. ACM SIGCOM, pp. 55-67, California, USA, Aug. 2001.

[2] Z. Yang, H. Ma, and J. Zhang, "A dynamic scalable service model for SIP-based video conference," in Proc. 9th International Conference on Computer Supported Cooperative Work in Design, Vol. 1, pp. 24-26, Coventry, UK, May. 2005.

[3] J. Schwenk and J. Ueberberg, Tracing Traitors using Finite Geometries, manuscript.

[4] B. Chor, A. Fiat, and M. Naor, Tracing Traitors, Proc. Crypto 94, LNCS 839, Springer-Verlag, Berlin,

[5] A. Fiat and T. Tassa, "Dynamic traitor tracing," J. Cryptology, vol. 14, no. 3, pp. 211–223, 2001.

[6] D. Boneh and J. Shaw, Collusion-Secure Fingerprinting for Digital Data, IEEE Transactions on Information Theory, vol. 44, no. 5 (1998), pp. 1897–1905 (see also Proc. Crypto 95, LNCS 963, Springer-Verlag,Berlin, 1995, pp. 452–465).

[7] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, A Secure, Robust Watermark for Multimedia, Information Hiding, LNCS 1174, Springer-Verlag, Berlin, 1996, pp. 185–226.

[8] 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," in Proc. IEEE GLOBECOM, Nov. 2006, pp. 1–5.

[9] "Youtube - Broadcast Yourself," Available at: http://www.youtube.com/

[10] "MSN Video," Available at: http://video.in.msn.com/

[11] R.S. Naini, and Y. Wang, "Sequential traitor tracing," IEEE Trans. On Information Theory, vol.49, no.5, pp. 1319–1326, 2003.

[12] K. Matsui, Basic knowledge of digital watermark, Morikita Shuppan,1998.

[13] B. Turnbull, "Important legal developments regarding protection of copyrighted content against unauthorized copying," IEEE Comm. Magazine,vol.39, no.8, pp. 92–100, Aug. 2001.

[14] D. Kundur, and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proc. of the IEEE, vol.92, no.6,pp. 918–932, June 2004.

[15] D. Boneh, and M. Franklin, "An efficient public key traitor tracing scheme," Advances in Cryptology - Crypto'99, pp. 338–353, 1999.

[16] R. Duda, P. Hart, and D. Stork, Pattern Classification(2nd ed.), John Wiley & Sons, 2000.

[17] K. Matsuda, H. Nakayama, and N. Kato, "A Study on Streaming Video Detection using Dynamic Traffic Pattern," IEICE Transactions on Communications (Japanese Edition), Vol. J19-B, No. 02, 2010.