Traitor tracing and secure transmission of files in networks

M. Dhana Sundari, G. Abirami, Linda Joseph
School of Computing Sciences and Engineering, Hindustan University

***Abstract*—Today in the competitive world transferring of files from on source to another destination without attacks is a challenging one. we can achieve easily by traitor tracing method.It is a copy right detection system which works by tracing the source of leaked files rather than by direct protection.when a copy of it is leaked to the public,the distributor adds a unique value to each copy given out. Watermarking is the key technology adopted by contemporary methods has many limitations and does not realistic for real time applications like video conference systems-learning systems,remote diagnosis systems and so on. But in proposed system, it can watch all the process from source to destination.**

***Keywords*—Digital Rights Management(DRM), traitor tracing, watermarking, digital finger printing.**

I. INTRODUCTION

Traitor tracing schemes were introduced to combat the typical piracy scenario whereby pirate decoders (or access control smartcards) are manufactured and sold by pirates to illegal subscribers. Those traitor tracing schemes, however, are ineffective for the currently less common scenario where a pirate publishes the periodical access control keys on the Internet or, alternatively, simply rebroadcasts the content via an independent pirate network. This new piracy scenario may become especially attractive (to pirates) in the context of broadband multicast over the Internet. A DRM system enables the secure exchange of intellectual property, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks.DRM allows content owners to distribute securely to authorized recipients and gives them control over the whole distribution chain.

In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

In *visible* digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In *invisible* digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of communication between individuals. An application is the copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in *source tracing*. A watermark is embedded into a digital signal at each point of distribution.

II.EXISTING SYSTEM

Existing System 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 L_C and L_W, respectively, the total load to deliver content which has traceability of traitors should be at least $N*(L_C+L_W)$. Here, N is the number of content users. It caused problems over the network because of unclear network environments and users.

The drawbacks of existing system includes possibilities of various attacks such as removal attack ,copy attack and sensitivity attacks. It is very complex to embed separate watermarks to every individual users and also difficult in real time applications.

In traitor tracing method using watermarking ,after receiving the contents user1 sends watermarking informations to s1,and user 2 sends same watermarking informations to s1.This concludes that the content is secondarily delivered from user1 to user2.

III.PROPOSED SYSTEM

The proposed method can determine who is watching the streaming content and whether or not a secondary content delivery exists. This information can be also used with general methods to construct a more practical traitor-tracing system. A method to cope with random errors and burst errors has also been investigated. It can watch all the process until it reaches the destination. A six digit code is sent to the destination via mail or Sms which is derived from the random generator algorithm and finally the file is read by pressing fingerprints in digital fingerprint reader. This code is generated randomly by pseudo random generator algorithm and this not be traited by anyone.

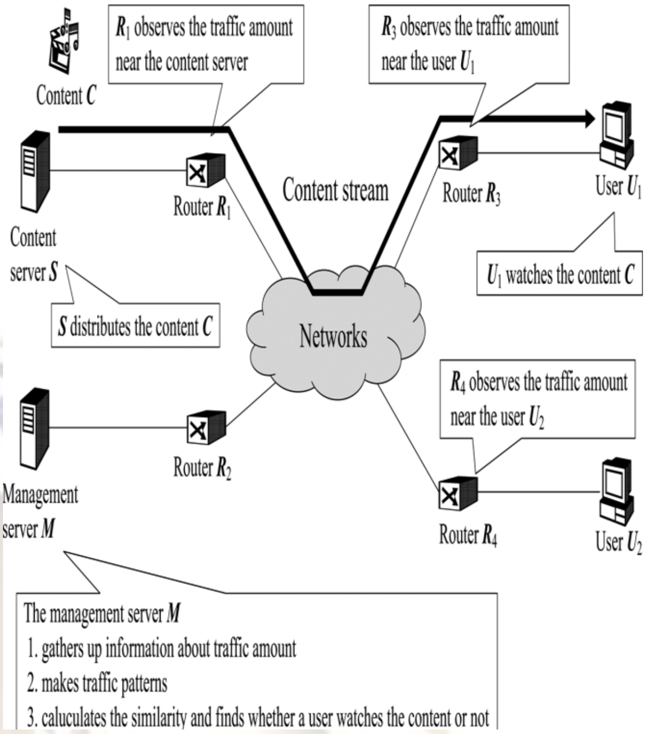
It helps to oversee the flow of contents and know who is watching them without monitoring the streaming data. This reduces not only the security risk on theft by a third party but also by the administrator. It has clear picture about network & its Path**.**

IV.ARCHITECTURAL DESIGN

Assume that the number of multiplications conducted in the calculation of similarity is , M.The total number of multiplications conducted in the proposed method is about (S-U)+1×M .

1. Here, S and U are the lengths of the server-side traffic pattern and the user-side traffic pattern, respectively.
2. M is a constant, which depends on U.
3. This calculation cost is much less than the cost of encoding and watermarking.

The content server S distributes the content C. Both users U1 and U2 receive the content C . The routers R1, R3, and R4 observe the amount of traffic. Router R1 monitors the flow of the content server S and sums up the sizes of packets. Here, the proposed system makes use of packet filtering about IP addresses to specify the content server's flow.The obtained information at Routers is sent to the management server M with protocols, such as Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP).


R_1 observes the traffic amount near the content server
R_3 observes the traffic amount near the user U_1
Content C
Content server S
Router R_1
Content stream
Router R_3
User U_1
U_1 watches the content C
S distributes the content C
Networks
R_4 observes the traffic amount near the user U_2
Management server M
Router R_2
Router R_4
User U_2
The management server M
1. gathers up information about traffic amount
2. makes traffic patterns
3. caluculates the similarity and finds whether a user watches the content or not

IV.LITERATURE SURVEY

A. Traitor tracing

If some digital content (e.g., a music clip) is encrypted using the public key and distributed through a broadcast channel, then each legitimate user can decrypt using its own private key. Furthermore, if a coalition of users collude to create a new decryption key then there is an efficient algorithm to trace the new key to its creators. Hence, our system provides a simple and efficient solution to the "traitor tracing problem"

In sequential traitor tracing scheme the content is broken into segments and marked so that a re-broadcasted segment can be linked to a particular subgroup of users. Mark allocation for a segment is determined when the re-broadcast from the previous segment is observed. They showed that by careful design of the mark allocation scheme it is possible to detect all traitors.

B. Video Fingerprinting

The main objective of fingerprinting and encryption in a DRM context is to protect video content from a set of attacks applied by one or more attackers. We define an attacker as any individual who attempts to use a given piece of content beyond the terms, if any, negotiated with the content provider. Common attacks on video data include illegal access and tampering. Our work focuses on the problem of piracy, the illegal duplication and redistribution of content; we call such an attacker a pirate. Overall, the objectives of this paper are twofold: 1) to present a state-of-the-art review and tutorial of the emerging areas of video fingerprinting and encryption highlighting design challenges for multicast environments; 2) to propose the approach of *joint* fingerprinting and decryption (JFD) to establish a better compromise between practicality and security for DRM applications.

C. Digital Fingerprinting

Digital fingerprinting is a technique for preventing unauthorized redistribution of multimedia content by embedding a unique identifying signal in each legally distributed copy. When an illicit copy is discovered, the embedded fingerprint can be used to identify the guilty user. A class of powerful attacks against such fingerprinting systems are collusion attacks by a group of users who may attempt to create a version of the content that cannot be traced back to any of them.

V.MODULE DESCRIPTION

A. Processing data from one to another

In this module, Traitor-tracing methods use digital watermarks and encryption keys to observe propagation of the content .The concept of general traitor tracing is to assign content with an individual identity. Ideally, watermarks embedded in the content are different from one other. A large amount of computations to encode many contents and to embed many watermarks. Since these costs are critical for realtime streaming, the reduction of these computations has been attempted.The file is transferred according to priority scheduling.

B. Analysis of Hacker and Digital Graph

In this module, DRM analyzes the interrupted person. Consequently, when the watermark is used over networks, it causes some problems because of unclear network environments and users. It is desirable to interoperate with a method to find suspicious content distributions without watermarking.

If the graph is above the centre line means someone is hacking and if the graph is below the centre line means no one is hacking the content.

C. Finding the interrupt by DRM

In this module, it does not require any additional computation cost at the content server.Instead,we place a management server to calculate the similiarity of traffic patterns.When we assume that the total number of multiplications conducted in the calculation of similiarity is M,the total number of multiplications conducted in the proposed method is about (S-U+1)*M.This calculation cost is much less than the cost of encoding and watermarking.

D. Generation of six digit code and fingerprinting

The six digit code is designed by the pseudo random generator algorithm.In this algorithm the code is generated randomly and it is sent to the destination via SMS or mail .When the content is sent to the user, DRM detects the traitor in between the process.

Digital Fingerprinting is a technique in which software identifies, extracts and then compresses characteristic components of a video enabling that video to be uniquely identified by its resultant fingerprint. Video fingerprinting is technology that has proven itself to be effective at identifying and comparing digital video data

Instead of username and password ,the client has to give thumb print to open the application.

VI.CONCLUSION

Sequential traceability schemes can be seen as a a step between static and dynamic schemes.The attack model in sequential schemes and dynamic schemes are the same and is different from a static traceability schemes. Traitor-tracing technology is one of these technologies and is used to observe the usage of content. General tracing methods have limitations, because of a high load to produce many contents and the watermark’s limitation. To advance the security of content delivery, we proposed a method, which takes advantage of the traffic pattern. To evaluate the performance of the proposed method, simulations and actual experiments were conducted. Finally, we obtained satisfactory results, verifying the effectiveness of our approach.

Furthermore, the most effective way an attacker can manipulate against our system is that the VBR content is changed into a constant bit-rate stream. This is analogous to copying the content into a USB memory and bringing it out from the server illegally.

VII. REFERENCES

1. O. Berkman, M. Parnas, and J. Sgall. E±cient dynamic traitor tracing. to appear at SODA 2000, 2000.
2. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. In Advances in Cryptology - CRYPTO'95, Lecture Notes in Computer Science, volume 963, pages 453{465. Springer-

Verlag Berlin, Heidelberg, New York, 1995.
3. B. Chor, A. Fiat, and M. Naor. Tracing traitors. In Advances in Cryptology - CRYPTO'94, Lecture Notes in Computer Science, volume 839, pages 257{270. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
4. I. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Transaction on Image Processing, Vol. 6 no. 12:1673{1687, 1997.
5. A. Fiat and M. Naor. Broadcast encryption. In Advances in Cryptology-CRYPTO'93, Lecture Notes in Computer Science, volume 773, pages 480{491. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
6. D. Kundur and K. Karthik, “Video fingerprinting and encryption principles for digital rights management,” Proc. IEEE, vol. 92, no. 6, pp. 918–932, Jun. 2004.
7. B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” IEEE Trans. Inf. Theory, vol. 47, no. 4, pp. 1423–1443, May 2001.
8. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, “Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications,” IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 573–586, May 1998.
9. M. Barni and F. Bartolini, “Data hiding for fighting piracy,” IEEE Signal Process. Mag., vol. 21, no. 2, pp. 28–39, Mar. 2004.
10. 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.
11. 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.
12. B. N. Park, W. Lee, and J. W. kim, “A license management protocol for protecting user privacy and digital contents in digital rights management systems,” IEICE Trans. Inf. Syst., vol. E88-D, no. 8, pp. 1958–1965, Aug. 2005.
13. Y. Matias and A. Shamir, “A video scrambling technique based on space filling curves,” in Proc. Advances in Cryptology (CRYPTO’87), 1988, vol. 293, pp. 398–417.

.

M.Dhana sundari, Chennai, 19.08.1989, M.E Computer science and engineering, School of Computing Sciences and Engineering, Hindustan University, Chennai, Tamil Nadu, India.

G.Abirami,Chennai,27.05.1983, M.E Computer science and engineering, School of Computing Sciences and Engineering, Hindustan University, Chennai, Tamil Nadu, India.

Linda Joseph, Chennai, Assistant Professor, School of Computing Sciences and Engineering, Hindustan University, Chennai, Tamil Nadu, India.