RESEARCH ARTICLE OPEN ACCESS

Peer-to-Peer content distribution using automatically recombined fingerprints

J.Murugeswari, C.Merlin Pauliesther
PG-student, Dept of IT Assistant Professer, Sathyabama University Chennai, India Dept of IT Sathyabama University Chennai, India

Abstract
Due to the recent advances in broad-band network and multimedia technologies, the distribution of multimedia contents are increasing. This will help a malicious party to duplicate and redistribute the contents; hence the protection of the ownership is required in multimedia content distribution. The encryption of content cannot solve the issue, because it must be ultimately decrypted at genuine users who have legal authority to distribute content. Therefore, additional protection mechanisms are needed to discourage unauthorized redistribution. One of the mechanisms is to generate the fingerprinting of multimedia which enables a seller to trace illegal users by embedding identification information into the content. The research on fingerprinting techniques is classified into two studies: collusion resistant fingerprinting systems and cryptographic protocol. Since each user download content with his/her own fingerprint and content is a little different. If users collect some of them, they try to find the difference and modify/delete the embedded information. Unicast transmission is applied in multimedia content distribution which will be give more security to buyers. Merchant will create number of seed buyers who need to distribute the content to child buyers. All the seed buyers should be online to distribute the content. The seed buyer and child buyer fingerprint are need to store in database which will be required to find the illegal redistribution.

Index Terms: recombined fingerprinting, cryptographic, content uploading and splitting

I. INTRODUCTION

The segments of the file are downloaded from other users and are expected to share with other user as well in peer-to-peer content distribution network [10]. The number of users is increased in peer-to-peer network and that will increased insecure between sender and receiver for content distribution.The cached copy of the content is located in distributed locations will be more availability of content distribution.The more availability of the content will be added advantage and able to send more users by single multicast transmission [9]. But this will be not secure if the content is very confident and need authorization to download the content. In this situation the unicast transmission will be more secure for sending document to each receiver separately [9]. In unicast transmission is to send fingerprint of the content to each receiver and this will help to find illegal redistribution [9].The anonymous fingerprinting is used for content distribution. In anonymous fingerprinting the merchant is not able to find fingerprint of the buyer that will give more security and privacy of the buyer. Implementing more security in content distribution will be burden to maintain more powerful server and increasing costly part of the protocols. The proposed method is to save bandwidth and effectively uses of CPU time in peer-to-peer network.

II. RELATED WORKS

The contents are shared to other user through P2P network is called content distribution. The watermarked content is obtained by both buyer and seller through asymmetric fingerprinting protocol [7]. If the seller extracted fingerprinting of the buyer and he/she is not able to do illegal distribution. Only Buyer is able to obtain his own fingerprinting from asymmetric protocol [7]. The contents are divided into different fragments and then distribute in network. The hash code will be appended with each fragments of the content and distributed to other users. The destination will receive the fragment from different source and merge with single content by identifying binary sequence of fingerprinting and hash code. The hash code of the each fragment is same by identifying the unique file. The destination should not identify which fragment coming from which source. So the following transaction should be captured and monitor illegal redistribution [9].

i) Hash code which is retrieved by child from parent
ii) Parent and child pseudonyms
iii) Date of transaction

A child is download fragments of the content from several parents. So the numbers of transactions are captured based on number of fragments in the content [9]. The transaction is not maintained which fragment is coming from which parent. This will

improve the privacy of the buyer. Redistribute the multimedia content to an unauthorized user outside its network is called content leakage.DRM and watermarking techniques are used to find a content-leakage in multimedia content distribution over the peer-to-peer network. Security is more important in content distribution over peer-to-peer network. A binary sequence of fingerprinting is separate into different piece of binary data and embedded into each content distribution.

A. Issues in Existing System

1) The tracing process is more difficult to maintain and manual process is required.
2) Involving more than one proxy for downloading and there is possibility whole fingerprinted copy of a buyer and illegally re-distribute that copy.
3) All the participant (buyers) need involve traitor tracing collaborating system implementation.
3) Due to security issues the entire participant (buyers) will not collaborating traitor tracing system.

III. MOTIVATION

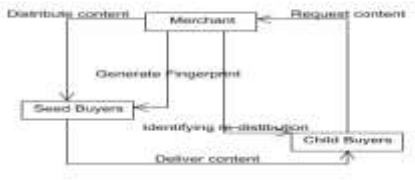
The distribution of the content to the authorized buyer by providing more security that will give privacy for each buyer. The system is automatically finding the illegal re-distribution by using traitor tracing protocol that will make the use of new system by more number of buyers and sellers. The system also identifies the illegal users and blocks those users will make confident level to buyer and seller.

IV. PROPOSED SYSTEM

The proposed system of this project is to perform recombined fingerprint with efficient, scalable, privacy-preserving and P2P-based fingerprinting system. Although the system proposed in this paper uses public-key encryption in the distribution and traitor tracing protocols, it must be taken into account that this encryption is only applied to short bit strings, such as the binary fingerprints and hashes, not to the content. The fragments of the content are encrypted using symmetric cryptography, which is much more efficient. The proposal in is more attractive, since embedding occurs only for a few seed buyers and the fingerprint of the other buyers are automatically generated as a recombination of the fingerprints of their "parents" in a graph distribution scenario. However, the traitor tracing protocol presented in those references requires an expensive graph search and disturbs a few honest buyers who must co-operate with the authority to identify the source of an illegal re-distribution.

A. Advantages of proposed system

1) To provide privacy for each buyers.
2) Recombined fingerprint for each buyers, for every transaction.
3) Identifying illegal re-distribution using traitor tracing protocol.
4) Identifying the illegal redistributing buyers.
5) Adding each illegal buyer to the block list.



V. IMPLEMENTATION

The proposed system of this project is divided into three major modules and described as below.

1. Content Uploading and Splitting
2. Generate Fingerprint and Distributing
3. Identifying illegal redistribution

Content Uploading and Splitting:

In this module, we have to create merchant, seed buyers and child buyers. Each buyer can be identified by their own pseudonyms. After all nodes has been created merchant will distribute the multimedia content to seed buyers. For distribution, merchant upload any of the multimedia content from their folder. That multimedia content has been splitted based on content size.

Generate Fingerprint and Distributing:

Once content has been splitted, it has to be distribute to number of seed buyers. Merchant generate random fingerprint for each multimedia content before distribute. That fingerprint must be maintained in database for identifying illegal redistribution. Merchant embedded part of fingerprint into the splitted content and then they distribute. Merchant checks the status of the seed buyers before distribution. If particular seed buyers are in offline means, merchant does not distribute the content. After particular seed buyers receive the splitted content, they send the content to requested child buyers.

Identifying illegal redistribution:

In the module, we have to identify the illegal re-distribution. Once a child buyer receives particular content from seed buyers, they access the content only their own use. In case any child buyers trying to redistribute the multimedia content means, transaction monitor has to monitor those illegal distributions. To identify illegal re-distribution, transaction monitor uses traitor tracing protocol. Using this protocol we are identifying the redistribution. For privacy preserving, we maintain the buyers fingerprint and pseudonyms for each buyers.

Database Design:

Table Name: MERCHANT

COLUMN NAME	DESCRIPTION
CNTNAME	Multimedia Content name or file name
CONFIN	Fingerprinting

Table Name: SEED_BUYER

COLUMN NAME	DESCRIPTION
SDNAME	Seed buyer unique identifier
SDENC	Seed buyer encryption data of key value
SDFIN	Seed buyer fingerprinting
SDHASH	Seed buyer hash code
DATE	Date of content distribution
CONNAME	Content name
UPFIN	Updated fingerprinting
RECVCON	Relative File path

Table Name: CHILD_BUYER

COLUMN NAME	DESCRIPTION
CDNAME	Child buyer unique identifier
CDENC	Child buyer encryption data of key value
CDFIN	Child buyer fingerprinting
CDHASH	Child buyer hash code
DATE	Date of content distribution
CONNAME	Content name
ILLEGALDIS	Illegal identification

Sample Output:

VI. CONCLUSION

In this paper, we discussed about the implementation of the fingerprinting protocol based on public key cryptosystems.Thehash message authentication code is used to construct binary code and that will be fingerprint of the content.The fingerprint is recombined and generates automatically from their parent and embedded with content distribution. The RSA algorithm is used to generate private and public key value and it is used to identify authorized users. This system will give more security to buyers and sellers who have distributed multimedia content through online.

REFERENCES

[1] Hiroki Nishiyama, Senior Member, IEEE, Desmond Fomo, Student Member, IEEE, Zubair Md. Fadlullah, Member, IEEE, and Nei Kato, Fellow, IEEE, "Traffic Pattern-Based Content Leakage Detection for Trusted Content Delivery Networks".

[2] David Meg´ıas, Member, IEEE , "Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints"

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," Advances in Cryptology-CRYPTO'95, LNCS 963, Springer, pp. 452-465, 1995.

[4] Y. Bo, L. Piyuan, and Z. Wenzheng, An efficient anonymous fingerprinting protocol. Computational Intelligence and Security, LNCS 4456, Springer, pp. 824–832, 2007.

[5] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," Asiacrypt 2000, LNCS 1976, Springer, pp. 415–428, 2000.

[6] C.-C. Chang, H.-C. Tsai, and Y.-P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," Computers & Security, vol. 29, pp. 269–277, Mar. 2010.

[7] J. Domingo-Ferrer and D. Meg´ıas, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community," Computer Communications, vol. 36, pp. 542–550, Mar. 2013.

[8] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. Burlington MA: Morgan Kaufmann, 2008.

[9] David Megras .Joesp Domingo-Ferrer. "privacy-Aware Peer-to-Peer Content Distribution Using Automatically Recombined FingerPrints"

[10] SAURABH AGGARWAL, JOY KURI and CHANDAN SAHA. "Give-and-take based peer-to-peer content distribution networks"