IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 3, March 2016*

# Peer to Peer Multimedia Content Distribution Using Automatically Recombined Binary Key

**Mrs. M. Rajeswari[1], M. Harini[2], K. Kiruthika[3], S. Nandhini[4]**

Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[1]

Student, Department of Information Technology, Panimalar Institute of Technology, Chennai, India[2, 3, 4]

**Abstract:** With increasing number of recent advancement in multimedia technologies, the distribution of multimedia contents have increased to a greater extend. Protection of ownership is required in the distribution of multimedia contents due to enormous increase in duplication and redistribution of contents. Encryption and decryption of contents also becomes cumbersome due to the usage of large amount of data and communication bandwidth to transfer data. In order to control unauthorized redistribution we generate binary key for multimedia contents. This enables us to trace the illegal users by using traitor tracing protocol. Merchant will create number of seed buyers who needs to distribute the content to the child buyers. Each seed buyer will be provided with his/her own binary key. On distribution of multimedia contents to the child buyers the binary key of different seed buyers are automatically recombined and the database is maintained. In case of any illegal distribution, merchant will block the illegal user and will not respond to the particular user.

**Index Terms:** Anonymous Binary Key (Fingerprinting), RSA, HMAC, FFMP, Transaction Monitor, Traitor Tracing Protocol.

## I. INTRODUCTION

In the peer-to-peer network, since the number of users has increased, an insecure distribution of contents between sender and receiver has also increased. Under the peer-to-peer network the fragments of the file are downloaded by different users from the merchant and this user will distribute the content to some other user. This has increased the availability of content and can be send to many users by single multicast transmission. But while sending an authorized content, simply transmitting the contents to different users cannot be secure. So, in order to resolve this problem we use unicast transmission. In unicast transmission the merchant allocate binary key for each receiver and this helps finding the illegal redistribution using this binary key. The anonymous way of generating binary key is being used for content distribution. This is the most convenient strategy to protect both the buyers' privacy and owner's rights since only the buyer obtains the binary key copy of the content, making it impossible for the merchant to illegally redistribute the content. It preserves the anonymity of the buyer's identities with respect to the merchant. The anonymous scheme also eliminates the homomorphic property of public-key cryptography. The practical way of implementing the homomorphic technique is difficult due to large amount of data usage and ultimately results in an increasing communication bandwidth required for transferring the contents. This eventually results in a need of maintaining a more powerful server and increase in the cost of the protocols. By using the anonymous technique this drawbacks can be eliminated and the use of CPU time in the peer-to-peer network can be maintained much more effectively. Illegal redistribution of the multimedia can be reduced by using this anonymous technique with the help of this unique binary key generation for each user.

In our proposed system we identify the illegal users by using the traitor tracing protocol and additionally we block this illegal user from further accessing any other multimedia contents from the server.

## II. SYSTEM OVERVIEW

The architecture of the proposed system is all about providing security to multimedia content distribution and protecting it from illegal users under a peer-to-peer system. The proposed system involves the steps like content uploading, Generation of the binary key and then followed by the distribution of contents to the buyers, identification of illegal users and then blocking of the illegal users. Thus this system is privacy-preserving, efficient, and scalable to the users to transfer the multimedia content. Thus we have solved all the drawbacks of the previous works with much efficiency.

In the present scenario there are many systems which involve the protection of the multimedia content. But still the privacy of the users are not kept in a secured manner and there are much chances of illegal distribution with use of some others binary key. In the proposed system we eliminate all this drawbacks by using an anonymous way of binary key generation. Under this techniques contents are send in form of frames, of hash code embedded with binary key to different buyers. From these two or more seed buyers the child buyers get the contents and their parent's binary key are also combined and this resembles as the child buyers binary key.

The traitor tracing protocol is also being used which helps in the tracing of the illegal users before being distributor. Knowing the illegal user the merchant can easily block this illegal user from further requesting for any other multimedia contents.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 3, March 2016*

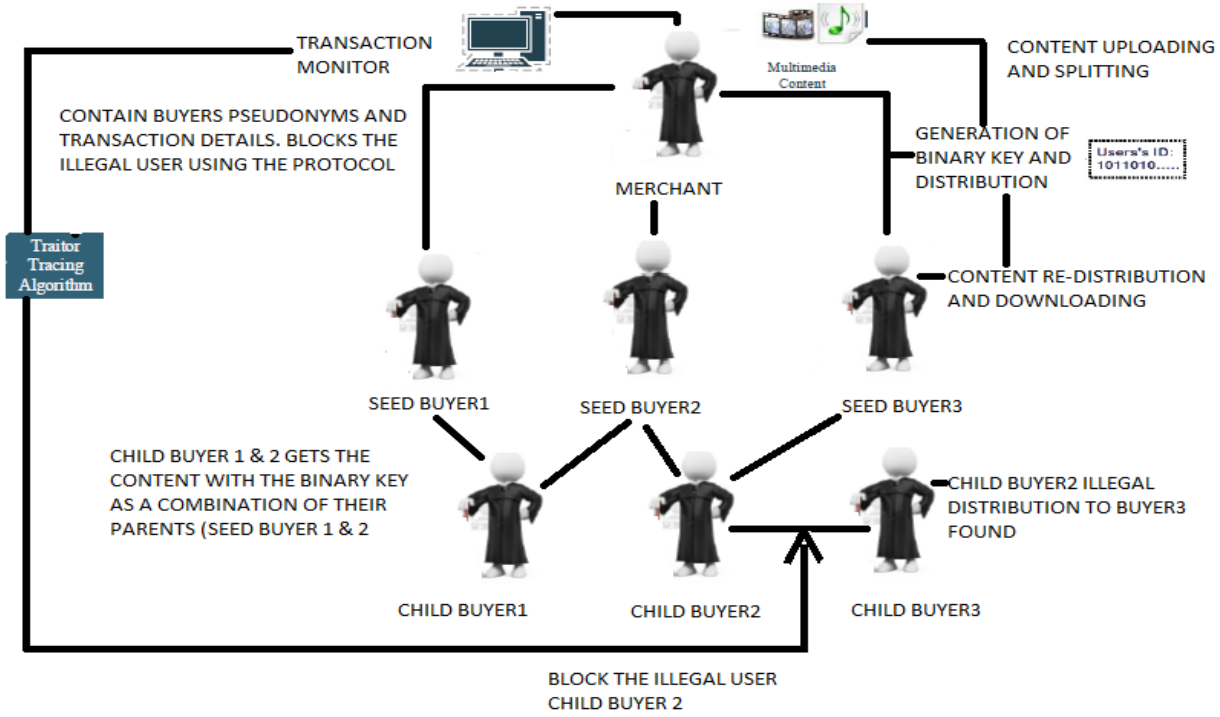



**Fig.1 THE ARCHITECTURAL VIEW OF THE PROPOSED SYSTEM**

A separate database is also maintained for the transaction of various users and only the pseudonyms are being used to provide security. The illegal distributor list will also be maintained separately for the use of merchant to block them from accessing the multimedia contents and their request is being denied.

## III. RELATED WORKS

There were many previous works on multimedia content distribution as in paper **"David Megias, "Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints," IEEE, Vol,12, N0.2, March/April, 2015."**The contents are normally divided into several fragments and each buyer is assigned with a Random binary sequence (generated by the merchant) also called as segments. These segments are totally combined to form a binary key. The merchant distribute these fragments to different seed buyers with their binary key embedded with the fragments. The child buyers get the contents from the seed buyers as a combination of binary key of two or more seed buyers.

The child buyer gets the fragments at least from two seed buyers or more. The fragments from different seed buyers are combined to get the overall multimedia file. Multimedia contents are thus obtained as a recombination of different seed buyers. The communication between the seed buyers and the child buyers are anonymous and thus the anonymity of different users are being maintained secure. Pseudonyms of different seed and child buyers are being provided by the merchant. The transaction monitor which records the pseudonyms and also contain the transaction list of different buyers. But the real identities of the buyers are known only by the merchant.

At the time of illegal distribution a search is made through the distribution graph. **Y. Bo, L. Piyuan, and Z. Wenzheng, "An efficient anonymous fingerprinting protocol," in Proc. Int. Conf. Comput. Intell. Security, 2007, pp. 824–832.**Under this each buyer binary key is being check and their correlation between their binary key and that of the illegal re-distributor is checked. The buyer with maximum correlation is being found as an illegal re-distributor under this process of traitor tracing protocol. Butbacktracking is very complicated under this process and it becomes very difficult to find the actual re-distributor. Security of the multimedia contents is more important in a peer-to-peer content distribution. The child buyers download the fragments from different buyers and transaction is also maintained basedon the number of fragments being send. The transaction do not contain the details about the parent of each fragment which results in the privacy of the buyers.**C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 13, no. 12, pp. 1618–1626, Dec. 2004.**Watermarking technique was also used to find the illegal distribution of the multimedia contents outside the peer-to-peer network. This system thus resulted in the anonymity under the transaction of the buyers. The traitor tracing protocol also helpful in finding the illegal distribution of the multimedia contents.

## ISSUES UNDER EXISTING SYSTEM

1) Tracing process is normally cumbersome and results in the participation of innocent buyers (since the size of the binary key is seen as illegal distributor-this cannot be true in all cases).

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 3, March 2016*

2) Backtracking is practically very difficult to handle.
3) Despite the use of different proxies to download the content/some proxies may collude to reconstruct the binary key of the buyer and illegally re-distribute that copy. This also will involve innocent buyers.

## IV. PROPOSED SYSTEM

The proposed system of this paper is to protect multimedia contents from illegal distribution with a help of automatically recombined binary keys and to block illegal users from further requesting the contents. ThisP2P system is aimed at providing an efficient, scalable and privacy-preserving content distribution to the users. The module involves mainly the content uploading in a P2P network and generation of binary key and distribution. Then it involves the identification of the illegal users and blocking them.

### A.CONTENT UPLOADING AND SPLITTING

In this module our first step is the network formation. Under this we create merchant, seed buyers, child buyers. Each buyer is identified only by his pseudonyms without revealing their actual details.

### MERCHANT:

It acts as the head of the entire network. All the transactions under this P2P network is being handled by this merchant. Merchant only has the authority to know the personal details of each buyers under this network. It has the rights to block any illegal re-distributors.

### SEED BUYER:

The seed buyer acts as the sub server below the control of the merchant. All the contents from the merchant are distributed to other users using this seed buyers. But the orders to distribute the contents are taken only by the merchant based on the user's request

### CHILD BUYER:

The child buyer is the buyers belie the seed buyers. They just need to give request to the merchant for any type of multimedia file. Later the merchant with the help of the seed buyers send the contents to the child buyers. At the time of creation the child buyers are provided with the public key, private key and pseudonyms. After all this is set the merchant for the distribution purpose uploads some multimedia content from its folder. The contents are also splatted in the form of fragments.

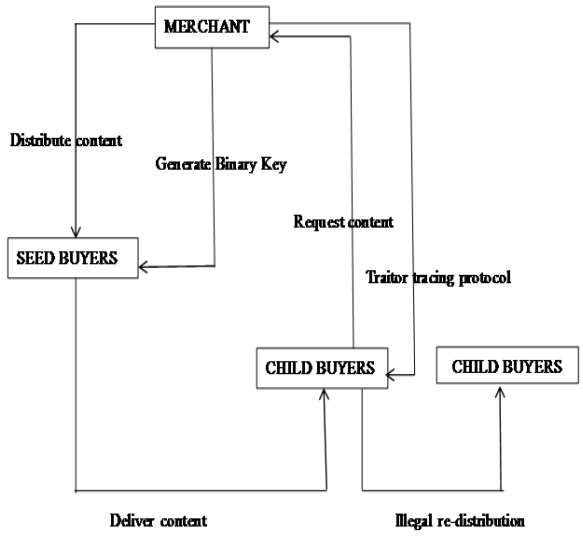



**Fig.2 BLOCK DIAGRAM**

### B.GENERATING BINARY KEY AND DISTRIBUTINGTHE CONTENTS

The content that are being splatted into the form of fragments is being converted in the form of hash code and a binary key is provided for the content. Thus each seed buyer will have a separate unique binary key to identify from where the content is being redistributed.

After the binary key is generated it is being send to the respective seed buyer. When the child buyer request for the contents to the merchant, it request the seed buyers to send the contents. Normally the child buyer will get his content from two or more seed buyers and their 'parent' binary keys are automatically recombined.

### C. IDENTIFYING THE ILLEGAL RE-DISTRIBUTION

This module aims at finding the illegal users. At times the content received by the child buyer from the seed buyer can be misused. Without permission of the merchant some child buyers may try to redistribute the contents to some other buyers. But this illegal transaction can be maintained by the transaction monitor with the help of the traitor tracing protocol. This protocol helps us to identify the illegal redistribution. The pseudonyms and the binary key is used to identify which buyer has illegally distributed the multimedia content

### D.BLOCKING OF THE ILLEGAL BUYERS

This module involves blocking the illegal Redistributors from further accessing the multimedia content. Now the binary key can be used to find the parent that is the seed buyer of the illegal distributor. After finding the perfect match of binary key that particular seed buyer is named as attacker. Further request by this buyer will not be replied by the merchant. The databases also contain the details of this attacker and help the merchant to block the attackers.

## V. IMPLEMENTATION

The proposed system is mainly used for identification of illegal users and blocking them. Both the phase can be either done under a smart phone or our PC. But under our project we have done using our Personnel computer.

### ➢ IDENTIFYING THE ILLEGAL USERS

This phase involves the identification of the illegal users of the multimedia contents. Suppose let's consider child buyer C207 is illegally transmitting contents (e.g. image) to another child buyer C014.At this time the traitor tracing protocol helps us detect this illegal user. This protocol checks the binary key embedded with each buyer's content and the illegal distributor is found. This can track a true illegal user with help of this binary key embedded with each fragments.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 3, March 2016*

At the same time the child buyer can't download the contents because it is found illegal. Thus the system provide us a much easier way to track the illegal user with less time and cost consumption. The data and communication usage for this system is also very low when compared with previous works.


Since C014 is not an authorised buyer the content and it never gets downloaded content. Thus the content is kept hidden from illegal buyers.



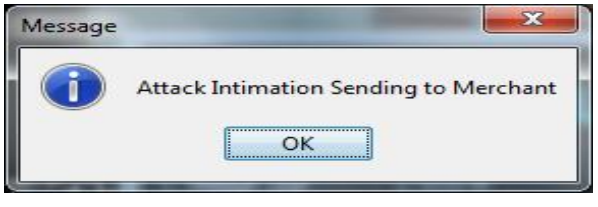

## ➢ BLOCKING OF THE ILLEGAL USERS

At times the seed buyer may also turn as an attackers. So at this case the illegal child buyer can be used to find that particular attacker. Suppose if C207 got contents from two seed buyers namely S525 and S545, the binary key of this seed buyers are checked with C207.Thus the attacker can also be found very easily.

Finding the attacker the merchant has the rights to block them from further requesting and gaining the multimedia content. The database maintain the names(pseudonyms) of all this attacker and the merchant all have a list to block them from accessing any further contents. Thus it is very efficient and no innocent buyers gets trapped in this due to some irregular results of testing.





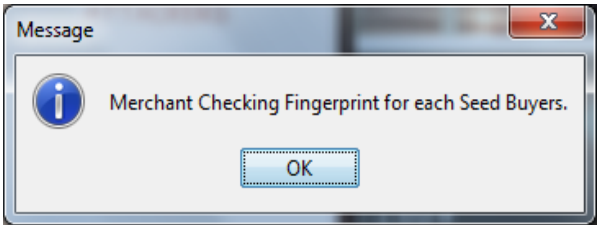


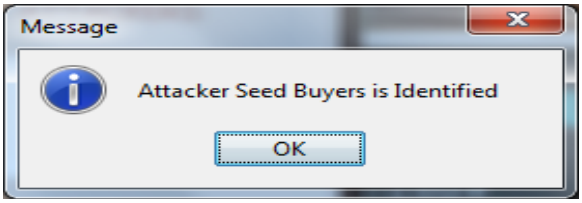
DOI 10.17148/IJARCCE.2016.53108

IJARCCE

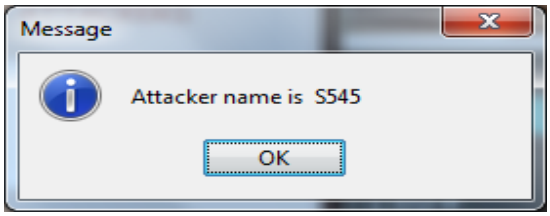
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 3, March 2016*




Att Attacker S545 is identified using the binary key of the child buyer C014.As soon as it found as the attacker its colour changes. It is not possible to find the attacker if the binary keys are not available and also the name of the buyer can be identified only with the help of the database. Later, the merchant stores the list of the attackers S545 in the block list. Thus the objective of this paper to block the illegal user is satisfied.





Merchant now stores the name of the attacker under the list ATTACKERS. The distribution of the content can also be blocked easily.

## VI. CONCLUSION

In this paper, we discussed about the implementation of the binary key protocol to form a perfect privacy-preserving system. The hash code and the binary key is used to keep the content in a secure manner. The binary key is recombined and generated automatically from their parents and it is being embedded in the content to be distributed. The illegal users are also being blocked, so number of such illegal users may be reduced. Thus this system provides more security to the buyers and the sellers of the multimedia contents.

## REFERENCES

1. David Megias, "Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints," IEEE, Vol,12, N0.2, March/April, 2015
2. Y. Bo, L. Piyuan, and Z. Wenzheng, "An efficient anonymous fingerprinting protocol," in Proc. Int. Conf. Comput. Intell. Security, 2007, pp. 824–832.
3. J. Camenisch, "Efficient anonymous fingerprinting with group signatures," in Proc. 6th Int. Conf. Theory Appl. Cryptology Inf. Security: Adv. Cryptology, 2000, pp. 415–428.
4. C.-C. Chang, H.-C. Tsai, and Y.-P. Hsieh, "An efficient and fair buyer-seller fingerprinting scheme for large scale networks," Comput. Security, vol. 29, pp. 269–277, Mar. 2010.
5. D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.
6. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington, MA, USA: Morgan Kaufmann, 2008.
7. R. O. Preda and D. N. Vizireanu, "Robust wavelet-based video watermarking scheme for copyright protection using the human visual system," J. Electron. Imaging, vol. 20, pp. 013022–013022-8, Jan.–Mar. 2011.
8. M. Fallahpour and D. Megıas, "Secure logarithmic audio watermarking scheme based on the human auditory system," Multimedia Syst., vol. 20, pp. 155–164, 2014.
9. S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, Dec. 2008.
10. M. Kuribayashi, "On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol," EURASIP J. Inf. Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.B.
11. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in Proc. 16th Ann. Int. Conf. Theory Appl. Cryptographic Techn., 1997,pp. 88–102.
12. B. Pfitzmann and A.-R. Sadeghi, "Coin-based anonymous fingerprinting,"in Proc. 17th Ann. Int. Conf. Theory Appl. CryptographicTechn., 1999, pp. 150–164.
13. J. Domingo-Ferrer and D. Megıas, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community," Comput. Commun., vol. 36, pp. 542–550, Mar. 2013.
14. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digitaldata," in Proc. 15th Ann. Int. Cryptology Conf. Adv. Cryptology,1995, pp. 452–465
15. D. Megıas and J. Domingo-Ferrer, "DNA-inspired anonymous fingerprinting for efficient peer-to-peer content distribution," in Proc.IEEE Congress Evol. Comput., Jun. 2013, pp. 2376–2383.
16. J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP J. Inf. Security, vol. 2007, pp. 20:1–20:7, Dec. 2007.