International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Automatically Recombined Fingerprints for Privacy Preserving In Improved Peer-To-Peer Multimedia Distribution

Radha Mothukuri[*1], Naidu.Lakshmibhavani[2], Padarthi.Niharika[3], Mandapalli.Sukanya[4]

[*1]Assistent Professor, Department of CSE , QIS College of Engineering and Technology, Ongole, Andhra Pradesh , India

[234]B.Tech, Department of CSE , QIS College of Engineering and Technology, Ongole, Andhra Pradesh , India

ABSTRACT

Unknown unique mark has been proposed as a helpful answer for the lawful dissemination of sight and sound substance with copyright insurance while saving the security of purchasers, whose characters are just uncovered if there should arise an occurrence of unlawful re-appropriation. Notwithstanding, the vast majority of the current unknown fingerprinting conventions are unreasonable for two principle reasons: 1) the utilization of complex tedious conventions and/or homomorphic encryption of the substance, and 2) a unicast approach for conveyance that does not scale for an expansive number of purchasers. This paper originates from a past proposition of recombined fingerprints which conquers some of these disadvantages. In any case, the recombined unique finger impression approach requires a mind boggling chart hunt down deceiver following, which needs the investment of different purchasers, and genuine intermediaries in its P2P conveyance situation. This paper concentrates on evacuating these disservices bringing about a productive, adaptable, security safeguarding and P2P-based fingerprinting framework.

Keywords : 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 uncast transmission will be more secure for sending document to each receiver separately [9]. In uncast 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].

Hash code which is retrieved by child from parent

Parent and child pseudonyms
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.

The main features of the preferred method are the following:

The content is divided into several ordered fragments and each of them is embedded separately with a random binary sequence. The binary sequence for each fragment is called segment and the concatenation of all segments forms the whole fingerprint.

The merchant distributes different copies to a reduced set of M seed buyers. The fingerprints of these buyers are such that their segments have low pair-wise correlations. The buyers other than the seed ones engage on P2P transfers of the content in such a way that each new buyer obtains fragments from at least two other Buyers. The total number of buyers is N M.

The communication between peer buyers is anonymous through an onion routing-like protocol using a proxy. The fingerprint of each new buyer is built as a recombination of the segments of its parents.

Proxies know the pseudonyms of source and destination buyers and they have access to the symmetric keys used for encrypting the multimedia content. A transaction record is created by a transaction monitor to keep track of each transfer between peer buyers. These records do not contain the embedded fingerprints, but only an encrypted hash of them. The fingerprints' hashes are encrypted in such a way that the private key of at least one parent is required for obtaining their clear text. The real identities of buyers are known only by the merchant. The transaction monitor records buyers' pseudonyms.

In case of illegal re-distribution, a search is required through the distribution graph. The search starts from the seed buyers and is directed by a correlation function between the traced fingerprint and the fingerprints of the tested buyers. These tested buyers must co-operate with a tracing authority to compute the correlation between their fingerprint and the one extracted from the illegally re-distributed file. The fingerprints' hashes recorded in the transaction monitor are enough to prevent buyers from cheating in this step.

At each step of the traitor tracing protocol, the buyer with maximum correlation is chosen as the most likely ancestor of the illegal re-distributor. This criterion is mostly right, but some incorrect choices may occur during the search process, requiring the exhaustion of a sub graph and backtracking.

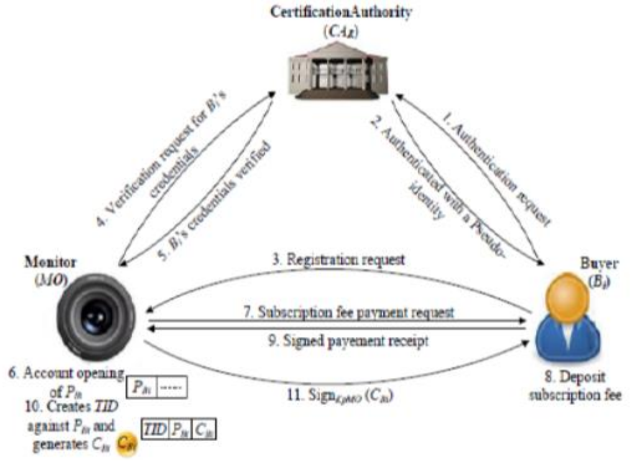
The search ends when perfect correlation is found between the fingerprint of the tested buyer and that of the illegally re-distributed file. If a buyer refuses to take a correlation test, the hash recorded

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 content is divided into several ordered fragments and each of them is embedded separately with a random binary sequence. The binary sequence for each fragment is called segment and the concatenation of all segments forms the whole fingerprint. The merchant distributes different copies to a reduced set of M seed buyers. The fingerprints of these the fingerprints' hashes are encrypted in such a way that the private key of at least one parent is required for obtaining their clear text. The real identities of buyers are known only by the merchant. The transaction monitor records buyers' pseudonyms. In case of illegal re-distribution, a search is required through the distribution graph. The search starts from the seed buyers and is directed by a correlation function between the traced fingerprint and the fingerprints of the tested buyers. These tested buyers must co-operate with a tracing authority to compute the correlation between their fingerprint and the one extracted from the illegally re-distributed file fingerprints of these.


CertificationAuthority
(CA_R)
1. Authentication request
2. Authenticated with a Pseudo-identity
3. Registration request
4. Verification request for B_i's credentials
5. B_i's credentials verified
Monitor
(MO)
Buyer
(B_i)
7. Subscription fee payment request
9. Signed payement receipt
6. Account opening of P_{Bi}
P_{Bi} ----
10. Creates TID against P_{Bi} and generates C_{Bi}
TID P_{Bi} C_{Bi}
11. $\text{Sign}_{K_{pMO}}(C_{Bi})$
8. Deposit subscription fee

The fingerprints hashes recorded in the transaction monitor are enough to prevent buyers from cheating in this step. At each step of the traitor tracing protocol, the buyer with maximum correlation is chosen as the most likely ancestor of the illegal re-distributor. This criterion is mostly right, but some incorrect choices may occur during the search process, requiring the exhaustion of a sub graph and backtracking. The search ends when perfect correlation is found between the fingerprint of the tested buyer and that of the illegally re-distributed file. If a buyer refuses to take a correlation test, the hash recorded in the transaction monitor can be used as evidence against her.

Advantages of Proposed System

This paper reviews the main features of the proposal suggested, highlights its main drawbacks, and suggests several significant improvements to achieve a more efficient and practical system, especially as traitor tracing is concerned, since it avoids the situations in which illegal redistributors cannot be traced with the proposal.

Furthermore, better security properties against potentially malicious proxies are obtained.

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.

This section analyzes the security and privacy properties of the proposed system according to the security model introduced. As detailed, attacks to the system may be classified as authentication/impersonation attacks, man-in the- middle attacks and protocol attacks. Authentication/ impersonation attacks should be overcome by using existing secure authentication protocols and are out of the scope of this paper. As man-in-the-middle attacks are concerned, there is no possibility of intercepting and decrypting the messages between a buyer and a proxy, since communications with the transaction monitor and the child buyer should also be attacked in order to obtain the session key used for encrypting the content. If the communication between the child buyer and the transaction monitor (Step 5 of Protocol 1) are strongly authenticated (e.g., using a Public Key Infrastructure), the possibility of a successful man-in the-middle attack can be neglected. The following sections deal with the security and privacy of the protocols proposed, first taking a formal approach and then with a description of more complex collusion attacks.

A. Formal Analysis of the Proposed Protocols

First of all, the security and privacy properties of Protocols 1 and 2 is analysed by means of two theorems (and their corresponding proofs).

1. Theorem 1: In Protocol 1, a malicious proxy trying to decrypt the fragments of the content would be detected.

Proof: If a malicious proxy tries to obtain the session key k by sending r to the transaction monitor there are two possibilities:

If the child buyer has already retrieved k from the database by sending the handle r to the transaction monitor, the register containing k would be either blocked or removed. Note that the transaction monitor is assumed to be honest for the management of the symmetric keys.

If the child buyer has not retrieved k from the transaction monitor, the proxy will obtain it, but the child buyer will find the corresponding register either blocked or removed. Then, the malicious behavior of the proxy can be reported to the authorities and the transaction monitor and the child buyer have enough information (such as pseudonyms and IP addresses) to identify the misbehaving proxy. Again, the assumption of honest behavior for the management of symmetric keys applies.

Hence, a malicious proxy trying to obtain k from r would be detected, since the register would be blocked either to the proxy or to the child buyer, raising an investigation. This completes the proof.

2. Theorem 2: By applying Protocol 2, an illegal re-distributor can be traced efficiently using a standard database search in the transaction monitor and it is not required to decrypt any of the fingerprints recorded by the transaction monitor. The output of the tracing protocol is the identity of at least one illegal re-distributor. Proof: If no collusion occurs, the fingerprint f would be first extracted by the tracing authority, which is trusted. Then the tracing authority would compute Egg= E (go, Kc) for each segment (using the public key of the transaction monitor), and finally obtain Ef after grouping the segments in sets of m consecutive elements and encrypting these groups with its public key Ka. After that, the transaction monitor, which is also trusted for transaction database search, would output the pseudonym of the illegal re-distributor. The pseudonym can be linked to the real identity by the merchant, who provides also a signed document that associates the real identity and the pseudonym. This completes the proof.

In case of collusion of several buyers, the extracted fingerprint would not be a valid codeword of the anti-collusion code used in the scheme. Then, the system described would be used: the encrypted hash Ehf =E (hf, Kc) would be searched instead of the encrypted fingerprint, where hf denotes the hash obtained applying the hash function to the traced fingerprint f. Thus, Protocol 2 would be used with the hash of the fingerprint instead of the fingerprint itself. As described, with a large enough hash space, hash collisions would be almost negligible and a traitor would still be identified in the vast majority of the cases. The requirement that the transaction monitor is trusted and returns the pseudonym of the buyer associated with the traced fingerprint (and not a different pseudonym) can be relaxed if a signature of the encrypted sets of segments of the fingerprint is provided by the proxies. These signatures can be verified using the public keys of the proxies. In that case, both the signatures and the pseudonyms of the proxies shall also be included in the registers of the transaction database to facilitate the verification of these signatures when required. B. Collusion Attacks on the Protocols This section discusses possible collusion attacks on the proposed protocols. 1. Buyer Frame Proofness As already discussed in, the merchant is not able to produce any buyer’s fingerprint by random guess due to the numerical explosion of the fingerprint space, even with a reduced number of seed buyers on the other hand, the transaction monitor has access only to the hashes of the fingerprints (not the fingerprints themselves without the private key of the authority). Since the hash function is not invertible, it is not possible for the monitor (even in coalition with the merchant) to reconstruct any buyer’s fingerprint. Possible collusions to disclose the specific fingerprint of an innocent buyer are the following:

- ✓ The tracing authority and the transaction monitor.
- ✓ All the proxies(for a transfer) and the transaction monitor.
- ✓ All the proxies (for a transfer) and the merchant.

In the first case, the authority and the transaction monitor may use their private keys to obtain the clear text of all the fingerprints. However, this possibility can be neglected since at least the authority must be trusted. In the second case, all the segments of the fingerprint could be decrypted using the private key of the transaction monitor, since the malicious proxies would not encrypt them with the public key of the authority. Also, the transaction monitor could collude with the proxies and use the session keys k to decrypt the fragments. Both possibilities would involve at least three malicious parties: all the proxies (two at least per each purchase) and the transaction monitor. In the third case, even if the transaction monitor does not provide her private key, a brute force attack segment by segment would be possible to reconstruct a buyer's fingerprint, because the number of different segments is small for each fragment (equal to M). Again, at least three malicious parties would be required: two (or more) proxies plus the merchant. Hence, the minimum coalition required to frame an innocent buyer is formed by three malicious parties (or two if one of them is the authority). Note that a coalition of the transaction monitor and the merchant is not enough to obtain the clear text of any fingerprint. As the proxies encrypt a set of m consecutive segments, and there are M possible values for each segment, the total number of combinations per set of consecutive segments is Mm. This avoids a brute force attack if m is reasonably large. For example, if M = 10 and m = 32, there would be 1032 possible combinations for each set of consecutive segments, what would be enough for security against a brute force attack if the segments were encrypted one by one (or grouped with a small value of m), the system would be vulnerable against a brute force attack for a collusion of the merchant and the transaction monitor. 2. Copyright Protection In order to ensure copyright protection, it is essential that the fingerprint embedded in each buyer's copy of the content and its encrypted version recorded by the transaction monitor is identical. If there is a way to cheat in the recorded fingerprint, the corresponding buyer would be able to re-distribute her copy illegally without any chance of being detected. As already remarked in, the content fragments are signed by the merchant from origin. The same approach can be used here for each encrypted segment of the fingerprint, making it impossible for a proxy to cheat about the fingerprint. The authority and the merchant could verify randomly, with some probability, the signatures of the set of contiguous segments reported by a proxy. If the signature was not verified, the proxy would be accused of forgery. Note that the fingerprints would still be protected since 1) only some sets of contiguous segments would be verified (not the whole fingerprint) and 2) those segments would still be encrypted with the transaction monitor's public key. However, a proxy may still try to get alternative fragments for the same position of the content by requesting them from different parents. That possibility would allow the proxy to cheat about the true fingerprint of the child buyer, since several correctly signed fragments would be available for him for the same content. This behavior can be avoided in several ways. For example, temporary records can be created in the transaction monitor by the parents to detect if a proxy tries to obtain two alternative fragments for the same content. 3. Buyers' Privacy

The identity of a buyer who has purchased a specific content could be revealed by a coalition of two parties: one of the proxies chosen by the buyer and the merchant (who can link her pseudonym to a real identity) or, similarly, the transaction monitor and the merchant. Better privacy could be achieved if, for example, the pseudonyms were encrypted by the proxies using the public key of the tracing authority. In that case, a coalition of the merchant and the transaction monitor would not be enough to break a buyer's privacy, but a coalition of a proxy and the merchant would still be enough. However, the merchant should not be interested, in principle, to break her client's privacy, since privacy would be one of the clear advantages of the proposed distribution system. Another threat to privacy is the fact that all anonymous communications between each child and each parent occur through a unique proxy. This means that this proxy has access to different pseudonyms (the parents' and the child's). This can be easily circumvented if more proxies are used in Protocol 1 between child and parent. With two proxies, each of them would know only the pseudonym of one of the parties (although they could still collide). With three or more proxies, only two of them would have access to different pseudonyms (either the parents' or the child's). Of course, increasing the number of proxies in each transfer would affect the efficiency of the system, since more communication burden would be required.

V. 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.

VI. 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-PreservingP2PMultimedia DistributionBasedonRecombined Fingerprints"

[3]. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," Advances in

[4]. Cryptology-CRYPTO'95,LNCS963,Springer, pp. 452-465, 1995.

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

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

[7]. 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.

[8]. 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.

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

[10]. David Megras .Joesp Domingo-Ferrer."privacy-AwarePeer-to-PeerContent DistributionUsingAutomatically Recombined FingerPrints"

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