Survey on Improved Privacy Preserving in Peer-to-Peer Multimedia Distribution

Sajna.N.S*,Annie.R.Das**

(*M.Tech student, Department of Computer Science and Engineering,Mohandas College of Engineering & Technology

Anad, Trivandrum

Email: nssajnashaan@gmail.com)

(**Asst.Professor,Department of Computer Science and Engineering,Mohandas College of Engineering & Technology

Anad, Trivandrum

Email: annierdas@gmail.com)

Abstract

The rapid popularity of network-based multimedia applications poses many challenges for multimedia content providers to provide efficient multimedia services. Recently, there are many research interests in providing efficient and scalable multimedia distribution service. When selling electronic content, the merchant would like each buyer to receive a same copy of the content fingerprinted with different serial number, in order to be able to trace redistributors should illegal redistribution happen. Fingerprinting schemes used to detect illegal redistributing multimedia data by enabling the original merchant of the multimedia data to identify the original buyer of a redistributed copy. Anonymous fingerprinting is a convenient solution for the legal distribution of multimedia contents with copyright protection while preserving the privacy of original buyers, whose identities are only revealed in case of illegal re-distribution happens.

Keywords*— *Anonymous fingerprinting, recombined fingerprints, P2p content distribution.

I. Introduction

Legal distribution of multimedia contents is a recurrent topic of research. Broadband home Internet access has enabled the growth of e-commerce, including direct downloads of multimedia contents. Keeping the fact, copyright infringement is one of the first threats to the multimedia content industry, Fingerprinting digital contents is well used technique along with this. fingerprinting with imperceptible mark in the distributed content (audio, pictures or video) to identify the content buyer. Instead of attached mark, the content is identical for every buyers, embedded mark will allow identifying the redistributors.

For scalability, unicast approach connection of merchant with convenient strategy is not good. Though broadcast distribution doesn't suits for fingerprinting applications because different fingerprints are required for various buyers to guarantee the traceability. The solution for that is Peer-to-peer distribution ,this technique blends some of the merits of the unicast and multicast solutions.

II. PEER TO PEER NETWORK

In a peer-to-peer network, every machine plays the role of client and server at the same time. In a peer-to-peer network, each peer shares data with a other peers and searches for the desired data by submitting queries to neighbors or to server. Once the desired data are found, the peer downloads the data directly from the other peer's computer. Data which are replicated among peers, this peer-to-peer network allows sharing of data by a large community at low cost, as dedicated servers are not needed.

Americans are now using high-speed Internet than they did when early peer-to-peer networks were formed. Napster, the first peer-to-peer network, appeared in 1999 to a steadily growing web audience. Napster which is created by Shawn Fanning quickly found the center of major lawsuits over copyright infringement as millions of people used the service to share their multimedia files. After being banned on college campuses throughout the US, Napster was ultimately forced to shut down. After that Bram Cohen's introduced BitTorrent program in 2004. This peer program was set up to be more efficient than Napster, and it served as the basis for how large files are shared on peer to peer networks today. BitTorrent has registered tens of millions of users. Similar to Napster, some users try to use BitTorrent to illegally share music and movies, even though much of BitTorrent's activities are legal. The conversion from MP3s to HD video, Peer-to-Peer networks have grown to serve multiple users at once.

Peer-to-Peer distribution needs many users in order to work efficiently. Each peers must use computers with an Internet connection too, if the connection is faster, the result is better. Regular computer networks rely on a central computer such as server to send out video to all the viewers' computers. This is like a "hub-and-spoke" design. The server is considered as the "hub" in the middle and viewers are the spokes which all have to connect to the "hub". It's highly different from a peer-to-peer network. The "hub-and-spoke" should work for sharing word documents, but it turns into a slow bottleneck when large files are sent back and forth.

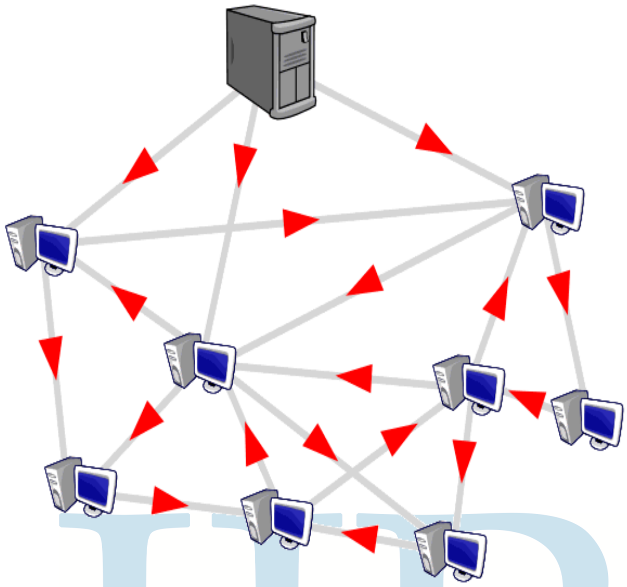

Fig1.Pee-to-peer network

III. LITERATURE SURVEY

Now a days computer networks allow the trading of digital data in an easy and cheap way. Fingerprinting schemes are a very popular method for supporting copyright protection. The main idea is that a merchant sells every customer a slightly different copy of the digital data. For example, in the case of an image, the merchant could darken or lighten some pixels in some location.The fingerprint must be such that a buyer cannot easily detect and cannot remove it.Once the merchant finds an illegally distributed copy,he can recognize the copy by its fingerprints and then hold its buyer responsible. Fingerprinting schemes helps to detect people from illegal copying of digital data by enabling the merchant of the original data to identify the original buyer of a copy that was redistributed illegally. Birgit Pfitzmann and Matthias Schunter[2] propose asymmetric fingerprinting, which provides copyright protection by identifying illegal redistributor with the help of asymmetric cryptography. In particular, it offers non-repudiation, that is there is a proof that one particular person was responsible for an action.

M. Kuribayashi[3] proposes the method for implementing the spread spectrum watermarking technique by designing parameters for rounding operation. The frequency components of digital contents are used for the adding fingerprint information, they must be arranged in order to truncate real value to integer. At that time, the accuracy of the frequency components should be considered not to degrade a quality of watermarked image. When the spread spectrum watermarking technique in [4] is applied, the accuracy of the representing watermark signal is sensitive for the implementation. By scaling the parameters by multiplying a constant factor, the accuracy was increased . Then, the trade-off between the scaling factor and how much data to be transmitted must be considered. In addition, the characteristic of the fingerprinting protocol, frequency components and the watermark signal must be separately encrypted after quantization. In this method, the consistency of the precision is a sensitive issue. The embedding operation is done by adding the frequency components and a spread spectrum sequence, then the additive homomorphic property of public-key cryptosytems [5, 6] can be directly exploited for the embedding. The separate rounding operation causes interference term in a deciphered data at a buyer side. Without the loss of secrecy of an original content, the interference term is removed after decryption. The performance of this method is calculated by comparing with the conventional scheme [4], which confirms the identification capability of illegal buyers.

Birgit Pfitzmann and Matthias Schunter propose anonymous fingerprinting [7].Here fingerprinting carry out anonymously. Each buyer already has a key pair of digital signature scheme, so that the public key can serve as a digital identity. Thus we require a buyer to sign under her identity in a protocol. It require buyers to register for the fingerprinting scheme under their digital identity. It allows us to make the protocols of the fingerprinting scheme concrete, without arranging how the validity of the initial digital identity is verified. In some condition, the registration should be added with the initial establishment of the digital identity. The parties where registration may happen are called registration centers.The reasonable choice was the buyer’s bank, in particular if the fingerprinted data are paid with unknown digital cash, because the buyer need to register with a bank and will only be unknown to this bank’s clients.

J. Camenisch [8] proposes a new scheme ,here the buyer issuing a group signature on a message describing the deal. In an ordinary group signature scheme there is no (fixed) revocation manager. Instead of the buyer chooses a secret and public key pair for the revocation manager here the public key is used for issuing the group signature, whereas the secret key is embedded into the sold content. So, finding an illegally redistributed copy puts the merchant to the position of revocation manager for that particular group signature and he can retrieve the identity of the culprit. With the help of group signature schemes, each buyer must register only once (registering basically amounts to join the group) and the merchant can retrieve an identity directly. One version of our scheme can even do without a registration center

.

D. Megias and J. Domingo-Ferrer [9] propose a peer-to-peer content distribution scheme based on a specific peer software in which the merchant creates a set of M seed copies of the content and sends them to M seed buyers. All subsequent copies are formed from the M seed copies. The copy obtained by a buyer is a combination of the copies supplied by her parents that are sources. The fingerprint of every buyer is constructed as a binary sequence combining the sequences of her parents.This is same as how DNA sequences of living beings are formed by combining the DNA sequences of their parents. This proposed scheme saves bandwidth and computation of the merchant, which still allows tracking illegal redistributors but preserves the anonymity of honest buyers.

D. Megias and J. Domingo-Ferrer[10] propose a peer-to-peer distribution scheme of fingerprinted content where the original merchant form only a set of M seed copies of the content and sends them to M seed buyers. The different copies are generated from the seed copies. The different non-seed buyer obtains a copy of the content by running a peer-to-peer purchase software tool. The copy obtained by individual buyer is a combination of the copies provided by her sources that is parents. The fingerprint of each buyer is a binary sequence that is generated automatically by the combination of the sequences of her parents. This peer to peer distribution technique makes it possible for the merchant to save bandwidth and CPU time for tracing the redistributed content.

Many anonymous fingerprinting methods make use of the homomorphic property of public-key cryptography [3]. These techniques allows embedding the fingerprint in the encrypted domain with the help of public key of the buyer.In such a way that only the buyer get the decrypted fingerprinted content after using her private key. In this way, developing a practical system using the above idea appears difficult, because public-key encryption expands data and substantially increases the communication bandwidth required for transfers [11]. This paper reviews the main features of the proposal suggested in [9], [10], highlights its main drawbacks, and suggests several significant improvements to achieve a more efficient and practical system, especially the traitor tracing was concerned, since it avoids the situations in which illegal redistributors cannot be traced with the proposal of [9], [10].Furthermore, better security properties against potentially malicious proxies are obtained.

The fingerprints produced are not stored in the transaction monitor in the original distribution protocol in order to protect the privacy of the buyers. The hash of the fingerprint are only stored in the transaction monitor for each buyer.

The automatic construction of fingerprints by recombining segments of the parent buyers' fingerprints is depicted in Fig. 2. It was worth pointing out the difference between the terms fragments and "segments" as used in this system. Each segment is of the fixed-sized pieces that form the whole fingerprint embedded in content, where the term fragment is used for the different pieces of the content. Each of the fingerprint contains a segment embedded into it. As discussed in [10], each child is interested in getting fragments from more than one parent, and each parent will not providing all the fragments to the same child. Because if two peers A and B get exactly the same copy of the fragment, then peer A could be held responsible for any unlawful content re-distributed by peer B and vice versa. Hence children and parents need to protect each others' privacy is known as the co-privacy property, as defined in [13].

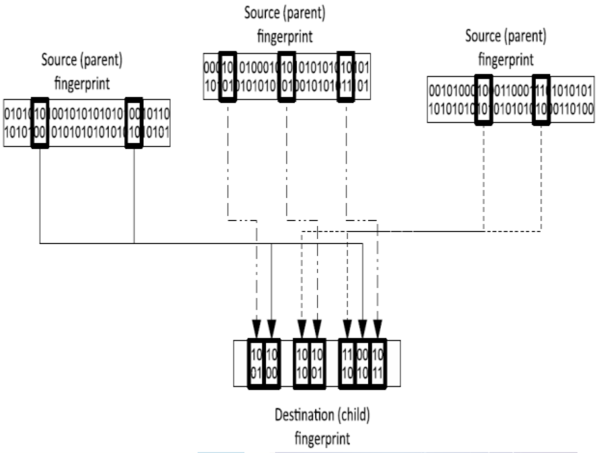

Fig 2. Automatic recombined fingerprint construction.

The new proposal[12] is to store also the fingerprints of the buyers in an encrypted form. The transaction registers would then be formed as follows:

P_i Username (pseudonym) of the buyer Bi.
H(c) Perceptual content hash (used for indexing in the content database).
E_hi Encrypted hash of the buyer's fingerprint.
E_{fi} Encrypted buyer's fingerprint.
d Transaction date and time (for billing purposes).

In the original proposal [10], E_{hi} was stored one time per parent with double encryption, using the public keys of the parent and the transaction monitor. In the improved proposal,E_{hi} is encrypted only with the public key of the transaction monitor. Having access to the fingerprints hashes does not allow the transaction monitor to reconstruct any buyer's fingerprint, since a hash function is not invertible, thereby preserving buyer frame proofness.

The improvements to the previous system done the storage of an encrypted version of the buyers fingerprints, E_{fi} , computed as follows:

$$E_{f_i} = E(E^c_{g_1}|E^c_{g_2}|\dots|E^c_{g_m}, K_a)|\dots| \\ E(E^c_{g_{(L-1)m+1}}|E^c_{g_{(L-1)m+2}}|\dots|E^c_{g_{Lm}}, K_a).$$

Each fragment of the content shall be transmitted with a fingerprint's segment g_j embedded into it and together with an encrypted version of the segment

$$\breve{E}^c_{g_j} \doteq E(g_j, K_c).$$

where K_c is the public key of the transaction monitor.
Each proxy selects a set of m continuous fragments of the content and facilitates the anonymous communication between parents and child for the transmission of those fragments. These m continuous fragments of the content carry m continuous segments of the fingerprint embedded into them.

IV. CONCLUSION

The recent use of automatic recombined fingerprints has been suggested in the literature [9], [10], showing remarkable advantages, the buyers fingerprints are unknown to the merchant that means it is achieving anonymously and fingerprint embedding is required only for a few seed buyers. The other fingerprints are automatically obtained as a recombination of segments. However, the published system has some shortcomings, the first one is it requires an expensive graph search in order to identify an illegal re-distributor, second is some innocent buyers are requested to co-operate for tracing, and third one is the peer-to-peer distribution protocol requires honest proxies. The co-operation of honest buyers in traitor tracing has several relevant drawbacks that can make the published system fail under some circumstances. The improvements suggested in the paper[12] overcome the drawbacks of papers [9], [10] by saving the fingerprints using multiple encryption.Hence we can replace the graph search by a standard database search, whilst buyers' frame proofness is retained.Here misbehaving proxies are not encouraged by means of random checks by the authority and using a four-party anonymous communication protocol to prevent proxies from accessing the clear text of the fragments of the content.

References

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

[2] Birgit Pfitzmann, Matthias Schunter: *Asymmetric Fingerprinting;* Eurocrypt '96, LNCS 1070, Springer-Verlag, Berlin 1996, 84-95.

[3] Smita Naikwadi, Niket Amoda," Advances In Image Processing For Detection Of Plant Diseases," International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol2, Issue 11, November 2013. 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.

[4] I. Cox, J. Kilian, F. Leighton, and T. Shamson, "Secure spread spectrum watermarking for multimedia", *IEEE Trans. Image Process.*, vol. 6, no. 5, pp. 1673.1687, 1997.

[5] T. Okamoto and S. Uchiyama, .A new public-key cryptosystem as secure as factoring,. in *Advances in Crypgology . EUROCRYPT'98*. 1998, vol. 1403 of *LNCS*,pp. 308.318, Springer-Verlag.

[6] P. Paillier, .Public-key cryptosystems based on composite degree residuosity classes,. in *Advances in Cryptology . EUROCRYPT'99*. 1999, vol. 1592 of *LNCS*,pp. 223.238, Springer-Verlag.

[7] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in Proc. 16th Ann. Int. Conf. Theory Appl. Cryptographic Techn., 1997,pp. 88–102

[8] J.Camenisch,"Efficient anonymous fingerprinting with group signatures' In Asiacrypt 2000, LNCS 1976, Springer, pp. 415-428, 2000.

[9] D. Megias 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.

[10] D. Megias and J. Domingo-Ferrer, "Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints,"Multimedia Syst., vol. 20, pp. 105–125, 2014.

[11] 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.

[12] D. Megias," Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints" IEEE transactions on dependable and secure computing, vol. 12, no. 2, march/april, 2015.

[13] J. Domingo-Ferrer and D. Megias, "Distributed multicast of fingerprinted content based on a rational peer-to-peer community,"Comput. Commun., vol. 36, pp. 542–550, Mar. 2013.