International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 25-Apr-2015,ISSN_NO: 2320-7248

Peer-to-Peer Hypermedia Sharing Built on Recombined Thumbprints

Swetha[1], Suganya[2],[3]Anitha Moses,[4]Mr.Kajendran

[1,2] PG Scholar, [3,4]Assistant Professor,
Department of MCA,Panimalar Engineering College
Anna University.

Abstract *– Thumbprinting emerged as a technological solution to avoid illegal content re-distribution. Anonymous fingerprint is a solution for legal distribution of multimedia contents with copyright protection. The identities of buyer are revealed only in case of illegal redistribution. Some of the problems in the existing fingerprint protocols are 1) use of complex time-consuming protocols and/or homomorphic encryption of the content, and 2) a unicast approach for distribution that does not scale for a large number of buyers. Recombined fingerprints methodology is used. Proposed system is efficient, scalable, privacy-preserving and P2P based fingerprinting system. The multimedia file is distributed in the peer-peer networks. The main work of the process is to identify any misuse of multimedia copies along the peer-peer network. The recombined fingerprint are used for unique identification of the merchant and buyers. Finally evaluate the performance of work based on efficiency, accuracy etc.*

Keywords: anonymous Thumbprinting, recombined Thumbprints, P2P contented sharing.

1 . Introduction

Thumbprinting emerged as a technological solution to avoid illegal content re-distribution. Anonymous fingerprinting is, thus, the most convenient strategy to protect both the buyers' privacy and the owner's rights, since it guarantees the following properties: 1) only the buyer obtains the fingerprinted copy of the content, 2) it preserves the anonymity of the buyers' identities with respect to the merchant.The fingerprint technique blends some of the advantages of the unicast and multicast solutions. Many anonymous fingerprinting schemes exploit the homomorphic property of public-key cryptography [5]. The proposal in [2], [12] 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.The 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.

Most fingerprinting systems can be classified in three categories [3], namely

symmetric, asymmetric and anonymous schemes. In symmetric schemes, the merchant is the one who embeds the fingerprint into the content and forwards the result to the buyer; hence, the buyer cannot be formally accused of illegal redistribution, since the merchant also had access to the fingerprinted content and could be responsible for the redistribution.

As scalability is concerned, the unicast approach in which the merchant establishes a connection with each single buyer is not a convenient strategy. However, broadcast distribution is not suitable for fingerprinting applications since different fingerprints are required for different buyers in order to guarantee traceability. Peerto-peer (P2P) distribution can be the answer to this difficulty, as proposed in this paper, since this technique blends some of the advantages of the unicast and multicast solutions. In fact, some content distributors are already operating under the P2P paradigm.

2. System model

Merchant distributes copies of the content legally to the seed buyers. Each fragment of the content contains a different segment of the fingerprint embedded into it.Seed buyers receive fingerprinted copies of the contents from the merchant. Other buyers purchase the content and obtain their fingerprinted copies from the P2P distribution system.The content is assembled from fragments obtained from different "parents". Anonymous connections with peer buyers are provided by means of proxies. Proxies provide anonymous communication between peer buyers by means of a specific protocol analogous to Chaum's mix networks .Transaction monitor keeps a transaction register for each purchase carried out for each buyer. This transaction register includes an encrypted version of the embedded fingerprints. Tracing authority checks illegal re-distribution, it participates in the tracing protocol that is used to identify the illegal re-distributor(s).

2.1 Mercantile:

he distributes copies of the content legally to the seed buyers. Each fragment of the content
contains a different segment of the fingerprint embedded into it. The segments have low pair-wise
correlations.

2.2 Seed buyers (Bi for i = 1, . . . ,M):

They receive fingerprinted copies of the contents from the merchant that are used by the P2P distribution system to bootstrap the system. They can be either real or dummy buyers as discussed in [13].

2.3 Proxies:

They provide anonymous communication between peer buyers by means of a specific protocol
analogous to Chaum's mix networks [5] (see below).

2.4 Tracing authority:

in case of illegal re-distribution, it participates in the tracing protocol that is used to identify the illegal re-distributor(s).

3. Security model

As Security is concerned, there are two main items to be protected: • Buyer frame proofness is related to the possibility that an innocent buyer is accused of illegal redistribution of the purchased content. • Copyright protection would be broken if any party obtains a copy of the content whose fingerprint is not included in the fingerprints' database of the transaction monitor (and thus can be re-distributed illegally) or the association of that particular fingerprint with the illegal re-distributor cannot be completed.

4 P2P distribution protocol

The improvements to the system stem from the storage of an encrypted version of the buyers fingerprints, Efi ,computed as follows: • Each fragment of the content shall be transmitted with a fingerprint's segment gj embedded into it and together with an encrypted version of the segment E c gj = E(gj ,Kc) where Kc is the public key of the transaction monitor. • Each proxy facilitates the anonymous communication between parents and child for the transmission of those fragments. Proxies selects a set of m contiguous fragments of the content for distribution in peer-to-peer network. The construction of the fingerprint with segments and sets of contiguous segments is shown in Fig.1. • The proxy concatenates the m contiguous encrypted segments, encrypts the concatenation using the public key of the tracing authority (Ka) and sends the result to the transaction monitor. • Hence, the transaction monitor stores the following encrypted version of the fingerprint: Efi = E (Ec g1 |E c g2 | . . . |E c gm ,Ka) | . . . | E (Ec g(L−1)m+1 |E c g(L−1)m+2 | . . . |E c gLm ,Ka) • Modification of the transmission protocol refers to the use of symmetric cryptography to encrypt the content in such a way that intermediate routers do not have access to the original text of the content. • The transaction monitor cannot decrypt Efi without the private key Ks a of the authority.

Fig. 1: Fingerprint's segments (g_j) and sets of m contiguous segments

5. Traitor tracing protocol

The new basic traitor tracing protocol (when no collusion occurs) begins with the extraction of the fingerprint of the illegally re-distributed copy by the tracing authority. Then, the authority uses the public key of the transaction monitor and its own public key to produce the encrypted fingerprint which can be efficiently searched in the database of the transaction monitor. Once the pseudonym of the illegal re-distributor is available,it can be associated to a real identity. • The fingerprint f of the illegally redistributed content is extracted by the tracing authority using the extraction method and the extraction key (provided by the merchant). • The fingerprint's segments gj are encrypted using the public key of the transaction monitor: E c gj = E(gj,Kc). •

Volume: 2 Issue: 1 25-Apr-2015,ISSN_NO: 2320-7248

6. Security and Privacy

An illegal redistributor 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. • If no collusion occurs, the fingerprint f would be first extracted by the tracing authority, which is trusted. Then the tracing authority would compute E c gj = E(gj ,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.

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

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 in [12] 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, Basic traitor tracing would be used with the hash of the fingerprint instead of the fingerprint itself. As described in [12], 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.

6.1 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.

7. Conclusion and future work

The final result is a fingerprinting system that features: Efficient and scalable distribution of multimedia contents in P2P networks. Efficient traitor tracing of illegal re-distributors through a standard database search. Privacy preservation and buyer frame proofness. Mutual anonymity for merchant and buyers and between peer buyers. Collusion resistance. Avoidance of fingerprint embedding except for a few seed buyers. In future work the multimedia contents is distributed in peer to peer networks and provide security by encryption and decryption using DES algorithm. But it takes high execution time. To overcome this drawback Blowfish algorithm is used for encryption and decryption and it provide security. Blowfish algorithm works on variable key length, it works for bit length 64-448.Because of this it takes less

execution time. The objective of blowfish algorithm is to encrypt the images in a short execution time with minimum cost. The images are encrypted which are all converted from the multimedia file before transferring to the buyer. It improves the efficiency of the process.

ACKNOWLEDGMENTS

This work was partly funded by the Spanish Government through projects TSI200765406-C03-03 "EAEGIS", EAEGIS", TIN2011-27076-C03-02 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES".

REFERENCES

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

[2] D. Meg´ıas and J. Domingo-Ferrer, "DNA-Inspired Anonymous Fingerprinting for Efficient Peer-To-Peer Content Distribution,"Proc. 2013 IEEE Congress on Evolutionary Computation (CEC2013), pp. 2376–2383, Jun. 2013.

[3] R. O. Preda and D. N. Vizireanu, "Robust wavelet-based video watermarking scheme for copyright protection using the human visual system," Journal of Electronic Imaging, vol. 20, pp. 013022–013022-8, Jan.-Mar. 2011.

[4] 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.

[5] M. Kuribayashi, "On the implementation of spread spectrumfingerprinting in asymmetric cryptographic protocol," EURASIPJournal on Information Security, vol. 2010, pp. 1:1–1:11, Jan. 2010.

[6] S. Katzenbeisser, A. Lemma, M. Celik, M. van der Veen, and M.Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. on Information Forensics and Security,vol. 3, pp. 783–786, Dec. 2008.

[7] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington MA: MorganKaufmann, 2008.

[8] J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP Journal on Information Security, vol. 2007, pp. 20:1–20:7, Dec. 2007.

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

[10] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan: An efficient and anonymous buyer-seller watermarking protocol. IEEE Transactions on Image Processing, vol. 13, pp. 1618–1626, Dec. 2004.

[11] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," Asiacrypt 2000, LNCS 1976, Springer, pp.