Efficient P2P Multimedia Distribution based on Encryption

M. Sireesha
PG Scholar,CSE
Sri Vasavi Engineering College
Tadepalligudem

A. Sirisha
Assistant Professor,CSE
Sri Vasavi Engineering College
Tadepalligudem

Abstract:- **Unidentified unique mark (UUM) has been suggested as an appropriate answer for the approved imparting of mixed media substance to patent assurance while safeguarding the privacy of purchasers, whose personalities are just appeared if there should be an occurrence of disallowed re-conveyance. Notwithstanding, a large portion of the current unidentified fingerprinting conventions are unreasonable for two primary reasons: 1) the utilization of complicated extended conventions and/or homomorphism encryption of the substance, and 2) a unicast advance for commitment that does not degree for a gigantic Number of purchasers. This paper originates from a prior suggestion of recombined fingerprints which beat several of these downsides. However, the recombined unique finger impression approach requires a complicated chart look for trickster following, which needs the association of different purchasers, and legitimate intermediaries in its P2P portion situation. This paper concentrate on expelling these detriments bringing about a capable, adaptable, security protecting and P2P-based fingerprinting framework.**

Key words: Secrecy-Preserving, Multimedia Sharing.

1. INTRODUCTION

System security comprises of the arrangements and strategies embraced by a system head to counteract and screen unapproved access, abuse, change, or dissent of a PC system and system open assets. System security includes the approval of access to information in a system, which is controlled by the system executive. Clients pick or are relegated an ID and secret word or other confirming data that permits them access to data and projects inside their power. System security covers an assortment of PC systems, both open and private, that are utilized as a part of regular occupations leading exchanges and correspondences among organizations, government offices and people. Systems can be private, for example, inside an organization, and others which may be interested in free. System security is included in associations, undertakings, and different sorts of foundations.

It does as its title clarifies: It secures the system, and additionally ensuring and supervising operations being finished. The most well-known and basic method for ensuring a system asset is by appointing it a one of a kind name and a relating secret word. System security begins with verifying, usually with a username and a secret key. Since this requires only one point of interest validating the client name i.e. the secret key this is here and there named one-variable verification. With two factor confirmation, something the client "has" is additionally utilized (e.g. a security token or 'dongle', an ATM card, or a cell telephone); and with three-variable validation, something the client "is" is additionally utilized. Once confirmed, a firewall authorizes access strategies, for example, what administrations are permitted to be gotten to by the system clients. In spite of the fact that powerful to counteract unapproved access, this part may neglect to check possibly unsafe substance, for example, PC worms or Trojans being transmitted over the system. Hostile to infection programming or an interruption aversion framework (IPS. detect and restrain the activity of such malware. An inconsistency based interruption discovery framework may likewise screen the system like wireshark activity and might be logged for review purposes and for later abnormal state investigation. Fingerprinting developed as a mechanical answer for stay away from illicit substance redistribution.

2. RELATED WORK

We propose a P2P content distribution scheme (based on a specific P2P software) in which the merchant creates only a set of M seed copies of the content and sends them to M seed buyers. All subsequent copies are generated from the M seed copies. The copy obtained by a buyer is a combination of the copies supplied by her “parents” (sources). The fingerprint of each buyer is constructed as a binary sequence combining the sequences of her parents, in a way parallel to how DNA sequences of living beings are formed by combining the DNA sequences of their parents. The proposed scheme, which saves bandwidth and computation at the merchant, still allows tracking illegal redistributors but preserves the anonymity of honest buyers. The proposed method is thus inherently scalable compared to other systems in the literature [15], [3], [1], [7], which require (non-scalable) unicast transmissions and rely on complex CPU-intensive and/or bandwidth consuming cryptographic protocols. The cryptographic protocols used in our approach reduce to the transmission of a few encrypted hashes with low computation and communication costs. In fact, the method proposed in this paper even avoids running the embedding algorithm for nonseed buyers and thus it outperforms the abovementioned methods. The rest of this paper is organized as follows. Section II introduces DNA-inspired fingerprints, which are the foundation of the proposed scheme. Section III describes the method for P2P distribution of DNA-inspired fingerprinted contents, including the algorithm for tracing illegal redistributors.

Fundamentally, fingerprinting comprises of inserting an indistinct imprint –fingerprint– in the appropriated substance to distinguish the substance purchaser. The installed imprint is diverse for every purchaser, except the substance must stay perceptually indistinguishable for all purchasers. Fingerprinting plans deflect individuals from illicitly redistributing advanced information by empowering the first dealer of the information to distinguish the first purchaser of a redistributed duplicate. As of late, topsy-turvy fingerprinting plans were presented. Here, just the purchaser knows the fingerprinted duplicate after a deal, and if the dealer discovers this duplicate some place, he gets a proof that it was the duplicate of this specific purchaser. In the event of unlawful redistribution, the implanted imprint permits the distinguishing proof of the re-wholesaler by method for a double crosser following framework, making it conceivable to take ensuing lawful activities. Despite the fact that fingerprinting systems have been accessible for about two decades, the initial couple of recommendations in this field are a long way from these days' necessities, for example, adaptability for thousands or a huge number of potential purchasers and the conservation of purchasers' security.

Most fingerprinting frameworks can be characterized in three classes, in particular symmetric, unbalanced and mysterious plans. In symmetric plans, the shipper is the person who installs the unique mark into the substance and advances the outcome to the purchaser; subsequently, the purchaser can't be formally blamed for illicit redistribution, since the vendor likewise had admittance to the fingerprinted content and could be in charge of the redistribution. In deviated fingerprinting, the shipper does not have admittance to the fingerprinted duplicate, but rather he can recuperate the unique mark in the event of illicit redistribution and in this way recognize the culpable purchaser. In unknown fingerprinting, notwithstanding asymmetry, the purchaser safeguards her obscurity (protection) and consequently she can't be connected to the buy of a particular substance, unless she takes an interest in an illicit re-conveyance. Shared (P2P) figuring or systems administration is a circulated application engineering that segments errands or workloads between associates. Associates are similarly favored, equipotent members in the application.

They are said to shape a distributed system of hubs. Peers make a bit of their assets, for example, preparing power, plate stockpiling or system transfer speed, straightforwardly accessible to other system members, without the requirement for focal coordination by servers or stable hosts. Companions are both suppliers and customers of assets, as opposed to the conventional customer server model in which the utilization and supply of assets is partitioned. Developing synergistic P2P frameworks are going past the time of companions doing comparative things while sharing assets, and are searching for different associates that can get special assets and abilities to a virtual group along these lines enabling it to take part in more prominent errands past those that can be expert by individual companions, yet that are advantageous to every one of the associates. Numerous unknown fingerprinting plans abuse the homomorphic property of open key cryptography. These plans permit installing the unique mark in the scrambled space (with people in general key of the purchaser) in a manner that exclusive the purchaser acquires the unscrambled fingerprinted content in the wake of utilizing her private key. Different methodologies for unknown fingerprinting don't misuse homomorphic encryption along these lines, yet either 1) require exceedingly requesting advancements, for example, open key encryption of the substance, secure multiparty conventions, duty conventions or zero knowledge evidences, among others, bringing about restrictive computational and communicational expenses; or 2) depend on hypothetical secure inserting calculations for which no verification of presence is accessible.

3. STATE OF THE ART ON FINGERPRINTS

Most fingerprinting schemes can be classified in three types [3]: symmetric, asymmetric and anonymous. In the first type, the merchant is the one who embeds the mark into the content; hence, the buyer cannot be formally accused of illegal redistribution, since the merchant also had access to the fingerprinted content and could be himself the redistributor. In Asymmetric fingerprinting, the merchant does not have access to the fingerprinted copy, but he can recover the mark in case of illegal redistribution and thereby identify the malicious buyer. In anonymous fingerprinting, in addition to asymmetry, the buyer preserves her anonymity and hence she cannot be linked to the purchase of a specific content, except if she participates in an illegal redistribution. A novel concept of automatic DNA-inspired binary fingerprints. The terms used in this paper are derived from those used in genetics to refer to DNA and heredity. The definitions of these terms in the context of this paper are introduced below.

3.1 Principles of DNA-inspired Fingerprints

In this paper, a DNA-inspired fingerprint is constructed as a binary sequence and each bit can be considered as the counterpart of the nucleotides in real DNA sequences. Although each of the real DNA sequences' nucleotides can be thought of as a two-bit symbol (since there are four different nucleotides), the analogy can still be established using 1bit nucleotides. This is similar to what is done in genetic algorithms [9]. Gene: a segment of the DNA sequence which encodes a given protein –and thus has some impact in heredity and in the biological chemistry of the living being– is called a gene. Similarly, a segment of the DNA-inspired fingerprint sequence is called a "gene" in this paper. DNA-inspired fingerprints are defined as a single bit stream, it is still possible to consider that a complementary sequence exists by using its negation. Crossovers can thus be simulated between a binary fingerprint and its negation.

Mating and heredity: in nature, the genes of an offspring are basically a combination of the genes of its parents (although some other processes such as mutation and crossover may produce fragments of DNA which are different in the offspring with respect to both its parents). Similarly, in this paper, when a buyer obtains a copy of a P2P-distributed content using some specific software, the DNA-inspired fingerprint of her copy will be a combination of the genes of

the sources of the content (referred to as "parents" from the biological analogy). In this case, the number of parents for a buyer does not have to be exactly two as in the natural world. Hence, the mating process in the suggested fingerprinting scenario must be understood in a generalized sense, not limited to two parents. In this proposal, fingerprints can be considered as being "automatically generated" from the fingerprints of the parents.

The upload and download processes for obtaining a file from different sources in a P2P fashion are shown in Fig. 1a. In this figure, the destination (or child) is downloading fragments of the file from three different sources (or parents). When all fragments are downloaded they are joined together to construct a copy of the content.

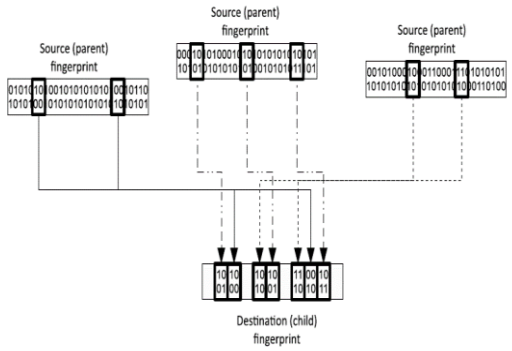

Figure 1: Downloading fragments and constructing a copy of content.

3.1.1 Requirements on fingerprint embedding

1) The DNA-inspired fingerprint must be a binary sequence that is spread along the whole file. The fingerprint must be formed as the concatenation of separated pieces (genes) that are embedded in different fragments of the file. These fragments will be distributed by the P2P software as a "atomic" components of the content.

1) 2) Obviously, the versions downloaded by different buyers will not be bitwise identical. The P2P-distributed download of the contents will produce different copies for different buyers, but all the copies of the contents should be equivalent from a perceptual point of view (all buyers require the same high quality for the purchased content). In this case, a standard hash function which produces different hash values even after a single bit change would not be useful for indexing, since the copies obtained by different buyers would not be associated to the same index.

3.2 P2P distribution protocol

To bootstrap the system, a few copies of the content with different fingerprints must be produced. The merchant can produce a small number M of instances of the content and embed different pseudo-random binary sequences (DNA-inspired fingerprints) into them. These copies are then transferred to the M seed buyers who may be genuine buyers of the content or dummy buyers created by the merchant to facilitate the distribution. In either case, the seed buyers will be contacted by second-generation buyers to download further copies of the content. The association of the first M fingerprints with the pseudonyms of the first M buyers must be recorded either by the merchant or some trusted authority. Once the system is bootstrapped, all further transactions occur without any need to run the embedding algorithm as far as at least two parents are chosen for each buyer (as discussed above). Note also that all fingerprints from buyer M + 1 to the final one (N) will remain completely anonymous (only known by the buyers themselves) and cannot be related to real identities. Thus, anonymous fingerprinting is obtained in a much simpler way than with any of the existing proposals in the literature [15], [3], [1], [7], which require running complex cryptographic protocols for every transaction. As detailed below, in our proposal only the transaction monitor keeps a record of the transactions between buyers in case they are required in future DNA relationship tests. In any case, real identities are not known by the transaction monitor and, hence, privacy is fully preserved.

3.3 The traitor tracing protocol

Assuming that the embedding scheme is secure and robust enough so that malicious users cannot easily erase their fingerprints without making the content unusable (this is the standard marking assumption, [2]), the following method can be used by a tracing authority to identify the source of an illegally distributed copy. The maximum correlation criterion will work with a high probability, but a higher correlation might accidentally be obtained for a non-ancestor of the buyer of the illegally distributed copy. For example, a descendant D of the illegal redistributor I may have, as another ancestor A, a node of the graph which is also an ancestor of I. This would produce a high correlation but the chain from A to D skips the illegal redistributor I. In this situation, backtracking is required in the tracing algorithm described above. A complete subnetwork should be exhausted until all nodes of the subgraph having no children are considered. When a complete subnetwork is exhausted, the element of T with the second maximum correlation would be chosen as the candidate ancestor of the traitor to be identified. When all elements of T I have been considered without success (i.e. without being able to accuse anyone), the procedure would backtrack to the set T.

4. ANALYSIS

This section presents a set of simulated experiments to illustrate the properties of the proposed system. In particular, we focus on the number of buyers which will be required to cooperate with the tracing authority in case of a traitor tracing investigation. All simulations presented below use DNA-inspired fingerprints formed by 4096 bits, divided into 128 genes of 32 bits each. A more detailed analysis and empirical results on the method proposed in this paper, including examples which are closer to real-world scenarios, can be found in [12].

Gener.	Popul.	Average DNA tests		Backtrack.
		1 simul.	100 simul.	(100 sim.)
$k = 2$	$N = 20$	3.40 (34.0%)	3.71 (37.1%)	0%
$k = 3$	$N = 40$	6.93 (23.1%)	7.29 (24.3%)	0%
$k = 4$	$N = 80$	12.26 (17.5%)	11.69 (16.7%)	0.6%
$k = 5$	$N = 160$	18.99 (12.7%)	17.05 (11.4%)	1.2%
$k = 6$	$N = 320$	24.31 (7.8%)	23.76 (7.7%)	2.7%

Figure 2: Average number and percentage of DNA relationship tests on non-seed buyers: Comparison between exponential and linear growth for the same population

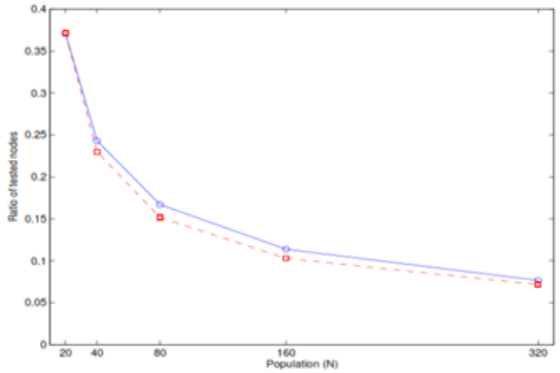

Figure 3: Average fraction of non-seed buyers affected by DNA relationship tests:Comparison between exponential growth (circle, solid) vs. linear growth (square, dashed) for the same population.

5. CONCLUSION

A DNA-inspired fingerprinting scheme designed for P2P content distribution is presented. The proposed scheme allows the merchant to trace traitors who redistribute the content illegally. The merchant knows at most the fingerprinted copies of the seed buyers, but not the fingerprinted copies of non-seed buyers (the vast majority). Hence, the merchant does not know the identities of non-seed buyers. Whenever a traitor needs to be traced, only a small fraction of honest users must cooperate by providing their fingerprinted copies (quasi-privacy). Collusion resistance against dishonest buyers trying to create a forged copy without any of their fingerprints is also discussed. Finally, buyer frame proofness is guaranteed since a malicious merchant does not have access to the fingerprinted copies of non-seed nodes. Thus, he will not be able to frame an honest buyer since random guess is not an option to construct a valid fingerprint (due to combinatorial explosion). Future research will involve designing backtrack-free protocols for traitor tracing in such a way that the fraction of honest buyers who must co-operate in case of an illegal redistribution is reduced. The security analysis of the proposed scheme against malicious proxies, who may even collude with other parties is also left for the future research.

REFERENCES

[1] Arjmand Samuel, Muhammad I. Sarfraz and ArifGhafoor, "A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data", IEEE Transactions On Multimedia, Vol. 17, No. 9, September 2015.
[2] Mohamed Hefeeda , Tarek ElGamal , Kiana Calagari and Ahmed Abdelsadek, "Cloud-Based Multimedia Content Protection System", IEEE Transactions On Multimedia, Vol. 17, No. 3, March 2015.
[3] FudongQiu, Fan Wu and Guihai Chen, "Privacy and Quality Preserving Multimedia Data Aggregation for Participatory Sensing Systems", IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015.
[4] Amr Alasaad, KavehShafiee and Victor C.M. Leung, "Innovative Schemes for Resource Allocation in the Cloud for Media Streaming Applications", IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 4, April 2015.
[5] Adi Hajj-Ahmad, Ravi Garg and Min Wu, "ENF-Based Region-of-Recording Identification for Media Signals", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 6, June 2015.
[6] Liang Zhou, Dan Wu, Baoyu Zheng and Mohsen Guizani, "Joint Physical-Application Layer Security for Wireless Multimedia Delivery", IEEE Communications Magazine, March 2014.
[7] Zhuo Wei, Yongdong Wu and Xuhua Ding, "A Hybrid Scheme for Authenticating Scalable Video Codestreams", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014.
[8] Guang Hua and Vrizlynn L. L. Thing, "A Dynamic Matching Algorithm for Audio Timestamp Identification Using the ENF Criterion", IEEE Transactions On Information Forensics And Security, July 2014.
[9] Michael Arnold, Xiao-Ming Chen and GwenaëlDoerr, "A Phase-Based Audio Watermarking System Robust to Acoustic Path Propagation", IEEE Transactions On Information Forensics And Security, March 2014.
[10] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," in Proc. 15th Ann. Int. Cryptology Conf. Adv. Cryptology, 1995, pp. 452–465.
[11] Y. Bo, L. Piyuan, and Z. Wenzheng, "An efficient anonymous fingerprinting protocol," in Proc. Int. Conf. Comput. Intell. Security, 2007, pp. 824–832.
[12] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," in Proc. 6th Int. Conf. Theory Appl. Cryptology Inf. Security: Adv. Cryptology, 2000, pp. 415–428.
[13] 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.
[14] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.
[15] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Burlington, MA, USA: Morgan Kaufmann, 2008.
[16] 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.
[17] M. Fallahpour and D. Megıas, "Secure logarithmic audio watermarking scheme based on the human auditory system," Multimedia Syst., vol. 20, pp. 155–164, 2014.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] D. Megıas and J. Domingo-Ferrer, "Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints," Multimedia Syst., vol. 20, pp. 105–125, 2014.
[23] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.

[24] Pando Networks, Inc., 2008. [Online]. Available: http://www.pandonetworks.com/
[25] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in Proc. 16th Ann. Int. Conf. Theory Appl. Cryptographic Techn., 1997, pp. 88–102.
[26] B. Pfitzmann and A.-R. Sadeghi, "Coin-based anonymous fingerprinting," in Proc. 17th Ann. Int. Conf. Theory Appl. Cryptographic Techn., 1999, pp. 150–164.
[27] 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.
[28] 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.