Improved Hybrid Fingerprint-Based P2P Media Distribution For Privacy Protection

MAKADIYA DHARMI
M.Tech Student, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. S. SHANTI
Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. M.SAMBASIVUDU
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Abstract: **It has been suggested that anonymous fingerprinting could be an easy way to ensure the lawful dissemination of copyright-protected multimedia content without compromising the privacy of customers, whose names would only be revealed in the event of illegal re-distribution of the content. This idea has been put forward as a potential solution to the problem. However, the majority of the currently available anonymous fingerprinting systems are not practical. This is due to the fact that they make use of complicated protocols that take up a lot of time, as well as homomorphic encryption of the data. Furthermore, they distribute the data using a unicast approach, which does not scale well for a large number of clients. The concept of recombined fingerprints serves as the foundation for this body of work, which also makes an effort to overcome some of these restrictions. On the other hand, recommended fingerprint approaches need a complex graph search for traitor monitoring, which in turn demands the participation of additional buyers and honest proxies in their P2P distribution scenario. Getting rid of these issues and developing a fingerprinting system that is not only efficient but also scalable, private, and makes use of P2P technology is the purpose of this research.**

Keywords: **Privacy; Homomorphic; Proxies; Unicast*;***

I. INTRODUCTION:

While the embedded mark is unique for each customer, the content must always seem to be the same to each and every consumer. In the event that the product is illegally re-distributed, the implanted mark enables the identification of the person responsible for the crime via the use of a traitor tracking system, which in turn makes it possible for further legal steps to be taken. While methods for fingerprinting have been around for about twenty years, the initial few suggestions in this sector are a far cry from the needs of today, such as the capacity to scale up to hundreds or millions of prospective buyers and the protection of purchasers' privacy. The vast majority of fingerprinting techniques may be placed into one of three categories: symmetric, asymmetric, or anonymous [1]. In symmetric schemes, the merchant is the one who imbeds the fingerprint into the content and then sends the result to the buyer. As a result, the buyer cannot be formally accused of illegally redistributing the content because the merchant also had access to the fingerprinted content and could be responsible for the redistribution. When asymmetric fingerprinting is used, the retailer does not have access to the copy that has been fingerprinted, but he is able to recover the fingerprint in the event that it has been illegally redistributed and, as a result, identify the customer who is responsible for the violation. In anonymous fingerprinting, in addition to asymmetry, the buyer maintains her anonymity (privacy), and as a result, she cannot be linked to the purchase of a particular piece of content, unless she takes part in an illegal act of redistribution. This is the case even if the fingerprints of both the seller and the buyer are collected. Anonymous fingerprinting is therefore the most practical strategy for protecting both the buyers' privacy and the owner's rights, as it guarantees the following properties: 1) Only the buyer obtains the fingerprinted copy of the content, rendering it impossible for the merchant to accuse her of unlawful redistribution; 2) it maintains the anonymity of the buyers' identities in relation to the merchant. As has been mentioned before, the fingerprints of the purchasers were not saved in the transaction monitor in the first version of the protocol for the distribution of the cryptocurrency [2]. This was done to ensure that the purchasers' personal information was kept confidential. Just a hash of the fingerprint was kept on file for each customer who made a purchase. The buyer's fingerprint hash was encrypted and saved many times, depending on the number of parents the buyer had. The buyer's parent's public key was used to encrypt the fingerprint hash (and also the public key of the transaction monitor). In this manner, the cooperation of at least one parent was necessary in order to get the plain text of the fingerprint's hash. According to the latest idea, the fingerprints of the purchasers would also be stored, albeit in an encrypted form.

II. PROBLEM STATEMENT:

The majority of fingerprinting systems fall into one of three categories: symmetric, asymmetric, or anonymous. In symmetric schemes, the merchant embeds the fingerprint into the content and sends the result to the buyer; therefore, the buyer cannot be formally accused of illegal re-distribution, as the merchant also had access to the fingerprinted content and could be held accountable for the re-distribution. With asymmetric fingerprinting, the merchant does not have access to the fingerprinted copy, but he may recover the fingerprint in the event of illicit resale and so identify the guilty purchaser. With anonymous fingerprinting, in addition to asymmetry, the customer maintains her identity (privacy), thus she cannot be traced to the purchase of a particular piece of information, unless she engages in an unlawful re-distribution [3][4]. Public-key encryption extends data and considerably increases the necessary communication capacity for transfers, making it difficult to implement this concept in a real system. Homomorphic encryption restricts the mathematical operations that may be done on the material for embedding, making it challenging to apply the more complex and resilient approaches described in the literature on data concealment. However, the use of this concept in a distributed environment (such as P2P networks) is not straightforward, since embedding would have to be conducted by peer purchasers, necessitating a complicated and supervised protocol.

III. PROPOSED METHODOLOGIES:

The material is separated into a number of ordered pieces, each of which is embedded with a distinct random binary sequence. Each fragment's binary sequence is referred to as a "segment," and the concatenation of all segments constitutes the fingerprint. The vendor delivers unique copies to a subset of M seed purchasers [5]. The fingerprints of these purchasers are such that the correlations between their parts are minimal. The buyers other than the seed purchasers participate in P2P content transfers so that each new purchaser acquires pieces from at least two other purchasers. N is the total number of purchasers. With a proxy and a technique like onion routing, peer-to-peer purchasers may communicate anonymously. Each new buyer's fingerprint is created by recombining the segments of his or her parents. Proxy servers are privy to the pseudonyms of source and destination purchasers as well as the symmetric keys used to encrypt multimedia information. A transaction monitor creates a transaction record for each transaction between peer purchasers. These records simply include a hash of the embedded fingerprints, not the fingerprints themselves. The hashes of the fingerprints are encrypted so that the private key of at least one parent is needed to decrypt them. The only person who knows the true identity of customers is the merchant. The transaction monitor tracks the aliases of purchasers. The distribution graph must be searched in the event of unauthorised redistribution. The search begins with the seed purchasers and is guided by a correlation function between the traced fingerprint and the tested purchasers' fingerprints. These purchasers must collaborate with a tracing authority in order to establish a link between their fingerprint and the one retrieved from the unlawfully redistributed file. The transaction monitor's fingerprint hashes are sufficient to prevent purchasers from cheating at this point. At each stage of the methodology for locating a traitor, the purchaser with the highest correlation is selected as the most probable ancestor of the unlawful redistributor. This criteria is largely accurate, although it may result in some wrong selections throughout the search process, necessitating the depletion of a subparagraph and backtracking. When a perfect connection is established between the fingerprint of the tested buyer and the fingerprint of the unlawfully redistributed file, the search is concluded [6]. If a buyer refuses to submit to a correlation test, the transaction monitor's recorded hash might be used as evidence against her. This paper examines the main features of the proposed system, identifies its major drawbacks, and proposes a number of significant enhancements to achieve a more efficient and practical system, particularly with regard to tracing traitors, as it avoids situations in which illegal redistributors cannot be traced. Moreover, improved security features against possibly hostile proxies are achieved. While the system presented in this work employs public key encryption in the distribution and traitor tracking protocols, this encryption is only applied to short bit strings, such as the binary fingerprints and hashes, and not the actual content. Content pieces are encrypted using symmetric cryptography, which is much more efficient.

IV. ENHANCED SYSTEM:

One of the proxies selected by the buyer and the merchant (who may connect her pseudonym to a real name) or, similarly, the transaction monitor and the merchant might expose the identity of a buyer who has bought a certain material. In order to increase anonymity, proxies might encrypt the pseudonyms using the tracing authority's public key. Whenever a buyer's fingerprint is kept in the transaction monitor's database, it opens the door for a potential attack. In order to steal the material in its entirety, an attacker may attempt to eavesdrop on a buyer's communications with her proxy or proxies. A record of all sales made to each customer is maintained. The integrated fingerprints are encrypted and stored alongside the transaction register. It contributes to the tracing technique required to locate the source of the problem(s) in the event of unauthorised redistribution. Anyone who buys seeds from him receives authorised copies of the material. An individual fingerprint section is encoded into each piece of material. There is little connection between the parts.

.

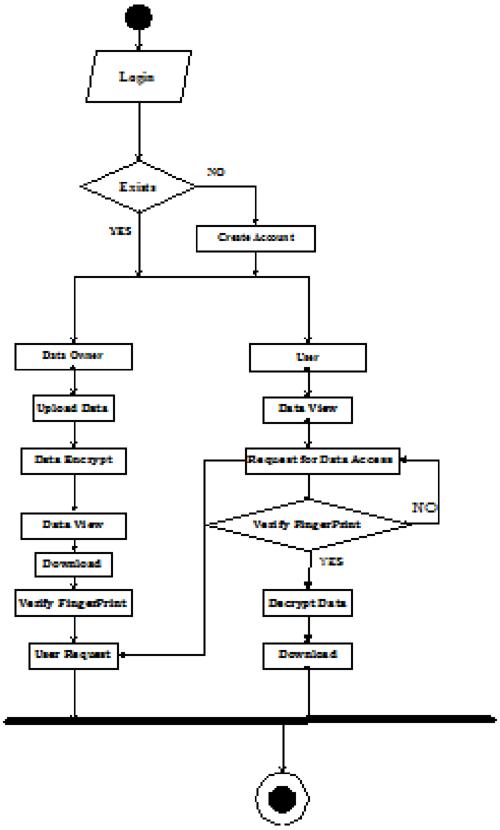

Fig 1: Activity of System

V. CONCLUSIONS:

This system demonstrates that the cooperation of honest purchasers in the tracking of traitors is associated with a number of significant disadvantages, any one of which has the potential to cause the disclosed system to fail under certain conditions. The flaws that are caused by recording fingerprints using multiple encryptions are circumvented as a result of the enhancements that are proposed in this paper. Specifically, the graph search is changed to a standard database search, and the buyers' frame-proofness is not compromised as a result of these modifications. In addition, malicious proxies are discouraged by random checks performed by the authority and by the use of a four-party anonymous communication protocol that prevents proxies from accessing the clear text of the fragments of the content. Both of these measures are taken to ensure that the content remains private. Since the merchant does not have access to the fingerprints of the purchasers, anonymity may be maintained. Embedding fingerprints is necessary for just a select few seed purchasers, while the other fingerprints are automatically acquired by the recombination of segment information.

REFERENCES:

[1] J. Camenisch, “Efficient anonymous fingerprinting with group signatures,” in Proc. 6th Int. Conf. Theory Appl. Cryptology Inf. Security: Adv. Cryptology, 2000, pp. 415–428.

[2] 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.

[3] D. L. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Commun. ACM, vol. 24, pp. 84–90, Feb. 1981.

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

[5] 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.

[6] M. Fallahpour and D. Megıas, “Secure logarithmic audio watermarking scheme based on the human auditory system,” Multimedia Syst., vol. 20, pp. 155–164, 2014.

[7] 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.

[8] 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.

[9] 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.

[10] 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.