Enhanced Secrecy-Preserving Peer to Peer Multimedia Sharing based on Recombined Fingerprints

D.Rajkumar[1] A. RajivKannan[2]
[1,2]Department of Computer Science & Engineering
[1,2]K.S.R. College of Engineering

Abstract— Unidentified fingerprint has been recommended as a suitable solution for the authorized sharing of multimedia contents with patent protection whilst preserving the confidentiality of buyers, whose identities are only shown in case of prohibited re-distribution. However, most of the existing unidentified fingerprinting protocols are unrealistic for two main reasons: 1) the use of intricate protracted protocols and/or homomorphism encryption of the substance, and 2) a unicast advance for contribution that does not extent for a massive Number of buyers. This paper stems from a foregoing proposition of recombined fingerprints which overcome a number of of these drawbacks. Yet, the recombined fingerprint approach requires a intricate graph seek for traitor tracing, which needs the involvement of other buyers, and honest proxies in its P2P allocation scenario. This paper focus on removing these disadvantages resulting in an proficient, scalable, privacy-preserving and P2P-based fingerprinting system.

Key words: Secrecy-Preserving, Multimedia Sharing

I. INTRODUCTION

Fingerprinting emerge as a procedural way out to avoid unlawful content re-distribution. Essentially, fingerprinting consists of embedding an undetectable mark— fingerprint— in the circulated content (which may be audio, still images or video) to identify the substance buyer. The fixed mark is different for each buyer, but the content must continue perceptually equal for all buyers. In case of unlawful re-distribution, the entrenched mark allows the recognition of the re-distributor by means of a traitor tracing method, making it possible to take consequent legal actions. Even though fingerprinting techniques have been accessible for nearly two decades, the first few proposals in this field are outlying from nowadays' requirements such as scalability for thousands or millions of credible buyers and the conservation of buyers' privacy. Broadband home Internet access supports direct downloads of multimedia contents Finger printing technique is used to avoid illegal substance re-distribution Fingerprinting consists of embed an unnoticeable mark in the distributed content used to identify the content buyer The embedded mark allows the identification of the re-distributor by means of a traitor tracing structure.

II. LITERATURE SURVEY

A. A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data (2015)

The system provides a multimedia big data sharing mechanism with privacy and security policies Secure User Data Repository System (SUDRS) and Intelligent Privacy Manager (iPM) models are used to provide security and privacy for multimedia data Policy and context based security scheme. Owner to view all multimedia data elements held by the SURDS along with sharing options provided by the Asset Manager. All multimedia data elements are divided into categories and types of files. Additional data elements can be uploaded by select 'Open file manager' on the top proprietor/donor to manage multimedia data elements held in the form of files by the File Manager. File Manager allows an owner/contributor to manipulate their data in terms of uploading new multimedia content. The disadvantages of this paper are redistribution access control is not provided.

B. Cloud-Based Multimedia Content Protection System (2015)

The system is used to protect different multimedia content types under the cloud environment 3-D Video Signatures Scheme and Distributed Matching Engine are used to provide multimedia data access with security. It supports creating amalgamated signatures that consist of one or more of the following elements: 1.Visual mark: Created based on the optical parts in multimedia objects and how they change with time; 2.Audio mark: Created based on the audio signals in multimedia objects; 3. Depth mark: If multimedia objects are 3-D videos, signatures from their depth signals are created; 4.Meta data: Created from information associated with multimedia items such as their names, tags, descriptions, layout types, and IP addresses of their uploaders. The disadvantages of this paper are Computational complexity is high in online redistribution verification process.

C. Privacy and Quality Preserving Multimedia Data Aggregation for Participatory Sensing Systems (2015)

The system supports privacy and quality preserving participatory sensing with multimedia data SLICER scheme integrates a data coding technique and message transfer strategies to achieve strong protection of participants' privacy. The domestic attack may come from both the participants and the service provider. We differentiate two cases: Protection against participants' attack. Each contributor may accept some slices, when it is preferred as a slice deliver for participants met. Similar with the peripheral attacker, the participant cannot decrypt the slice for delivering shield against service provider's attack. Given that the service provider has full access to the sensing records contributed by the participants, it can easily infer secret information about the participants, if proper privacy-preserving design is not provided. Still, SLICER can achieve the k-anonymity and protect participants' privacy information against the service provider. Therefore, we can draw the following theorem. The disadvantages of this paper are Privacy on query processing is not supported.

D. Innovative Schemes for Resource Allocation in the Cloud for Media Streaming Applications (2015)

The system provides streaming resources from the cloud to the media content providers Prediction Based Resource Allocation (PBRA) algorithm is used to manage streaming resource allocation for content distribution. The reservation plan, the media substance provider reserves possessions in advance and pricing is exciting before the possessions are utilized (upon getting the appeal at the cloud provider, i.e., prepaid possessions). The ondemand plan, the media content supplier allocates streaming possessions ahead required. Pricing in the on-demand plan is stimulating by pay-per-use starting point. In general, the prices (tariffs) of the reservation research are cheaper than those of the ondemand plan (i.e., time reduce rates are only offered to the reserved (prepaid) resources). The Disadvantage of this paper are Media content security and privacy are not considered.

E. ENF-Based Region-of-Recording Identification for Media Signals (2015)

Electrical Network Frequency (ENF) signals are used to verify the location of multimedia content recording process. Multiclass Region-of-recording Classification scheme is adapted to verify the recording location of multimedia contents. Dimensionality reduction schemes are identified to be helpful to assist efficient implementations of machine wisdom in many applications concerning a high dimension of features. To examine their effects on our difficulty, we have experimented with dissimilar dimensionality reduction schemes, purposely, the Fisher's Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) [20]. Using LDA, we trim down the dimensionality of our data from the original dimensionality of 16 to $M - 1$, where M is the amount of classes. Grids With Varying Profiles A probable factor impacting the efficiency of ENF-based spot classification is the unpredictability of a grid's ENF attributes with time. The power profile of a positive grid may exhibit different types of behaviours, depending on the time of a day or the term of a year. For our dataset, we have made sure to collect data from both daytime and nighttime, and when probable, we have try to collect data from different times in a year. The disadvantages of this paper are Security and privacy are not provided for multimedia data.

F. Joint Physical-Application Layer Security for Wireless Multimedia Delivery (2014)

Wireless multimedia data delivery scheme is secured with stream based data security models Joint physical application layer security system provides the security for multimedia data delivery process. Watermarking technology extend the guard of multimedia content behind decryption by embedding a mark that cannot be apparent in the multimedia content. In other words, one embeds an subjective watermark into multimedia contents by applying unnoticeable changes to the original multimedia contents. Fundamentally, these alterations depend on a private key at the detector, and are tested and examine at the decoder. In preparation, the decoding idea uses the received watermarked multimedia content and a private key to approximate and test the watermark this is called a blind detection architecture. The disadvantages of this paper are Device level authentication and energy factors are not considered.

G. A Hybrid Scheme for Authenticating Scalable Video Code streams (2014)

Scalable video coding (SVC) scheme is adapted to secure video transmission process hybrid authentication (HAU) scheme employs both cryptographic authentication and content-based authentication techniques for video authentication. The authentication tag generation procedure includes MAC production and feature extraction, where MACs are constructed by taking the encoded image of the bottom layer and a secret key as inputs, while the features of each frame are extracted from the maximum quality and resolution images of SVC bitstreams. Note that if an SVC codestream has spatial enhancement layers, HAU should originally downsample the main resolution to the same resolution as the base layer, then extract features from the downsampled one. Hence, extent of the feature value is allied to the base layer's resolution for each AU (Access Unit). Tag Conveyance is required to carry the authentication tag (i.e., feature hash V and MAC φ) to the recipient together with the SVC codestream for confirmation. In HAU, we summarize the tag into SVC user data as a new SEI (Supplement Enhancement Information) NALU as was done in. The payload type of the new SEI is Unregistered User Data communication so as to preserve SVC format.The disadvantages of this paper are User level privacy is not supported.

H. A Dynamic Matching Algorithm for Audio Timestamp Identification Using the ENF Criterion (2014)

Audio files are verified with Electrical Network Frequency (ENF) factors A threshold-based dynamic matching algorithm (DMA) is used to perform autocorrecting the noise affected frequency estimates. Deviations of Frequency Estimation of deviate frequency inference of recorded audio data may come from noise, frequency decision problem, or the compensate. The noise and frequency decision problems can be measured as one problem, which is explain as follows. Let the window mock-up size of the STFT be NW and sample frequency be fs Hz, then the windowed part has a time interval of TW = NW/ fs seconds. The disadvantages of this paper are Content and distribution security are not considered.

I. A Phase-Based Audio Watermarking System Robust to Acoustic Path Propagation (2014)

Audio watermarking techniques are used to authenticate the audio files. Audio watermarking algorithm is enhanced with psychoacoustic model, resynchronization framework and correlation based detector for authentication. The Analysis-Synthesis structure auditory signals are quasi-stationary within a short time period of about 2-50 ms. Moreover, the human auditory system somehow perform a time-frequency examination of audio signals. As a result, it is common preparation in audio dispensation to be appropriate a short-time Fourier transform (STFT) to attain a time-frequency depiction of the signal so as to mimic the behavior of the ear. The disadvantages of this paper are Video authentication is not supported.

III. PROBLEM IDENTIFICATION

Anonymous fingerprint is used for the legal distribution of multimedia contents with copyright protection with privacy of buyers. Buyers identities are only revealed in case of illegal re-distribution. Recombined fingerprints model overcomes delay and scalability issues. Traitor tracing protocol is used to identify the illegal distribution of multimedia contents. The recombined fingerprint approach uses a complex graph search for traitor tracing. Traitor tracing requires the participation of other buyers and honest proxies in the P2P distribution scenario. P2P Distribution Protocol manages the Merchant, Seed Buyers, Proxies and Peer Buyer transactions. Proxies know the pseudonyms of starting place and target buyers and they have access to the symmetric keys used for encrypting the multimedia content. A operation confirmation is created by a transaction observe to keep track of each transport between peer buyers. These records do not hold the embedded fingerprints, but only an encrypted hash of them. The fingerprints' hashes are encrypted in such a method that the private key of at slightest one parent is requisite for obtain their clear text. Proxies are used to handle anonymous communication between the peer buyers and higher authorities. Standard database search process is not secured. Proxy misbehaviour identification is not supported. Spatial and temporal factors are not adapted. Limited privacy on communication process.

IV. CONCLUSION

The utilize of routine recombined fingerprints has been freshly suggested in the narrative showing significant advantages: the fingerprints of buyer are unidentified to the seller (achieving anonymity) and fingerprint embedding is required only for a few seed buyers, but the other fingerprints are routinely obtained as a recombination of segments. However, the published system has some shortcomings: 1) it requires an classy graph search in instruct to recognize an illicit re-distributor, 2) some blameless buyers are requested to assist for tracing, and 3) the P2P distribution protocol requires honest proxies. This document shows that the collaboration of truthful buyers in traitor tracing entails several relevant drawbacks that can make the published scheme be unsuccessful under a few conditions. The improvements recommended in this paper overcome the drawbacks by recording the fingerprints by way of multiple encryptions in such a method that the graph search is replaced by a paradigm database explore, whilst buyers' frameproofness is retained. Also, mischievous proxies are discouraged by resources of random checks by the ability and via a four-party unspecified communication protocol to prevent proxies from accessing the clear text of the wreckage of the content.

REFERENCES

[1] Arjmand Samuel, Muhammad I. Sarfraz and Arif Ghafoor, "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] Fudong Qiu, 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, Kaveh Shafiee 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 Gwenaël Doerr, "A Phase-Based Audio Watermarking System Robust to Acoustic Path Propagation", IEEE Transactions On Information Forensics And Security, March 2014.

