ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 12, pp.76366-76369, December, 2018
DOI: https://doi.org/10.24941/ijcr.33574.12.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

CLOUD BASED SECURE CONTENT SHARING APPLICATION FOR PREVENTING AND DETECTING THE ILLEGAL CONTENT REDISTRIBUTION OF MULTIMEDIA

[1,]Ankita S. Bunage and [2]Prof. R. V. Mante

[1]PG Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati – 444604, Maharashtra, India
[2]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Amravati – 444604, Maharashtra, India

ARTICLE INFO

Article History:
Received 20th September, 2018
Received in revised form
30th October, 2018
Accepted 29th November, 2018
Published online 31st December, 2018

Key Words:
Multimedia Content, Illegal Redistribution, Copyright Prevention, Leakage Detection, Watermarking, Secure Watermarking, Media Player.

ABSTRACT

The wild development of multimedia content is pushing forward the worldview of cloud-based media facilitating nowadays. Due to developing time of web and the ease of using it, the copyright assurance and confirmation of content has become exceptionally imperative issue. To unravel the issue of copyrights, digital watermarking has been used over quite a while. Still, the issue of secured outsourcing isn't completely illuminated since replicating media substance is nearly cost-free, and the authorized clients afterward redistribute the media content misguidedly. Therefore, it is imperative to bestow secure cloud-based media sharing with the competence of tracing illegal content redistribution. In this paper, a brief introduction to digital watermarking and their techniques are given. Also, we studied all the previous methods for detecting the illegitimate content redistribution and reviewed their limitations. To improve the security of the content and for preventing and detecting the content leakage, we give a brief idea about a new proposed solution- cloud based secure content sharing application with the media player for halting the unauthorized access.

Citation: Ankita S. Bunage and Prof. R. V. Mante. **2018.** "Cloud based secure content sharing application for preventing and detecting the illegal content redistribution of multimedia", *International Journal of Current Research*, 10, (12), 76366-76369.

INTRODUCTION

Content sharing situations such as social networking are dynamic in terms of the number of on-line clients, storage capacity, network bandwidth, computational capability, applications and stages, hence it isn't simple for a benefit supplier to distribute resources following the traditional client-server model. The reckless development of interactive media content is pushing forward the worldview of cloud-based media facilitating nowadays. Cloud Computing gives a modern standard to bolster the around the world computing request for Data Innovation administrations. Whereas, there are a few security debate and challenges in cloud computing are: Data Breaches, Data Loss, Malicious Insiders, Denial of Service, Vulnerable Systems and APIs. Be that as it may, to overcome this security dangers and challenges, the earlier exertion is to ensure the information whereas uploading and downloading to/from the cloud by utilizing the encryption calculations and methods. Still, the encrypting data before outsourcing, does not unravel the total issue. Since, the authorized recipient/ client is able to duplicate the information and can forward to the unauthorized collector or client.

Corresponding author: **Ankita S. Bunage,**
PG Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati – 444604, Maharashtra, India.

This issue is alluded as content copyright issue. Replicating of data from web has ended up a customary movement. Securing this data is essential and for the same there are numerous calculation and methods, a few of which incorporates Cryptography, Steganography and Watermarking. Cryptography may be a strategy of making the mystery data or the data incoherent by apply a few changes or substitutions on it, commonly known as encryption and decoding. Steganography may be a strategy of stowing away the secret data on a few carrier file that can be anything i.e. image, audio or video. Computerized Watermarking may be a strategy of implanting a few mystery data within the primary computerized substance to supply security, integrity and authentication. The Digital watermarking has been planned as a key to the issue of copyright security of multimedia information in an organized network environment. It makes conceivable to immovably relate to an advanced archive a code permitting the recognizable proof of the information creator, proprietor, authorized buyer, and so on. The watermark is envisioned to be permanently embedded and ought to not alter the substance of the work. The most reasons of utilizing the computerized watermark are: proprietorship assertion, fingerprinting, verification and integrity confirmation, content labeling, utilization control. Numerous of the watermarking strategies had been proposed and examined.

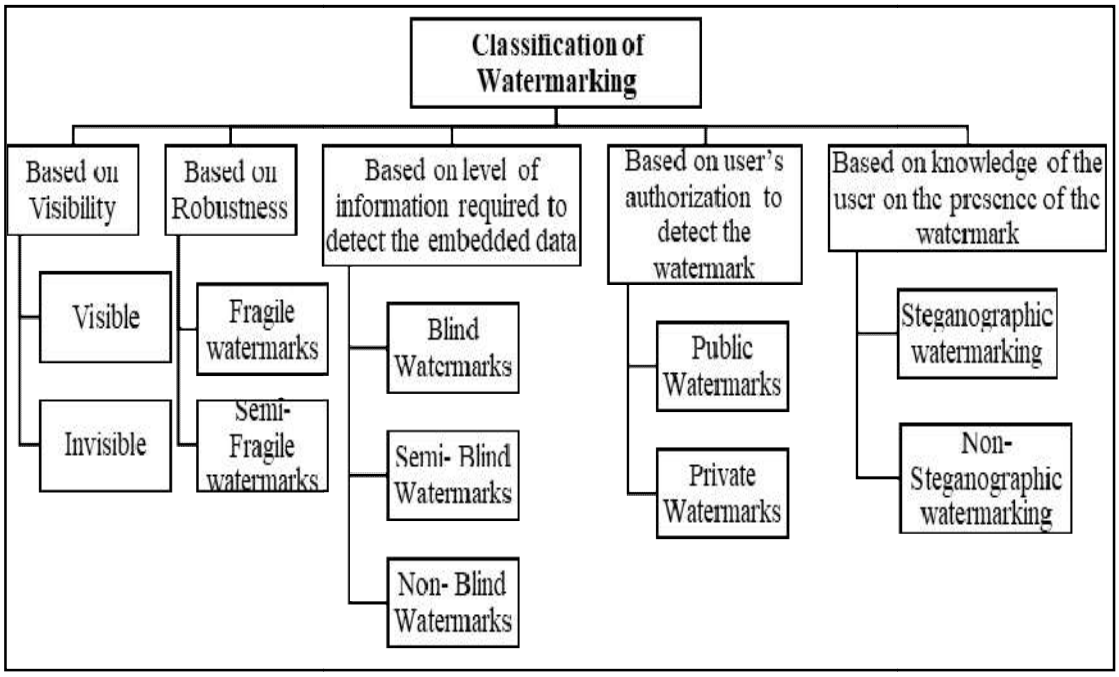

Fig. 1. Different Types of Watermarking Techniques

Also, some advanced systems had developed to detect the traitor who leaked the authorized data to unauthorized party. Following diagram gives the classification of watermarking. Despite the fact that computerized watermarking can be utilized for cheater following, the current frameworks are just ready to distinguish the double crosser if the substance supplier watched some released/ill-conceived information from unapproved client. In the event that, content supplier is ignorant about pilfered duplicates of information, there is no utilization of frameworks utilizing backstabber following and watermarking systems. Also, there are few diverse types of attacks like exclusion attack, symmetrical attack and cryptography attack that may possible on digital watermarking. Therefore, to take care of the copyrights issue and for conspirator tracing, a new watermarking method is proposed here for mixed media content is utilized in content sharing. The brief idea about the proposed system is mentioned in a chapter III.

LITERATURE SURVEY

Interactive media information has been developing exponentially day by day. In any case, uploading and downloading interactive media content needs the cloud-based framework since of tremendous information upkeep issue. Subsequently, there's a need to secure multimedia information of distinctive types over the cloud changes from the scholastic world to trade applications. The number of considers had done which appears the prerequisite of security in cloud computing. Investigate is being carried out by the way from past decade. Following study begin with outlining the overview of interactive media content challenges and issues. And afterward on a few researches given the solutions for securing multimedia copyrights issues.

Multimedia Content Challenges and Issues: Er.Shilpi Harnal et al (2016), have given a outline of desires and encounters for media cloud computing. In this paper, the basic concept of general-purpose cloud computing environment alongside distinctive benefit models, deployment models and also the common security issues for cloud are given. A widespread study and think about of secure and privacy-preserving P2P dispersion frameworks discussed in (Amna Qureshi, 2016). This paper gives brief outline of the state-of-the-art procedures proposed to ensure copyrighted substance and client security.

Existing Systems for Copyrights Prevention: The encryption may be a great strategy to avoid copyright but there may be chances of spillage of encryption key. In this way, to illuminate this issue, an unused strategy to partition the encryption key into partial keys utilizing the secret sharing scheme, and permitting them to be distributed into diverse nodes is created (Yoshihiro Kawahara, 2010) Typically, robust strategy to suppress copyright infringement among the content transferred onto node to node video sharing administrations, and is particularly planned for customer created media (CGM). In spite of the circumstance that this framework is adaptable and effective, reduction within the time is required to get the content when more than 10% of the nodes are malicious. Afterward on, homomorphic encryption had developed. Homomorphic encryption could be a cryptographic method based on scientific issue computational complexity hypothesis (Baohua Chen, 2014) Later on, proxy re-encryption had used for data leakage prevention in cloud computing (Giuseppe Ateniese, 2005). Afterwards, a typical public key cryptography called as Attribute-based encryption (ABE) was firstly proposed, a type of public-key encryption in which the secret key of a handler and the ciphertext are contingent on upon attributes. Here, the decoding of a ciphertext is conceivable as it were in case the set of abilities of the user key matches the attributes of the ciphertext. A scalable and fine-grained cloud-based data sharing system is used in (Shucheng Yu, 2010), by uniquely merging ABE, PRE, and lazy re-encryption.

Existing Systems for Copyrights Detection: Copy detection is built on mark implanting: the merchant embeds an imperceptible mark into the content before selling it. There are two kinds of mark: watermarks and fingerprints. A unused development to get fingerprinting codes for copyright security

which survive any conspiracy methodology including up to three buyers (3-security) is compose by diffusing code, with a double Hamming code (Shucheng Yu, 2010). All known fingerprinting plans are symmetric within the taking afterwards: Both the buyer and the vendor know the fingerprinted duplicate. To realize the arrangement, deviated plans were presented, where only the buyer gets the precise watermarked content, and thus the buyer cannot claim that a pilfered duplicate was started from the dealer. Prior watermarking plans had a restriction though: a malicious content supplier may outline a client by unjustifiably blaming him of leaking a media protest. To illuminate this issue, a client ought to be able to argue against that during a dispute. This practical necessity leads to the afterward advancement of reasonable watermarking procedures (Yi-Jia Peng, 2017; Priyanka, 2016; Yoshihiro Kawahara, 2010; Sudha1, 2014 and Conghuan, 2012). Whereas guaranteeing traceability, reasonable watermarking encourage gives fairness to avoid the content supplier from framing clients. In any case, for secure cloud-based media sharing, how to appropriately apply reasonable watermarking to empower reasonable backstabber following isn't however clear and remains to be completely explored.

Existing Systems for traitor tracing: A secured system architecture is design as an initial effort in (Yifeng Zheng, 2016). An encoded cloud media center is proposed which hosts the encrypted SVC videos. A key shortcoming is that this technique is only applicable for videos. Dynamic data leakage is illustrated by Govinda K., Divya Joseph in 2017, (Govinda, 2017), by using guilty agent detection over cloud. In this paper, primarily the detection of the faulty agent who purposefully leaked the secured data is done. Through this model, a sense of integrity and security in cloud is achieved. So that the third party can store, their precious data over cloud. The anticipated method uses s-max algorithm to perceive the data outflow. Cloud based buyer dealer watermarking convention based on progressed SS conspire is outlined in (Yi-Jia Peng, 2017). In this paper, two approaches are given: The first one contain cloud as infrastructure service provider and cloud as a platform service provider. In former one, seller used cloud service to speed up watermark whereas, in latter one, cloud behaves as an E- commerce platform. The most downside of first one is that CP has to contact every buyer during transaction. However, in second one, BS only need to contact with cloud. But, the disadvantage here is that it uses paillier cryptosystem. It needs Lattice based computation which is very complex computational task. Imposing access control alone, though, cannot fully shield content provider's welfares, as authorized users may in future become traitors that illegally redistribute media content to the public.

This realistic threat must have treated properly. In this article, secure media sharing with fair traitor tracing in the protected cloud media center is deliberated. Here, a new grouping of proxy re-encryption (for safe media sharing) and fair watermarking (for fair defector tracing) is used. The homomorphic properties are leveraged exist in in proxy re-encryption to encirclement operations in fair watermarking. Two protocols are proposed for different application scenarios (Leo Yu Zhang, 2018). The AES algorithm is used for encryption. And the homomorphic algorithm is used in proxy re-encryption with watermarking. The drawback of this system is that it used AES and homomorphic algorithm. Both increases the extent of the cipher text and doubles the size of file. Only data leakage is detected but cannot prevented. After the study of all the above methods and approaches of watermarking and reviewing all existing systems, some of the following observations are made:

Though watermarking and watermarking with encryption provides good solution for leakage detection, the drawback is the size of the file increases after watermarking and encryption. Also, all the encryption techniques are notorious, and traitor may be able now to decrypt and remove the watermark. Then again, there is no any way to prevent the access to leaked content access to leaked content.

PROPOSED SYSTEM

To overcome these glitches and to give another approach, we propose a cloud based secure content sharing application which detect and prevent the illegal redistribution of multimedia. We use a user defined encryption algorithm, which is very secure as its decryption process is not well known, in case of key leakage. This encryption algorithm is very secure and doesn't increase size of cipher text after encryption. Similarly, we use a user defined watermark which contains identification bits of both: content provider and client. Watermark will be checked at the time of download due to which leakage will be prevented. Another addition to our framework is media player for preventing leakage and for tracing the traitor if media is leaked in any case. Media player would check the access permission by using watermarked bytes online.

Conclusion

This paper reviews the recent studies and issues on content providing over cloud. Watermarking is becoming progressively popular, and many new methods and innovative techniques have been proposed and tested, which requires a new system with encrypted cloud. This article has discussed the recent advancement, limitations and problems in digital watermarking. A new model is proposed by combining user define encryption and watermarking. A user defined encryption algorithm maintain the size of the file as it is after encryption and watermarking. In this system, we also considered the leakage detection as well as prevention issue using our own media player. Therefore our system is more effective than existing system.

REFERENCES

Alfredo Rial, Mina Deng, Tiziano Bianchi, Alessandro Piva, and Bart Preneel, Member, 2010. "A Provably Secure Anonymous Buyer–Seller Watermarking Protocol", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4.

Amna Qureshi, Helena Rifa-Pous and David Megias, 2016. State-of-the-art, Challenges and Open Issues in Integrating Security and Privacy in P2P Content Distribution Systems", The Eleventh International Conference on Digital Information Management (ICDIM2016), IEEE, pp.1-9.

Ankitha.A.Nayak, Venugopala P. S, Dr. H. Sarojadevi, Dr. Niranjan, N. Chiplunkar, 2014. "A Survey and Comparative Study on Video Watermarking Techniques with Reference to Mobile Devices", IJERA, ISSN: 2248-9622, Vol. 4, Issue 12(Part 6), December pp.39-44.

Baohua Chen1, Na Zhao, 2014. "Fully Homomorphic Encryption Application In Cloud Computing", IEEE.

Birgit Pfitzmann, Matthias Schunteri, "Asymmetric Fingerprinting", Spnnger-Verlag Berlin Heidelberg, , pp. 84-95, 1996.

Cheung, S.C., Hanif Curreem, 2002. "Rights Protection for Digital Contents Redistribution Over the Internet", 26 th Annual International Computer Software and Applications Conference.

Chin-Laung Lei, Pei-Ling Yu, Pan-Lung Tsai, and Ming-Hwa Chan," 2004. An Efficient and Anonymous Buyer-Seller Watermarking Protocol," IEEE Transactions on image processing, vol. 13, no. 12.

Chunlin Song, Sud Sudirman, Madjid Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", ISBN: 978-1-902560-22-9.

Conghuan Ye1, 2, Ji Li1, Zenggang Xiong, 2012. "A Secure Content Distribution Based On Chaotic Desynchronization", International Symposium on Computer, Consumer and Control.

D. Usha Nandini, M.E., Divya. S, M.E. 2017. "A Literature Survey on Various Watermarking Techniques", International Conference on Inventive Systems and Control.

Dr. Amit Verma, 2Navdeep Kaur Gill, 2016. "Analysis of Watermarking Techniques", InternatIonal Journal of Computer SCIenCe and technology, Vol. 7, ISSue 1.

Er. Shilpi Harnal and Dr. R. K. Chauhan, 2016. "Issues & Perspectives with Multimedia Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 11, November.

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, 2005. "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage.

Govinda.K, Divya Joseph, 2017. "Dynamic Data Leakage using Guilty Agent Detection over Cloud", International Conference on Intelligent Sustainable Systems.

Jaishri Guru, Hemant Damecha, 2014. "Digital Watermarking Classification: A Survey", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct.

Lalit Kumar Saini, Vishal Shrivastava, 2014. "A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun.

Leo Yu Zhang, Yifeng Zheng and Jian Weng, 2018. "You Can Access But You Cannot Leak: Defending Against Illegal Content Redistribution in Encrypted Cloud Media Center," IEEE Transactions on Dependable and Secure Computing.

Lintian Qiao, Klara Naahrstedt, "Watermarking Schemes and Protocols For Protecting Rightful Ownership And Customer's Right".

Mahsa Boreiry, Mohammad-Reza Keyvanpour, 2017. "Classification of Watermarking Methods Based on Watermarking Approaches", Artificial Intelligence and Robotics (IRANOPEN).

Mahsa Boreiry, Mohammad-Reza Keyvanpour, 2017. "Classification of Watermarking Methods Based on Watermarking Approaches", IEEE Conference on Artificial Intelligence and Robotics.

Nurul shamimi kamaruddin, Amirrudin Kamsin, Lip Yee Por, and Hameedur Rahman, 2018. "A Review of Text Watermarking: Theory, Methods, and Applications", IEEE. Translations and content mining.

Panagiotis Papadimitriou, 2011. Data Leakage Detection", IEEE Transactions On Knowledge And Data Engineering, VOL. 23, NO. 1.

Prassanna, J., Punitha, K. and Neelanarayanan, V. 2015. "Towards an analysis of data accountability and auditing for secure cloud data storage", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Procedia Computer Science 50 pp.543 – 550.

Priyanka V. Padwal 1, Nilesh P. Sable, 2016. "Protection of Multimedia Content in Cloud Computing", *International Journal of Innovative Research in Computer and Communication Engineering,* Vol. 4, Issue 7, July.

Ritu Gupta, Sarika Jain and Anurag Mishra, 2015. "Watermarking System for Encrypted Images at Cloud to check Reliability of Images," International Conference on Next Generation Computing Technologies.

Sameeka Saini, 2015. "A survey on watermarking web contents for protecting copyright", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems.

Shucheng Yu, Cong Wang†, Kui Ren, and Wenjing Lou, 2010. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society.

Srijith K. Nair, Bogdan C. Popescu, Chandana Gamage, Bruno Crispo, Andrew S. Tanenbaum, 2005. "Enabling DRM-preserving Digital Content Redistribution", 7th IEEE International Conference on E-Commerce Technology.

Sudha1, S. S., Rahini, K. K. 2014. "Prevention Of Watermarking Attacks Using Cryptography Method", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 3, Issue 2, February.

Swapnali More and Sangita Chaudhari, 2016. "Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization, Procedia Computer Science 79, 2016 pp.69 – 76.

Valer Bocan, M hai Fagadar-Cosma, "Scalable and Secure Architecture for Digital Content Distribution".

Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li, 2011. "Multimedia Cloud Computing" IEEE Signal Processing Magazine, Volume 28, Issue 3, pp.59-69.

Yifeng Zheng, Xingliang Yuan, Xinyu Wang, Jinghua Jiang, Cong Wang, and Xiaolin Gui, 2016."Towards Encrypted Cloud Media Centre with Secure Deduplication", IEEE Transactions on Multimedia.

Yi-Jia Peng, Yung-Chen Hsieh, Chih-Wen Hsueh, Ja-Ling Wu, 2017. "Cloud-based Buyer-Seller Watermarking Protocols," IEEE Trans. on Smart World.

Yoshihiro Kawahara, Liang Wang and Tohru Asami, 2010. "Resilient Suppressor Mechanism against Illegal Content Redistribution on Peer-to-Peer Video Sharing Networks", IEEE Communications Society.

****