# Secure Watermarking for Defending Against the Illicit Content Redistribution of Multimedia in Cloud Based Content Sharing Application

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

[1]PG Scholar, [2]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Department of Computer Science and Engineering, Amravati, India

***Abstract :*** The multimedia information including audio, images and documents has been becoming one of the most transmission contents over the internet. However, this extensive multimedia data can easily acquire by people through the internet. Thus, the copyright assurance and confirmation of content has become remarkably authoritative issue. This problem is solved by introducing watermarks into the contents. But, the problem of content leakage is yet not fully solved as authorized person may become traitor and would leak the authenticated data to non-authorized one.

To overcome this situation and to improve the security of the content, we introduced a new idea of implementation of watermarking. In this paper, we proposed a combination of content sharing application over cloud and the media player. In this content application, the content leakage can be stopped and spotted by watermarking. And the unauthorized access can be stumbled with the help of media player.

***Index Terms*** **- Illegal Redistribution, Multimedia Content, Copyright Prevention, Leakage Detection, Watermarking, Secure Watermarking, Media Player**

## I. INTRODUCTION

With the booming market of digital content and the friendly use of internet, the protection of multimedia content had become more and more challenging. 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 files that can be anything i.e. image, audio or video. 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.

Digital watermarking provides a technique to insert a unique code which has been considered as an alternative or complement to Cryptography for content protection. The owner inserts distinct watermark into a sold copy of content to recognize the buyer. However, whenever there is a need to find the buyer (who is authorized user) of the specific content, Seller can trace back to find the owner (Buyer) of the illegal redistribution by the watermark he inserted. For building a successful multimedia content distribution system, a fair-trading environment, a proper watermarking scheme, and an effective method for scalability extension are the most important issues one has to deal with. 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

## II. LITERATURE SURVEY

A number of watermarking procedures have been projected to track down the distributors of illegal replicas [7], [8]. However, most of them ignore the fairness to the customers at all, and the others address the issue ineffectively, considering the current practice of law enforcement. Another mutual limitation of these protocols is the lack of appropriate mechanisms to protect customer privacy during transactions. The encryption may be a great and was the first strategy to avoid copyright [21],[30],[31]. A scalable and fine-grained cloud-based data sharing system is used in [32] by exclusively merging ABE, PRE, and lazy re-encryption.

All prior watermarking approaches had a restriction that a malicious content supplier may outline a client by unjustifiably imputing him of leaking a media protest. So, there was a need to improve watermarking procedures [18], [20], [21], [22], [23]. A secured system architecture is design as an initial effort for traitor tracing where an encoded cloud media center is proposed which hosts the encrypted SVC videos [17]. A key shortcoming is that this technique is only applicable for videos.

Cloud based buyer dealer watermarking convention based on progressed SS conspire is outlined in [18]. Here, cloud as infrastructure as well as a platform service provider is used to speed up watermark and as an E- commerce platform respectively. The most downside of first one is that CP has to contact every buyer during transaction. However, in second one, it uses paillier cryptosystem which is very complex computational task.

Afterwards, a new grouping of proxy re-encryption (for safe media sharing) and fair watermarking (for fair defector tracing) used the homomorphic properties occur in in proxy re-encryption in [19]. The AES algorithm and the homomorphic algorithm is used for encryption and proxy re-encryption with watermarking respectively. 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, we

observed: Size of a file increases after watermarking and there is no any way to prevent the access to leaked content access to leaked content.

## III. PROPOSED SYSTEM

In the proposed model we are combining cloud-based sharing application and media player. Here, we are preventing the copyright access by implementing new watermarking technique. While securely uploading of media files over cloud, we use a user defined encryption algorithm and after uploading we are adding watermarking bytes to the file with the help of proxy server. The proposed system is basically consisting of two parts: one is cloud based secure content sharing application and another is media player to open the downloaded file. After the subscription of CP's services, authorized user would be able to download the file and media player (MP). Downloaded file would be is in encrypted format and to open that file, user need to use the provided media player only. MP would check whether the identities stored in that specific file and user credentials are matching or not. If identities are not matched then it means that authorized user whose identity is watermarked in a file is a leaker and at that time that file won't be decrypted or not open. On the other hand, CP would be notified about illegal redistribution of his copy with the help of web services.

The framework mainly consists of four entities:

- Users: User will register himself and then login. User can be a Content Provider by uploading files with specifying access permission details. Later on, by applying encryption algorithm, files are uploaded to the cloud. Then user can view the shared files with him and can download these files. He can download and install the media player. Among these, user is able to track the usage, can view the payment details and most importantly he can view the leakage report.
- Cloud: It stores all the encrypted media content of the user. Upon receiving the request from the owner, it delegate the decryption right to an authorized user, as well as embed both the watermarks of the CP and the user imperceptibly in the desired media object. Cloud Admin can login the account and then he is able to view users, tracking the usage, tracking the payment and he is authorized to activate or deactivate the users.
- Media Player: After downloading the media object, a separate media player will check the authentication and authorization of the user. If user have access permission to selected file, the media player will decrypt it and open for user, otherwise the user will be treated as leaker and automatic notification will be send to owner of the file.
- Proxy Server: A proxy server acts as an intermediary for requests from users seeking media files from other servers (cloud). Proxies were invented to add structure and encapsulation to distributed systems. When a proxy server receives a request to download the shared media file, then cloud sends the encrypted media file to proxy server. Proxy server will embed the watermark bytes by fetching owner id and user id in some order. The watermarking done here is called as re-encryption of media file. After re-encryption that file would be available for downloading but in encrypted format.

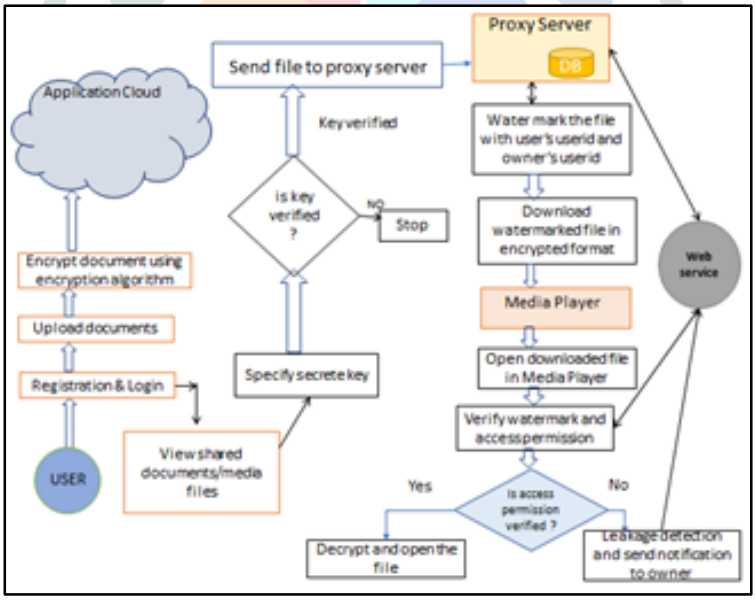


**Figure No. 1:** Working of the System

## IV. RESULTS AND DISCUSSION

Table 4.1: Comparison of size of file before and after encryption

| Type of file | Size of file | Encryption Time | Decryption time | Encryption size |
|---|---|---|---|---|
| Doc | 349.191 | 35.1273 | 0.524288 | 349.191 |
| Doc | 349.191 | 30.933 | 33.0301 | 349.191 |
| Doc | 743.365 | 51.3802 | 72.3517 | 743.365 |
| Video | 2417.99 | 27479 | 17513.3 | 2417.99 |
| Audio | 743.365 | 43007.3 | 53.4774 | 743.365 |
| Image | 248.931 | 2334.13 | 2491.94 | 248.931 |

Our work is

thoroughly associated to the contour of work on secure data sharing in cloud computing. In this work we encapsulate the idea of proxy-based re-encryption with the technique of watermarking which leads to make the system secure and allow the system to detect the leakage of files to unauthorized user. With this, we have achieved the target of minimizing the encryption size after encryption and watermarking. Following table illustrates the size of media files before encryption and after encryption. Also, table depicts the encryption and decryption time.

## V. CONCLUSIONS

The major focus of our work is to prevent as well as to detect the leakage of multimedia content to unauthorized user. In the existing system all efforts had made for traitor tracing. Whereas, in our work we first prevent the illegal access by the usage of media player. Media player would decrypt the downloaded media file if and only if access permissions are verified. Watermark will be checked at the time of download due to which leakage will be prevented. However, if in case media content is leaked out then traitor tracing would be carried out with help of watermark embedded in file.

Another factor is the technique used for encryption and watermarking. We used new encryption algorithm is very secure as it is not well known and doesn't increase size of cipher text after encryption. Similarly, we use our watermark technique which is encoded first by our encryption algorithm and then re-encrypted those bits into encrypted media file. Another objective we achieved is to maintain the size of the file after encryption and watermarking.

## REFERENCES


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

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

**[3]** Prassanna.J, Punitha.K and Neelanarayanan.V, "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 ( 2015 ) pp.543 – 550.

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

**[5]** Amna Qureshi , Helena Rifa-Pous and David Megias ," 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, 2016, pp.1-9.

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

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

**[8]** Nurul shamimi kamaruddin , amirrudin kamsin, lip yee por, and hameedur rahman, "A Review of Text Watermarking: Theory, Methods, and Applications", IEEE. Translations and content mining, January, 2018.

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

**[10]** Dr. Amit Verma, 2Navdeep Kaur Gill, "Analysis of Watermarking Techniques", InternatIonal Journal of Computer SCIenCe and technology, Vol. 7, ISSue 1, Jan - March 2016.

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

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

**[13]** Ankitha.A.Nayak, Venugopala P. S, Dr. H. Sarojadevi, Dr.Niranjan.N. Chiplunkar, "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 2014, pp.39-44.

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

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

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

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

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

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

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

**[21]** Yoshihiro Kawahara, Liang Wang and Tohru Asami, "Resilient Suppressor Mechanism against Illegal Content Redistribution on Peer-to-Peer Video Sharing Networks", IEEE Communications Society, 210.

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

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

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

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

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

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

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

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

**[30]** Baohua Chen1, Na Zhao, "Fully Homomorphic Encryption Application In Cloud Computing".

**[31]** Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage∗

**[32]** Shucheng Yu∗, Cong Wang†, Kui Ren †, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society,210.

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

**[34]** Panagiotis Papadimitriou," Data Leakage Detection", IEEE Transactions On Knowledge And Data Engineering, VOL. 23, NO. 1, JANUARY 2011.

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