A Survey on Multimedia Content Protection

Supriya A V[1], Prof. Sudheer Shetty[2]

[1]M.Tech, Dept.of CSE, Sahyadri College of Engg. & Management, Mangaluru, Karnataka, India
[2]Professor & HOD, Dept.of CSE, Sahyadri College of Engg. & Management, Mangaluru, Karnataka, India

---***---

Abstract - *To provide rich media services, multimedia computing has emerged as a noteworthy technology to generate, edit, and search media contents, such as images, graphics, video, audio, and so on. Due to tremendous evolution in Internet technologies and multimedia, content copying has become quite effortless. This paper reviews brief literature on multimedia data security over the cloud and multimedia content protection in terms of copy detection.*

***Key Words*: Multimedia, Content protection, Digital Signature, Watermarking, Hashing, Content Based Copy Detection, Cloud computing**

1. INTRODUCTION

There are a number of data types in use today that can be characterized as multimedia data types. These are the elements used for the building blocks of other generalized multimedia environments, platforms, or integrating tools.

The basic types can be described as follows:

Images: There is great variance in the quality and size of storage for still images. Digitalized images are sequence of pixels that represents a region in the user's graphical display. The space overhead for still images varies on the basis of resolution, size, complexity, and compression scheme used to store image. The popular image formats are jpg, png, bmp, tiff.

Audio: An increasingly popular data type being integrated in most of applications is Audio. It is quite space intensive. One minute of sound can take up to 2-3 Mbs of space. Several techniques are used to compress it in a suitable format. The popular audio formats are mp3, wma, wav, ogg.

Video: One on the most space consuming multimedia data type is digitalized video. The digitalized videos are stored as sequence of frames. Depending upon its resolution and size, a single frame can consume up to 1 MB. Also, to have a realistic video playback, the transmission, compression, and decompression require continuous transfer rate. The popular video formats are mp4, wmv, mov, avi, flv.

Advancements in multimedia content creation, recording, processing, its growing popularity and free web hosting facilities resulted in easy duplication of copyrighted contents such as images, audio clips and videos. Illegitimately redistributing such protected content over Internet causes revenue loss for content owners. Such copies also consume significant memory on the storage.

2. RELATED WORK

There is a requirement to protect multimedia data of various types over the cloud, from the point of academic world and business. Number of studies showing the need of security in cloud computing especially for the multimedia content storage and the various proposed techniques to enhance security. Research is being carried out in this regard from past decade.

Er.Shilpi Harnal et al.[1] explained about multimedia supported cloud environment, necessity and challenges in such an environment for rich multimedia communication and computation. They did a survey of different multimedia cloud computing architectures, security and other issues and possible solutions proposed by various authors.

Wenwu Zhu et.al [2] presented the basic concept and a novel framework of multimedia cloud computing. They addressed multimedia cloud computing from two perspectives which are multimedia-aware cloud and cloud-aware multimedia.

Chun-Ting Huang [3] conducted a detailed survey on recent multimedia storage security research activities in association with cloud computing. They concentrated on four hot research areas which are data integrity, data confidentiality, access control, and data manipulation in the encrypted domain.

Prassanna J et al.[4] analyzed an innovative mechanism that technically and systematically logging any data access stored in the cloud along with well supported auditing mechanism using Cloud Information Accountability (CIA) framework. It utilized the homomorphic linear authenticator (HLA) and stochastic masking to promise that the third party audit would not be able to discover any information about the user's precious data or informational content stored on the cloud data storage.

Swapnali More et al. [5] proposed a secure and efficient privacy preserving public auditing scheme. This auditing scheme makes use of Advanced Encryption Standard (AES) algorithm for encryption, Secure Hash Algorithm-2 (SHA-2)for integrity check and RSA signature for digital signature calculation.

Amna Qureshi et al. [6] presented a study of media content protection and its impact on end user privacy. Paper also discussed about recent proposals of Peer-To-Peer(P2P) content distribution system that focus on the mentioned issue. Moreover, various difficulties and open research issues are called attention to.

Sonal Guleria et al. [7] presented a novel framework for access control in cloud to assist the design of security structure and to decrease the complexity of system design and implementation. Author proposed a hybrid approach by combining RSA and Data Encryption Standard (DES) algorithms to encrypt large multimedia content before storing on the cloud.

Tamleek Ali et al. [8] presented architecture for the use of cloud computing for secure distribution of rich multimedia content as well as documents. Proposed Usage Control (UCON) model enforced fine-grained continuous usage control on protected objects residing in the cloud.

A Kahng et al.[9] followed an approach using Watermarking, where some distinct information called watermark is implanted in the multimedia content itself. Content authenticity is verified by searching for the implanted information. This method required inserting watermarks in the media before releasing them and matching after extraction. So this method is not ideal for the content which has been released without watermarks. Watermarking technique is suitable for distributing media content on environments using DVDs and not suitable for ever-growing online videos which would be uploaded to free hosting sites like YouTube.

Avinash Varna et al.[10] suggested a new framework named FASHION, standing for Forensic hASH for informatION for multimedia forensics. Framework used Radon transform and Scale space theory to design alignment component of forensic hash.

J. Lu et al.[11] suggested Content Based Copy Detection (CBCD). In this approach, unique signatures are generated for original contents. Signatures are likewise generated for inquiry (suspected) objects downloaded from online locales. At that point, the closeness is figured amongst original and suspected data to discover potential duplicates.

Mandeep Singh Sandhu et al. [12] described about distributed framework where the data will be distributed across various cloud platforms to make it more secure. To prevent unauthorized access, Simple Mail Transfer Protocol (SMTP) mailing services are used and both Message Digest-5(MD5) along with DES algorithms are used for better encryption of data.

Chun-Shien Lu et al. [13] proposed a method for content management of digital images based on mesh-based image hashing scheme. Method showed significant improvement on image hashing by resisting geometrical distortions over the existing methods.

V Ramachandra et al. [14] proposed Scale-Invariant Feature Transform (SIFT) points based technique to perform video copy detection. The technique computes SIFT points in each view of video and uses the number of matching SIFT points to verify matches. Comparing all SIFT points in each frame of video is not viable for large databases due to the storage overhead and search complexity.

Lingyu Yan et al.[15] proposed a fast feature aggregating method for image copy detection using machine learning based hashing which achieves fast feature aggregation with neighborhood preservation and discrimination enhancement. They projected high-dimensional local features into low dimensional Hamming code thus efficient to compute pair wise similarity by using a simple XOR and bit-count operation, which further improved the efficiency of feature aggregation.

M Diephuis et al.[16] proposed architecture for message privacy preserving copy detection and content identification for images based on the signs of the Discrete Cosine Transform (DCT) coefficients. The architecture allowed for searching in encrypted data and places the computational burden on the server. Sign components of the low frequency DCT coefficients of an image are used to generate a dual set of keys that in turn are used to encrypt the source image and serve as a robust hash that can be queried for content identification.

3. CONCLUSIONS

Due to the exponential growth of online data and revolution in multimedia technologies, multimedia data copying has become quite easy. So provision of security and protection to the data stored in the cloud has become inevitable. In this paper, we conducted a brief survey of various aspects involved in multimedia data security and content protection techniques in cloud environment. By analyzing the related work, we can identify the gaps that need to be addressed in order to achieve more protection to the content. Some of the previous works focus on providing protection to only one type of multimedia data. Many methods use image processing and signal processing techniques which are computationally intensive, time consuming and involve high complexity. There is a need for a simple, single practical solution for multimedia content protection for various types such as audio, video and images based on copy detection which will be quite fast, storage efficient, involving less complexity, with low communication and computational costs yet scalable to large scale databases. Research can be carried out in this direction.

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] Chun-Ting Huang, Zhongyuan Qin and C.-C. Jay Kuo, "Multimedia Storage Security in Cloud Computing: An Overview", 2011 IEEE 13th International Workshop on Multimedia Signal Processing, 2011, pp.1-6.

[4] 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.

[5] 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.

[6] 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 (ICDIM 2016), IEEE, 2016, pp.1-9.

[7] Sonal Guleria and Dr. Sonia Vatta, "To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm", IJAIEM, Volume 2, Issue 6, June 2013.

[8] Tamleek Ali, Mohammad Nauman, Fazl-e-Hadi and Fahad bin Muhaya, "On Usage Control of Multimedia Content in and through Cloud Computing Paradigm", 2010 5th International Conference on Future Information Technology , 2010, pp.1-5.

[9] A. Kahng,J. Lach, W.Mangione-Smith, S.Mantic, I.Markov, M.Potkonjak, P.Tucker, H.Wang and G.Wolfe, "Watermarking techniques for intellectual property protection", in Proc.35th Annu.Design Autom. Conf. (DAC '98), 1998, pp.776-781.

[10] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE Electronic Imaging Symp.—Media Forensics Security, 2010.

[11] J.Lu, "Video fingerprinting for copy identification: From research to industry applications," in Proc. SPIE, 2009, vol. 7254, pp.725402:1–725402:15.

[12] Mandeep Singh Sandhu and Sunny Singla, "An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013.

[13] Chun-Shien Lu, Chao-Yong Hsu, Shih-Wei Sun and Pao-Chi Chang, Robust Mesh-based Hashing for Copy Detection and Tracing of Images", 2004 IEEE International Conference on Multimedia and Expo(ICME)(IEEE Cat.No.04TH8763) , Vol. 1, 2004, pp.731-734.

[14] V. Ramachandra, M. Zwicker, and T. Nguyen, "3D video fingerprinting," 2008 3DTV Conference: The True Vision – Capture, Transmission and Display of 3D Video, 2008, pp. 81–84.

[15] Lingyu Yan, Fuhao Zou, Rui Guo, Lianli Gao, Ke Zhou and Chunzhi Wang, "Feature Aggregating Hashing for Image Copy Detection", Springer Science 2015, DOI 10.1007/s11280-015-0346-0.

[16] M. Diephuis, S. Voloshynovskiy, O. Koval and F. Beekhof, "DCT Sign Based Robust Privacy Preserving Image Copy Detection for Cloud-based Systems", 2012 10th International Workshop on Content - Based Multimedia Indexing (CBMI) IEEE, 2012, pp.1-6.