Survey on: Multimedia Content Protection using Cloud

A. M. Chavan
Dept. of Computer Science and Engineering,
DKTE‘s TEI (An Autonomous Institute), Ichalkaranji, India.
e-mail:chavanaishu@gmail.com

Abstract— There is need for large scale multimedia content protection system. There are varying workloads for which cloud infrastructure provide cost efficiency, rapid development and scalability. Data protection along with security whole together contribute to the success of cloud. Security is very important in today's online world. It is widely accepted that cloud computing has the unrealized ability to make privacy disable. The cloud is been chosen because it provides some security features. The greatest challenge is to process data securely in cloud. One of the factor leading to high performance in cloud is nothing but the security. For the protection purpose, a system for multimedia content protection on cloud infrastructure is presented. The system can be used to protect various multimedia contents such as 2D video and 3D videos, graphics which is animated, images, audios clips etc. Multimedia is the combination of data, text, image, audio, or video in a single application. The system can be deployed on both public cloud and private cloud. Two major components to be considered are method to create signatures of 3D videos and matching engine for multimedia objects. Depth signals are captured from 3D videos. This system detects the duplicated multimedia content that is copyright material in an online environment.

Keywords— *Multimedia, Content protection, Video Signature, Watermarking, Content Based Copy Detection, Cloud computing, Video copy detection, depth signature.*

*****

I. INTRODUCTION

The growth in digital technology and amazing power of processing, computation speed and low in coast, digital equipment's are in hand to hand. Advanced in processing , high quality recording equipment of video, image and audio and also availability of high speed internet and free hosting sites have make duplicate copyrighted material illegal redistribution of media content make bad effect on media content reputation. Very high size and bulk volume of media content on internet finding illegal compromised copies over web of internet become very complex, and computationally expensive operation.

To protect different kinds of multimedia content novel system for multimedia content protection on cloud infrastructure can be used. There are various types of media content, like 2D video, 3D videos, images songs, audio, regular video clips. Due to cloud infrastructure their get a computing hardware and software resources present design can be deployed easily. Because of cloud infrastructure system is cost effective, scalar. System is somewhat complex due to component are as 1) crawler to download media content from huge sits, 2) Signature method to create signature or fingerprint of media content, and 3) distributed matching engine to store signature. Designed system work base on second and third component and utilize off-the-shelf tools for crawler [1].

The contribution of the paper as follows:

- Different types of multimedia content are supportable to the system supports
- Creating 3-D video signatures that captures the depth in stereo content.
- Distributed matching engine that finds the nearest neighbour for large-scale datasets.
- Rigorous evaluation study using real implementation to assess the performance of the proposed system and compare it against the closest works in academia and industry.

II. LITERATURE REVIEW AND RELATED WORK

Watermarking is one of the approach to protect various types of multimedia content, in which some important information about content is embedded. The authority of video is verify by searching the information into watermark. But before releasing the video, watermark is need to insert into them. If video are already realised the watermark approach is not suitable there. Watermark is not suitable for uncontrollable area where videos are rapidly uploaded like YouTube.

M Diephuis et al. [2] proposed an architecture in which contents are identified in images based on DCT (Discrete Cosine Transform) this method also preserves piracy in copy detection. Architecture places the computational burden on the server it searches the encrypted data. Low frequency sign components DCT coefficients of an image are used to generate dual set of keys. These keys are used to encrypt the original image and hash value is calculated for content identification.

A framework to access and control the cloud is presented in Sonal Guleria et al. [3] it facilitates the security of the system and also reduces its complexity. Here combination of encryption algorithms such as RSA and DES are used for better security. Files are encrypted before storing them on cloud.

R. Amirtharathna et al. [4] proposes techniques to avoid the duplication of the contents, these techniques involves the audio fingerprinting along with the K-medoids algorithm. The redistribution of audio contents are totally avoided by using these techniques. From the study of the related work it is clear that there are few techniques to protect the content in Cloud environment.

S. Lee et al. [5] Video fingerprints are feature vectors that differentiate between two different video clips. Video query is identified in database (DB) and the distance between video query and fingerprints in database is identified. Here a video fingerprinting method based on centroid of gradient orientations. Because of this method video is robust against resizing, lossy compression, change in frame rate, etc.

In content based copy detection (CBCD) signature or fingerprint are extracted from original multimedia object. Also from query or suspected object signature are created by downloading form online site. The similarity between two videos are computed and find out the potential duplication between videos. Before CBCD many different methods are introduced for matching the signature are classified into four categories: spatial, temporal, color and transform-domain. Spatial signatures are mainly the block-based and are the most widely used. The drawback of spatial signature is the lack of capacity to recover quickly against large geometric transformations. As compared to spatial signatures, Temporal and color signatures are less robust and they are used to enhance spatial signatures. Transform-domain signatures are difficult to carry out and not widely used in practice [6].

You tube Content ID [7], Vobile VDNA and Mark Monitor [8] used signature method for media protection, and these are industrial examples. The CBCD can help us to protect multimedia contents like 2D and 3D videos, images, audio clips, songs. This system is to be developed on public/ or private cloud. This system has two types of components (i) method to create signatures of 3D videos (ii) Matching engine to check these signatures. Robust Signatures are created for 3D videos that capture the depth signals. By using 3D signature methods we handle the 3D videos.

(i) 3D videos signatures

Content-based copy detection of 3-D videos is a fairly new challenges. We are discus about only two previous works [9] and [10]. The work in [9] computes SIFT points in each frame of video and find the number of matching points called as SIFT points to verify matches whether video content duplicated or not. But for large amount of multimedia data comparing all SIFT points in each frame is not practical. There is storage overhead and search complexity. On the other hand, the work in [10] assumes that the depth maps are given or estimated. Estimating the depth map from stereoscopic videos is quite expensive. The method in [10] is suitable for 3-D videos encoded in the video plus depth format, but not for stereoscopic videos. Proposed method in this paper captures the depth properties without calculating the depth map itself and it is computationally efficient because it does not compare all features in the frame.

There are so many different methods are available for 2-D video copy detection. Hampapuret et al. [11] use the temporal features of the video as the signature. Similarly, Tasdemiret et al.[12] use motion vectors as the signature for each frame. Some methods use colour histograms as signatures, e.g., [11]. The colour histogram signature is prone to global variations in colour which are common when recoding video. Another group of methods use interest points of video frames as signature and by which it determine originality of video. For example, Liuet et al.[13] use local SIFT features as the frame signature.

All of the above 2-D video fingerprinting methods can be implemented in the proposed system. In addition, while some of these methods can be used for 3-D video copy detection, they are designed for 2-D videos, and they ignore the information in different views and the depth of 3-D videos. This information is important especially in the presence of 3-D video transformations such as view synthesis, where views from different viewpoints can be generated using the depth map of the 3-D video. When two new views of video frame are synthesized, the positioning of each pixel in the frame is changed, and some areas are occluded while other areas become visible. The colour, luminance, gradient and even the interest points in each block can change as well when a new view is synthesized. Thus, the extracted signature using any of the 2-D methods will change accordingly. Therefore, when searching for similar signatures, manipulated versions may not be identified. The importance of using signatures that have some information from the depth signal has been shown in [10].

(ii) Distributed matching engine

There are many of the previous works, e.g., [14] which designed a system for image matching, distributed matching engine is general and it can support different types of multimedia objects, including images, 2-D videos, and 3-D videos. To achieve this generality, engine is divided in two stages. In first stage for a given data point there are computed nearest neighbors, and in the second stage based on the object type post-processes the computed neighbors. In many application computing nearest-neighbors is a common problem. The focus of this paper is on distributed techniques that can scale to large datasets such as [14], [15], [16], and [17]. Liao et al. [15] build a multi-dimensional index using R-tree. Lu et al. [16] construct a Voronoi-like diagram using some selected pivot objects. Searching can be done in parallel by grouping the data points around the closest pivots and then assigning them to partitions. The system in [16] is also designed for low dimensional datasets; it did not consider data with more than 30 dimensions. In contrast, in this experiments there is used images and videos with up to 128 dimensions. Aly et al. [14] propose a distributed system for image retrieval. Drawback emerges because of using single machine that directs all the query points, that slowdowns the system. Whereas this system does not use a central machine, and thus it is more robust and scalable.

III. CONCLUSION

Copyright of multimedia data has become very easy due to exponential growth of data in multimedia technologies. Here belief survey has conducted that involve different technologies to protect the multimedia contents. To achieve better protection few gaps are need to be addressed. Only one type of media was protected in the existing approaches. But those approaches were computationally complex and time consuming. So there is need for solution to protect the multimedia content with less complexity, low computational costs and low communication. So research has to be carried out in this direction.

REFERENCES

[1] 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.

[2] 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.

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

[4] R.Amirtharathna, Prevention Mechanism for Redistribution of Audio Contents in Cloud, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, and September 2015.

[5] S. Lee and C. Yoo. Robust video fingerprinting for content-based video identification. IEEE Transactions on Circuits and Systems for Video Technology, 18(7):983–988, July 2008.

[6] J. Lu. Video fingerprinting for copy identification: From research to industry applications. In IS & T/SPIE Electronic Imaging, volume 7254 of SPIE Proceedings, pages 725402–725402. International Society for Optics and Photonics, SPIE, 2009.

[7] S. Ioffe. Full-length video fingerprinting. Google Inc., July 24 2012. US Patent 8229219

[8] E. Metois, M. Shull, and J. Wolosewicz. Detecting online abuse in images. Mark monitor Inc., Apr. 12 2011. US Patent 7925044

[9] V. Ramachandra, M. Zwicker, and T. Nguyen, “3D video fingerprinting,” in Proc. 3DTV Conf.: True Vis.—Capture, Transmiss. Display 3D Video (3DTV’08), Istanbul, Turkey, May 2008, pp. 81–84.

[10] N. Khodabakhshi and M. Hefeeda, “Spider: A system for finding 3D video copies,” in ACM Trans. Multimedia Comput., Commun., Appl. (TOMM), Feb. 2013, vol. 9, no. 1, pp. 7:1–7:20.

[11] A. Hampapur, K. Hyun, and R. Bolle, “Comparison of sequence matching techniques for video copy detection,” in Proc. SPIE Conf. Storage Retrieval Media Databases (SPIE’02), San Jose, CA, USA, Jan. 2002, pp. 194–201.

[12] K. Tasdemir and A. Cetin, “Motion vector based features for content based video copy detection,” in Proc. Int. Conf. Pattern Recog. (ICPR’10), Istanbul, Turkey, Aug. 2010, pp. 3134–3137.

[13] Z. Liu, T. Liu, D. Gibbon, and B. Shahraray, “Effective, and scalable video copy detection,” in Proc. ACM Conf. Multimedia Inf. Retrieval (MIR’10), Philadelphia, PA, USA, Mar. 2010, pp. 119–128.

[14] M. Aly, M. Munich, and P. Perona, “Distributed Kd-Trees for retrieval from very large image collections,” in Proc. Brit. Mach. Vis. Conf. (BMVC), Dundee, U.K., Aug. 2011.

[15] H. Liao, J. Han, and J. Fang, “Multi-dimensional index on hadoop distributed file system,” in Proc. IEEE Conf. Netw., Archit. Storage (NAS’10), Macau, China, Jul. 2010, pp. 240–249.

[16] W. Lu, Y. Shen, S. Chen, and B. Ooi, “Efficient processing of k nearest neighbour joins using Map Reduce,” in Proc. VLDB Endowment (PVLDB), Jun. 2012, vol. 5, no. 10, pp. 1016–1027.

[17] A. Stupar, S. Michel, and R. Schenkel, “Rankreduce – processing k-nearest neighbor queries on top of mapreduce,” in Proc. Workshop Large-Scale Distrib. Syst. Inf. Retrieval (LSDS-IR’10), Geneva, Switzerland, Jul. 2010, pp. 13–18