A Mechanism for Copyrighted Video Copy Detection and Identification

Vaishali Dewar¹, Priya Pise²

¹Savitribai Phule Pune University, Indira College of Engineering and Management, Pune, Maharashtra, India

²Prof. at Savitribai Phule Pune University, Indira College of Engineering and Management, Pune, Maharashtra, India

Abstract: Rapid development in the field of multimedia technology has made easier to store and access large amount of multimedia data. There are lots of easy editing and publishing mechanism available which makes duplication of multimedia data feature very easy which can cause the violation of digital rights. So, copy rights security becomes a critical problem for the mutimedia data over the cloud. This has led to the requiring mutimedia copy protection and detection in a large range of the multimedia applications to find illegallymade duplicated copyrighted multimedia copies over the Internet. Watermarking technique was used for same purpose. Using this technique some distortion like Fourier transformation is added in multimedia copy and to play or view the multimedia object in original form this distortion need to be removed by some softwares or players, which makes dependent on those players. However Content based copy detection (CBCD) technique is independent of any software based dependency and identifies copyrighted materials from its content itself. In this technique signatures are created from content itself using SIFT. Content owners specify multimedia objects that they want to protect. Then, system creates signatures from that file and inserts them in the distributed index. The Crawl component once a day downloads recent objects from online hosting sites. The signatures for a query object are created. After downloading of all objects and the signatures are created, the signatures are matched with all indexed signature. If signature matches then this will trap the site which duplicates copyrighted copy without rights. This is effective mechanism, but to fasten this process we have used Audio video cryptosteganography which adds secrete information in multimedia object itself which can neither be removed nor can be identified visually as watermarks are visible. This secrete information is considered as copyrighted information before forming the digital signature. If this secrete information matches with secrete information from database then all contents in the multimedia will be cross verified using CBCD and in this way copyrighted material will be identified.

Keywords: CBCD-Content based copy detection, cryptosteganography, multimedia objects, SIFT

1. Introduction

Rapid development in the field of multimedia technology has made easier to store and access large amount of multimedia data. There are lots of easy editing and publishing mechanism available which makes duplication of multimedia data feature very easy which can cause the violation of digital rights. So, copy rights security becomes a critical problem for the mutimedia data over the cloud. This has led to the requiring mutimedia copy protection and detection in a large range of the multimedia applications to find illegally-made duplicated copyrighted multimedia copies over the Internet.

Duplication of copyrighted materials makes huge loss to content owners. Consider an example where a party creates a video and sales its copyrights to a hosting party say YouTube which pays for it per view of the video on YouTube to content owner. But if that copyrighted material is leaked and hosted on some different hosting site then it will make loss to Content owner as well as YouTube. So this copyrighted stealing need to be caught. But how ?

2. Proposed Methodology

Watermarking technique was used for same purpose. Using this technique some distortion like Fourier transformation is added in multimedia copy and to play or view the multimedia object in original form this distortion need to be removed by some softwares or players, which makes dependent on those players. We propose a new design that achieves rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources. Along with CBCD mechanism we will use cryptosteganography mechanism to hide secrete copyright information in multimedia object to fasten the copyright detection mechanism. The design is cost effective because it uses the computing resources on demand. The design can be scaled up and down to support varying amounts of multimedia content being protected. The proposed system is fairly complex with multiple components, including:

- 1) Crawler to download thousands of multimedia objects from online hosting sites,
- 2) Signature method to create representative fingerprints from multimedia objects,
- 3) Reference registration where secrete information is inserted in multimedia copy using cryptosteganography
- 4) Distributed matching engine to store signatures of original objects and match them against query objects.

CBCD – Content Based Copy Detection

Content based copy detection (CBCD) technique is independent of any software based dependency and identifies copyrighted materials from its content itself. In this technique signatures are created from content itself using SIFT. Content owners specify multimedia objects that they want to protect. Then, system creates signatures from that file and inserts them in the distributed index. The Crawl component once a day downloads recent objects from online hosting sites. The signatures for a query object are created. After downloading of all objects and the signatures are

Volume 4 Issue 12, December 2015 <u>www.ijsr.net</u> Licensed Under Creative Commons Attribution CC BY created, the signatures are matched with all indexed signature. If signature matches then this will trap the site which duplicates copyrighted copy without rights.



Figure: System Architecture

This is effective mechanism ,but to fasten this process we have used Audio video cryptosteganography which adds secrete information in multimedia object itself which can neither be removed nor can be identified visually as watermarks are visible. This secrete information is considered as copyrighted information before forming the digital signature. If this secrete information matches with secrete information from database then all contents in the multimedia will be cross verified using CBCD and in this way copyrighted material will be identified.

The proposed system can be deployed and managed by any of the three parties mentioned: content owners, hosting sites, or service providers.

- Distributed Index: Maintains signatures of objects that need to be protected;
- Reference Registration: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index and Audio video cryptosteganography adds secrete information in multimedia object itself.
- Query Preparation: Creates signatures from objects downloaded from online sites, which are called query signatures. It then uploads these signatures to a common storage;
- Object Matching: Compares query signatures and secrete information versus reference signatures and secrete information in the distributed index to find potential copies. It also sends notifications to content owners if copies are found;
- Parallel Crawling: Downloads multimedia objects from various online hosting sites. The Distributed Index and Object Matching components form what we call the Matching Engine. The second and third components deal with signature creation. For the Crawling component, we designed and implemented a parallel crawler and used it to download videos from YouTube. The details of the crawler are omitted due to space limitations.

3. Conclusion

In this paper, we presented a content based copy detection system. The system is based on inserting digital signatures using Audio video cryptosteganography which adds secrete information in multimedia object itself as a copyright information in the media itself and authorizing it so that it can be used to fasten the content based copy detection method. This mechanism will help to detect copyrighted multimedia stealing and will help to stop loss to content owner due to illegally duplicating copyrighted material.

References

- [1] Mohamed Hefeeda, Tarek ElGamal, Kiana Calagari and Ahmed Abdelsadek "Cloud-based Multimedia Content Protection System". IEEE, 1520-9210, 2015
- [2] Sunil K Moon, "Application of data hiding in Audio-Video using Anti Forensic Technique for Authentication and Data Security", 978-1-4799-2572-8/14/\$31.00 c 2014 IEEE
- [3] A.PerumalRaja, B.Venkadesan, R.Rajakumar "Efficient Framework for Video Copy Detection Using Segmentation and Graph-Based Video Sequence Matching". IEEE, 2250-3153, Volume 4,9, September 2014
- [4] Hong Liu, Hong Lu, and XiangyangXue,"A Segmentation and Graph-Based Video Sequence Matching Method for Video Copy Detection". IEEE, 2250-1706, Volume 25, NO. 8, AUGUST 2013
- [5] DhanalakshmiSrinivasan,"An Effective Approach for Video Copy Detection and Identification of Misbehaving Users". 0975-9646, Volume. 4 (6) ,863-867, 2013
- [6] Vishwa Gupta, Parisa Darvish, Langis Gagnon, Gilles Boulianne,"CONTENT-BASED VIDEO COPY DETECTION USING NEAREST-NEIGHBOR MAPPING". 4673-0382, Vol.1 (6) ,2013
- [7] Vishwa Gupta, Parisa Darvish, Langis Gagnon, Gilles Boulianne, "VIDEO COPY DETECTION USING INCLINED VIDEO TOMOGRAPHY AND BAG-OF-VISUAL-WORDS". 305-732, Vol.1 (6) ,2012
- [8] Shikui Wei, Yao Zhao, Ce Zhu, ChangshengXu,andZhenfengZhu,"Frame Fusion for Video Copy Detection". IEEE, 305-732, VOL. 21, NO. 1, JANUARY 2011
- [9] Mani MalekEsmaeili, MehrdadFatourechi, and Rabab KreidiehWard,"A Robust and Fast Video Copy Detection System Using Content-Based Finger printing". VOL. 6, NO. 1, MARCH 2011
- [10] Zhu Liu, Tao Liu, David Gibbon, BehzadShahraray,"Effective and Scalable Video Copy Detection". VOL. 1, NO. 1, 2011
- [11]Hye-Jeong Cho, Yeo-Song Lee, Chae-Bong Sohn, Kwang-Sue Chung, and Seoung-Jun Oh,"A NOVEL VIDEO COPY DETECTION METHOD BASED ON STATISTICAL ANALYSIS". VOL. 1, NO. 978-1-4244-4291, 2009
- [12]Zheng Cao, and Ming Zhu ,"An Efficient Video Copy Detection Method Based on Video Signature". VOL. 1, NO. 978-4795-4/09, 2009