www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16001-16004

Copy Detection of Multimedia Contents in Cloud

R. Amirtharathna[1], Mrs. P.Vijayasarathy[2]

[1] Krishnasamy College of Engineering & Technology,
S.Kumarapuram, Cuddalore, Tamilnadu, India
amirtha800@gmail.com

[2] Krishnasamy College of Engineering & Technology,
S.Kumarapuram, Cuddalore, Tamilnadu, India
sarathy.viji@gmail.com

Abstract: ***In Cloud, we describe the ways to enable protection of Multimedia contents from redistributing. Web has billions of documents including video, audio and images, but there is no central management system, where duplication of contents is more common . It is said that each and every document has a duplicate copy. This is more prevelant in videos stored in multiple formats, versions, size etc. and are found unaware by content creators when modified and republished using Video Editorial Tools. This may lead to security problems and also reduplicating the identity of owners and also loss of revenue to content creators. This also occupies a enormous space over the web. In cloud storage too it is more common involving both public and private clouds. But the private cloud is said to be more secure when compared to the public cloud. So to avoid this situation some of the techniques have been used to avoid duplication of contents and focused mainly over the 3D-video contents.***

Keywords: reduplication, public/private cloud, Signatures, Greedy Optimization Technique.

1. Introduction

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

Advances in processing and recording equipment of Audio content as well as the free availability of free online hosting sites have made it relatively easy to duplicate copyrighted materials like audio, video and music clips. Finding illegally made copies over the internet is a complex and computationally expensive operation. We present a novel system for Audio content protection on cloud infrastructures to protect the audio contents. The system can run on private clouds, public cloud, or any combination of public/private clouds. The system can be used to protect variation in audio content. Our system achieves rapid deployment deployment of audio content because it is based on cloud infrastructures that can quickly provide computer hardware and software resources. The design is cost effective because it uses computing resources on demand. The design can be scaled up and down to support varying amounts of audio content be protected.

The proposed system involves (i)a crawler to download the audio content from online hosting sites (ii) signature that has been created (iii) object matching process. Through experimental results the system proves flexibility since it is being deployed in both private and the public clouds. The system is said to be cost effective since the cloud preferred is mainly our own cloud and not needed to pay to the Amazon like private clouds. It is said to be offering high accuracy since experiments with real deployment in terms of precision with RankReduce.

The contributions of this paper are as follows.

- Complete multi-cloud system for audio content protection. The system supports different types of audio content and can effectively utilize varying computing resources.
- Signatures are created based on steganography process.
- A matching engine to match the audio contents.
- The audio contents used in our system are subjected to various transformations such as blurring, cropping, resizing etc. and also subjected to various complex transformations such as synthesizing new virtual views and converting the audios to anaglyph and other depth formats.

2. Existing System

The availability of free online sites have made easy to duplicate copyrighted materials. To prevent and avoid copyrighting, Copy Detection Mechanism has been done for the multimedia contents. Copy Detection is a process of detecting illegally copied videos by analyzing them and comparing them with the original content. It is based on the length of the film and works only for whole films without

modifications. On applying to short clips of a video[4] it does not detect that the clip is a copy. The Copy Detection involves: (i) Watermarking that introduce an invisible/visible signal into video to ease the detection of illegal copies. Placing Watermark[1] on video such that it is easily seen by audience allow content creator to detect easily whether image is copied. (ii) Spatial Signature – Fingerprint that creates a unique signature of video based on the spatial feature that is size of the contents. (iii) Temporal Signature – A Temporal Signature is a detectable phenomenon which defines the objects position in time. (iv) Color Signature – The Color Signature is based on the color level of image created an algorithm that examines the colors of a clip by creating a binary signature from every frame.

2.1 Disadvantages

- If the original images are not watermarked[1], then it is not possible to detect the images are copies.
- Though the Spatial Signatures are created based on the shape and size of the multimedia contents it leads to loss of resilience that is flexibility.
- Though the Temporal and Color Signatures are created based on time duration and color of the multimedia contents it said to be less robust in nature.

3. Proposed System

To avoid the problem of illegally redistributing multimedia contents, Signatures are created and then undergo Copy Detection of multimedia contents are done and then alert the users. It could be done by involving, (i) Digital Signature Algorithm (DSA) (ii) Greedy Optimization Technique (GOT) (iii) Pattern Matching Algorithm (PMA).

3.1 Advantages of Proposed System

- Datas are maintained with high accuracy.
- Avoid redistributing and duplication of multimedia contents.
- Scalability is achieved – Capability to handle the growing amount of work[2].
- Elasticity is achieved.
- Flexibility – Offers ability or capability of being changed or adjusted to meet particular or varied needs.
- Robust – It is the ability to continue operating despite of abnormalities (fault tolerance).
- Protect the user identity from leakage or revealing.

4. Paper Description

This paper addresses the problem of redistributing the multimedia contents over the web and this could be done involving various techniques and the processing could be done as follows.

4.1 Digital Signature Algorithm (DSA)

Involving fingerprinting mechanism the depth signatures are created by capturing depth properties that are the distance of the surface of scene object from viewpoints. Contents are taken and undergone signing is done with private key and public key along with hash function and now the content is now verified using user's public key, global public key and then compared.

4.2 Greedy Optimization Technique (GOT)

In this technique, duplication is identified even after transformation. Here optimal solution could be obtained from a set of feasible solutions that is transformations are done by undergoing midpoint segmentation by splitting the full motion video into frames by identifying the midpoints involve pixel partitioning and each centre to be point themselves.

4.3 Pattern Matching Algorithm (PMA)

The Pattern Matching Algorithm is that used to find the match of pattern of length M in a multimedia stream of length N. Here the original content with signature i.e. reference register is compared with the embedded or the queried signature are compared and alerts the users in cloud when detected.

4.4 Privacy Preserving Technique

A privacy preserving mechanism[5] is done that utilize ring signatures to construct homomorphic authentication that allow computation to be done on cipher text. Ring Signature is that involving the identity of the signer to be hidden and kept secret from other members involved.

5. System Architecture

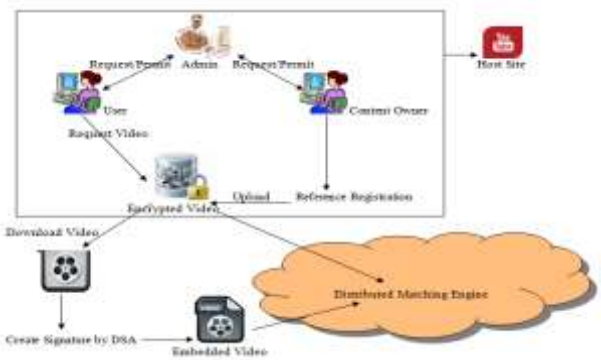

Figure 1: System Architecture

In the above figure the Copy detection of the similarities are being identified and the alert is being sent to both the content owner as well as warning is sent to the user who tries to upload the similar content and protects the content from being uploaded. This could be done when the multimedia contents are being embedded with signature created using the Digital Signature Algorithm and involving the Greedy Optimization technique and then by using the Distributed Matching Engine the contents are allowed to be compared in Cloud. Thus prevents the contents from copyrighting and also reduce the revenue loss that occurs to the Content Owners.

6. Steps Involved

The following are the steps involved,

- Upload Sequence Video
- Analysis and Testing Process
- Signature Creation
- Video Embedding
- Upload the Embedded Video and same Content Video in Cloud Server
- Copy Detection

7. 1 Upload Sequence Video

The Videos like 2D, 3D, also audio[3] contents, text data and other relevant videos are uploaded into the system. It could be loaded from the system and hosted. After hosting the text and video contents in the space those contents are loaded and played in the space available. Then for each text content and the 2D, 3D, image or audio content their corresponding ASCII values are being obtained.

7. 2 Analysis and Testing process

Initially the text document and videos like 2D, 3D, audio or image content are being loaded and their corresponding ASCII conversions are obtained. Now the input files information are obtained along with their storage path and the files are analyzed and tested so that the input files like text, 2D-video, 3D-video, audio or images are being loaded and processed successfully.

7. 3 Signature Creation

In this process, the signature is created with the help of the Digital Signature Algorithm (DSA) can be used by the recipient of a message to verify that the message has not been altered during transit as well as ascertain the originator's identity. A digital signature is an electronic version of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. It involve the contents to be taken and undergo signing with private and public key along with hash function and then the contents are then verified using user's public key along with global public key are compared.

7. 4 Video Embedding

In this process, initially we will take the original video and signature in which we have to embed into original image. Then we have to convert the video file into number of frames, we consider each frame as an image. Here we set the counter value to frames. Then we have converted the text data into binary format. Binary conversion is done by taking the ASCII value of each character and converting those ASCII values into binary format. We are going to set the counter value to the length of the binary message, so that the loop repeats that much times.

7. 5 Upload the Embedded Video and same Content Video in Cloud Server

In this process, the input signature i.e., upload the Embedded Video and same Content Video is uploaded with the server authenticated signatures and an automatic signature upload should assess whether a questioned signature is an authentic signature normally used by the reference writer[8]. These parameters were evaluated with different classifiers such as nearest neighbor[7].

7. 6 Copy Detection

In this process, the system compares the signatures by verifying the embedded video and the same content video[4] that is hosted by user by automatically checking the hosted data that is the data that was originally hosted by content owner with signature created with the help of reference register in the cloud server storage space along with the similar 2D,3D video[6], text document, audio content[3] or image that is hosted by the user and thus when similar contents are detected the system alerts the content owner that someone is trying to host the similar multimedia content in the host site and thus also warns the user that the content already exist and thus block the contents from uploading .

7. Experimental Results

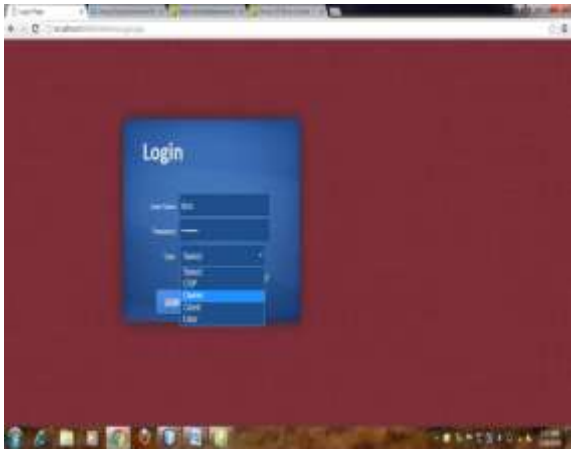

Figure 2: Login Page

Figure 3: Upload Video

Figure 4: Load Content

8. Conclusion

The Copy Detection of Multimedia Contents in Cloud is that there millions of Multimedia contents are present in web. It is said that nearly 50% of the entire text document has atleast one duplicate copy. It is prevalent with Multimedia contents too. So in the host site the Content Owner would upload and test the text files, 2D-videos, 3D-videos and audio contents and the Signatures are created by involving Digital Signature Creation in the reference registration and the users either view or download the contents involving the key generated by the admin. Also that content appears to be in embedded form in the site. The homomorphic encryption involved prevents the signer identity from revealing their user identity. This enhances security in the system and also scalability is achieved. Further the system is said to more robust in nature.

9. Other Recommendations

The Multimedia contents uploaded in the site would support only the mpeg format at present. But the future work is that the current system could be extended in such a way that they would involve all formats of Multimedia content and text file, the formats may support jpeg, mpeg, mpg, avi, png files etc. Also the security in the system would also be extended by making the system more secure than the present system.

Acknowledgement

This paper is prepared based upon the following references and to the best of our knowledge all the datas addressed are correct and true.

References

[1] Kahng, J. Lach, W. Mangione-Smith, S. Mantik, 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)*, San Francisco, CA, USA, Jun. 1998, pp. 776–781.

[2] 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.

[3] P. Cano, E. Batle, T. Kalker, and J. Haitsma, "A review of algorithms for audio fingerprinting," in *Proc. IEEE Workshop Multimedia Signal Process.*, Dec. 2002, pp. 169–173.

[4] S. Lee and C. Yoo, "Robust video fingerprinting for content-based video identification," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 7, pp. 983–988, Jul. 2008.

[5] Boyang Wang, Baochum Li, Member, IEEE and Hui Li, Member, IEEE, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", in *Proc. IEEE*.

[6] 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.

[7] 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.

[8] J. Bentley, "Multidimensional binary search trees used for associative searching," in *Commun. ACM*, Sep. 1975, vol. 18, no. 9, pp. 509–517.

[9] J. Dean and S. Ghemawat, "MapReduce: Simplified data processing on large clusters," in *Proc. Symp. Oper. Syst. Design Implementation (OSDI'04)*, San Francisco, CA, USA, Dec. 2004, pp. 137–150.

Author Profile

R.Amirtharathna is a PG Scholar (Student of M.E./CSE) in Computer Science & Engineering Department, in Krishnasaour College of Engineering and Technology, Tamil Nadu, India. She received Bachelor of Engineering (B.E.) degree in 2014 from Krishnasaour College of Engineering and Technology, S.Kumarapuram, Cuddalore, Tamil Nadu, India. Her research interests are Cloud Computing, Multimedia etc.

Mrs.P.Vijayasarathy is a faculty working as Assistant Professor in the Department of Computer Science & Engineering in Krishnasamy College of Engineering & Technology, S.Kumarapuram, Cuddalore, Tamilnadu, India since 2009.