ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Prevention Mechanism for Redistribution of Audio Contents in Cloud

R.Amirtharathna

PG Scholar, Dept. of CSE, Krishnasamy College of Engineering & Technology, Cuddalore , Tamil Nadu, India

ABSTRACT: Web has billions of documents available. It is said that each and every document has a duplicate copy. This may lead to security problems and also reduplicating the identity of owners. 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 audio content. Those techniques involve the Audio Fingerprinting along with the K-medoids Algorithm and thus prevent the reduplication of the audio content.

KEYWORDS: Web Crawler, reduplication, public/private cloud, Signatures, K-medoids Algorithm, Audio-Fingerprint.

I. 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 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.

II. Related work

In the Related Works, distribution of copyrighted audio contents by uploading them to online hosting sites like YouTube can produce loss of income and stealing of their contents and less efficient to the content creators. Watermark is not efficient to them. Watermarking [10] is a method that introduces an invisible or visible signal to ease the detection of illegal copies. Placing watermark over the content enable the content owner to easily identify that the content has been watermarked. Another method is by involving Spatial Signatures where the fingerprints are created based on the size of the contents [5] [15]. YouTube Content ID [9], Vobile VDNA, and Mark Monitor are some of the industrial examples which use fingerprinting for media protection, while methods such as [12] can be referred to as the academic state-of-the-art. Unlike previous works, the contribution of this paper is to design a large-scale system to find copies that can be used for different types of audio content and can leverage multi-cloud infrastructures to minimize the cost, expedite deployment, and dynamically scale up and down.

The drawbacks in the related works are as below:

- If the original image is not watermarked, then it is not possible to detect original images are copies.
- It causes loss of security of the content as well as the owner.
- This also enables loss of revenue to the content creators.
- This method causes loss of resilience.
- Also this system is that be less efficient.
- The Spatial Signatures are created based on the size of the audio contents it leads to loss of resilience

III. Proposed technique

A. *Design Considerations:*

To avoid the problem of illegally redistributing the audio contents in cloud, Signatures are created and then undergo Copy Detection mechanism and then alerts the owners as well as the users when detected with similarities. It could be done by involving,

- Steganography
- K-medoids algorithm
- K-nearest algorithm
- Pattern matching
- Audio Fingerprinting

The advantage of the proposed technique is that it offers high accuracy, flexibility, minimized cost, elasticity and scalability.

B. *Description of the Proposed Technique:*

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

Step 1: Steganography:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Steganography includes the concealment of information within computer files.

Step 2: K-medoids Algorithm:

In general, K-medoids is a classical partitioning technique of clustering that clusters the data set of n objects into k clusters known a priori. Also k-medoids is used here in a way such that the audio is split into frames and in each frame its centres are identified as similar to k-means. But here the centres are points themselves. The centre of the images is found and then involves the midpoint segmentation by the way of pixel partitioning and then process. In this paper it is used for partitioning the audio file as frames and then identifying the midpoint of each frame. The process is as follows:

1. Initialize: randomly select (without replacement) *k* of the *n* data points as the medoids
2. Associate each data point to the closest medoids.
3. While the cost of the configuration decreases:
   - For each medoids *m*, for each non-medoids data point *o*:
   - Swap *m* and *o*, recompute the cost
   - If the total cost of the configuration increased in the previous step, undo the swap.

Step 3: K-nearest Algorithm:

In this paper, the k-nearest neighbor algorithm is used in identifying the closest neighbor in accessing the contents from the cloud. K-Nearest Neighbors algorithm (or k-NN for short) is a non-parametric method used for classification and regression [16]. In both cases, the input consists of the k closest training examples in the feature space. The output depends on whether k-NN is used for classification or regression:

- In k-NN classification, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its k nearest neighbors (k is a positive integer, typically small). If k = 1, then the object is simply assigned to the class of that single nearest neighbor.
- In k-NN regression, the output is the property value for the object. This value is the average of the values of its k nearest neighbors.

Step 4: Distributed Matching Engine:

It compares query signatures versus reference signatures in the distributed index to find potential copies [6]. It also sends notifications to content owners if copies are found and also alerts the user that the content has been existing already and prevents from uploading. Here the Pattern Matching Technique is used even after undergoing various transformations the similarities could be detected.

Step 5: Audio Fingerprinting:

An audio fingerprint is a content-based compact signature that summarizes an audio recording. Audio Fingerprinting [12] technologies have recently attracted attention since they allow the monitoring of audio independently of its format and without the need of meta-data or watermark embedding. Audio fingerprinting is best known for its ability to link unlabeled audio to corresponding metadata [5] (e.g. artist and song name), regardless of the audio format. Although there are more applications to audio fingerprinting, such us: Content-based integrity verification or watermarking [10] support, this review focuses primarily on identification. Audio fingerprinting or Content-based audio identification (CBID) systems extract a perceptual digest of a piece of audio content, i.e. the fingerprint and store it in a database. When presented with unlabeled audio, its fingerprint is calculated and matched against those stored in the database. Using fingerprints and matching algorithms, distorted versions of a recording can be identified as the same audio content.

IV. System Architecture

Step 1: Developing Cloud Server:

Dropbox like cloud server could be used to store the audio content and here it is the own private cloud that has been created and do not involve the other private clouds like Amazon and others since they are not cost effective and are to be paid at regular duration.

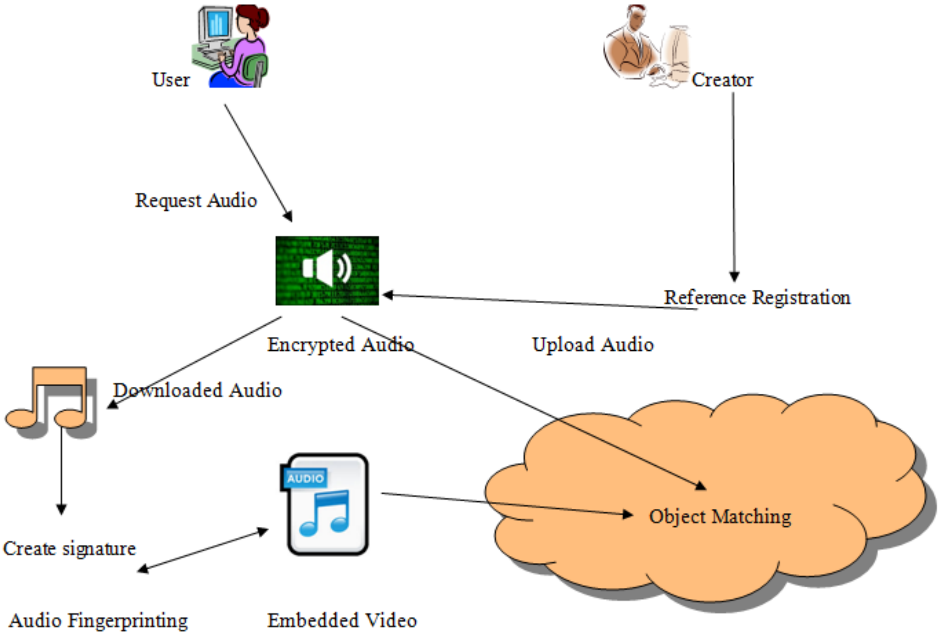


Fig. 1 System Architecture

Step 2: Signature Creation:

Depth signatures are being created involving the depth properties of the audio content that is by involving the characteristics such as the distance of the surface of scene objects from viewpoints. This signature [5] [15] is created and then further embedded into the audio that has been uploaded by the content creator. This signature creation is made by Reference Registration as the content owner wants to protect the content. The signatures are then embedded into the content by various processes.

Step 3: Object Matching Process:

The object matching involves comparing the query signature with the original one and gets the alert when notified by the similarities in content even after undergoing some complex as well as simpler transformations.

Step 4: Audio Fingerprinting:

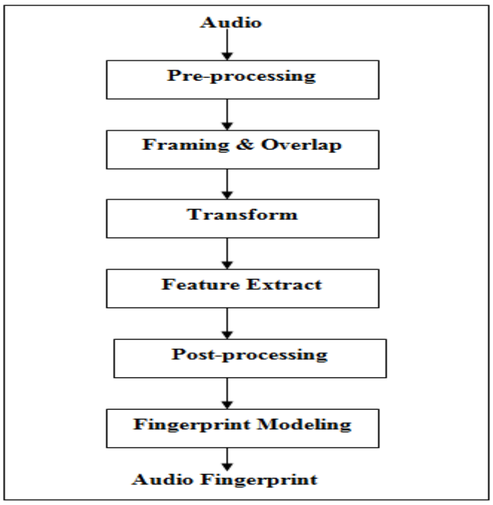


Fig. 2 Audio Fingerprinting

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Based on these processes the fingerprinting is being done for that audio content and thus audio is being changed into the audio fingerprinted file.

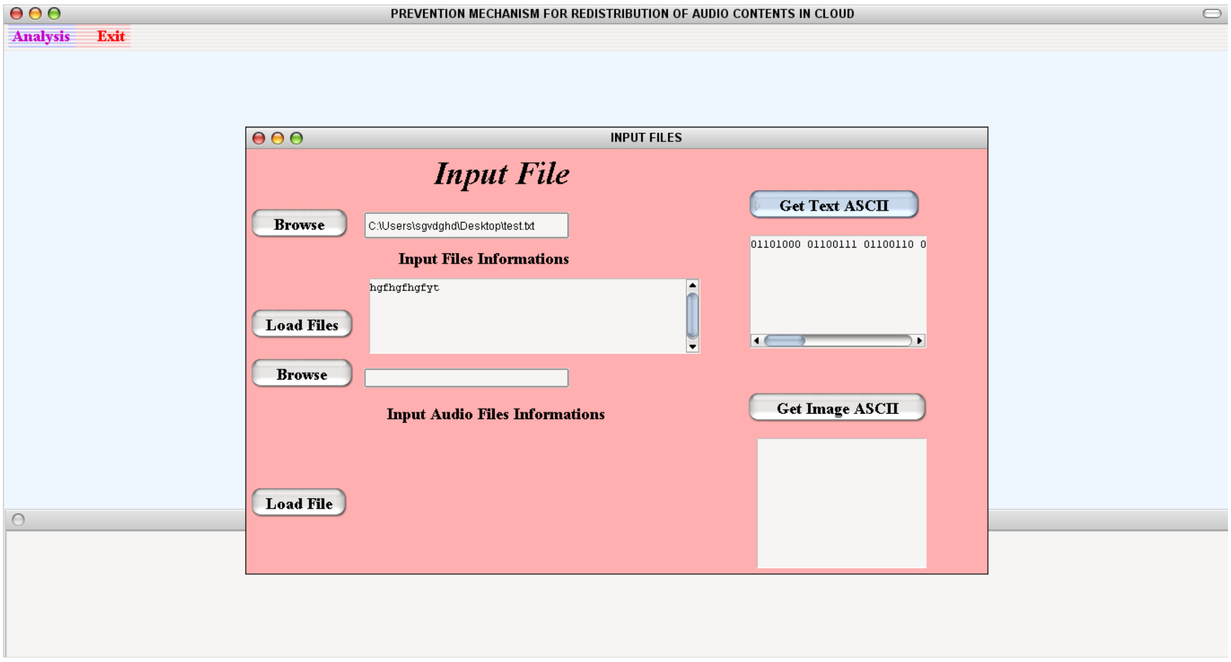
V. Experimental Setup

The experimental setup requires the following hardware and software requirements as minimum needs in carrying out the paper.

• SYSTEM	: PENTIUM IV 2.4 GHZ.
• HARD DISK	: 40 GB.
• MONITOR	: 15 INCH VGA COLOR.
• MOUSE	: LOGITECH MOUSE.
• RAM	: 512 MB
• KEYBOARD	: STANDARD KEYBOARD
• OPERATING SYSTEM	: WINDOWS XP
• PLATFORM	: JAVA TECHNOLOGY
• TOOL	: NETBEANS 6.9.1
• FRONT END	: JDK 1.7
• BACK END	: MYSQL 5.0

VI. Experimental Results

This experimental result shows that the input files are loaded and its corresponding ASCII values are obtained for both text and audio files respectively.



C:\Users\sgvdghd\Desktop\test.txt

hgfhgfhgfyt

01101000 01100111 01100110 0

Fig. 3 Obtaining Text File ASCII

VII. Conclusion and Future Work

In this paper the process of redistributing the audio contents are completely avoided and the system proved to be much effective than the other existing techniques and thus offers flexibility, robustness, computational efficiency, scalability in terms of both scale up and scale down and thus proved to be much effective and privacy preserving.

Hence in this paper we focus on the security of the audio contents. But further it could be extended to all types of multimedia contents including the images, text, video clips, 2D-videos, 3D-videos etc. and they also could be subjected to all sorts of transformation and further improvements could be made to enhance the security of both the contents as well as the content owners.

VIII. ACKNOWLEDGEMENT

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

REFERENCES

1. Abdelsadek, “Distributed index for matching multimedia objects,” M.S. thesis, School of Comput. Sci., Simon Fraser Univ., Burnaby, BC, Canada, 2014.
2. A. Abdelsadek and M. Hefeeda, “Dimo: Distributed index for matching multimedia objects using MapReduce,” in *Proc. ACMMultimedia Syst. Conf. (MMSys’14)*, Singapore, Mar. 2014, pp. 115–125.
3. 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.
4. J. Bentley, “Multidimensional binary search trees used for associative searching,” in *Commun. ACM*, Sep. 1975, vol. 18, no. 9, pp. 509–517.
5. 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.
6. 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.
7. J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, “Imagenet: A large-scale hierarchical image database,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recog. (CVPR’09)*, Miami, FL, USA, Jun. 2009, pp. 248–255.
8. 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.
9. S. Ioffe, “Full-length video fingerprinting. Google Inc.,” U.S. Patent 8229219, Jul. 24, 2012.
10. A. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. J. Lu, “Video fingerprinting for copy identification: From research to industry applications,” in *Proc. SPIE*, 2009, vol. 7254, pp. 725402:1–725402:15.
16. W. Lu, Y. Shen, S. Chen, and B. Ooi, “Efficient processing of k nearest neighbor joins using MapReduce,” in *Proc. VLDB Endowment (PVLDB)*, Jun. 2012, vol. 5, no. 10, pp. 1016–1027.

BIOGRAPHY

R.Amirtharathna is a PG Scholar in the Computer Science & Engineering Department, in Krishnasamy College of Engineering and Technology, Tamil Nadu, India. She received Bachelor of Engineering (B.E.) degree in 2014 from Krishnasamy College of Engineering and Technology, Tamil Nadu, India. Her research interests are Cloud Computing, Multimedia etc.