International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 5 Ver VI || May 2018 || PP 26-29

A Secure System For Multiedia Content Protection Using 3d Signatures

Mrs. Shubhangi B. Aradle[1], Prof. V.R.Chirchi[2]
PG Student, PG Department, MBES College of engineering. Ambajogai, Maharashtra.
Assistant Professor, PG Department, MBES College of engineering, Ambajogai, Maharashtra.
Correspoonding Auther: Mrs. Shubhangi B. Aradle

Abstract
Cloud Computing is a resellient means flexible it also cost-effective, and robust platform for business or consumer Information Techonology services over the world wide web. Security and data protection are important for cloud success. Cloud Computing prestiges to many technologies and also inherits their protection issues. The integration of these types is commonly known as multimedia. Cloud Computing is a very expressive, expand technology that could provide cost-effectiveness. Multimedia Systems is complete entire, digitilized. It is only computer controlled system and interactive. Content protection system can be used to secure a various multimedia content that is Text, pictures as Images, Audio Songs and 2-D and 3D video system. It can be exert on private as well as public cloud system. This system has two novel components:
1. Create signatures of 3-D videos.
2. Distributed matching engine for multimedia content.
Keywords – *Cloud computing, Multimedia system, 3-D videos, Distributed matching, Security, Exert.*

Date of Submission: 10-05-2018 Date of acceptance: 28-05-2018

I. Introduction

Exactly what is cloud that cloud is a big server. It accessing the data by using WAN. Now a days it is widely used in IT companies. It requires hardware and software resources. Cloud computing data is access by a remoteiy control system with user information and software application. Cloud computing apply in high performance computing like miltery application. The proposed system is fairly complex with the component, including (i) crawler to download thousands of multimedia objects from online hosting sites, (ii) signature method to create representative fingerprints from multimedia objects, and (iii) distributed matching engine to store signatures of original objects and match them against query objects. We propose novel methods for the second and third components, and we utilize off-the-shelf tools for the crawler. We have developed a complete running system of all components and tested it with more than 11,000 3-D videos and 1 million images. We deployed parts of the system on the Amazon cloud with varying number of machines (from eight to 128), and the other parts of the system were deployed on our private cloud. This deployment model

was used to show the flexibility of our system, which enables it to efficiently utilize varying computing resources and minimize the cost, since cloud providers offer different pricing models for computing and network resources. Through extensive experiments with real deployment, we show the high accuracy (in terms of precision and recall) as well as the scalability and elasticity of the proposed system.

The contributions of this paper are as follows.

• Complete multi-cloud system for multimedia content protection. The system supports different types of multimedia content and can effectively utilize varying computing resources.

• Novel method for creating signatures for 3-D videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process.

• New design for a distributed matching engine for high-dimensional multimedia objects. This design provides the primitive function of finding -nearest neighbors for large-scale datasets. The design also offers an auxiliary function for further processing of the neighbors. This two-level design enables the proposed system to easily support different types of multimedia content. For example, in finding video copies, the temporal aspects need to be considered in addition to matching individual frames.

II. Literature Review

A.B.Kahng, J.Lach, W.H.Mangione-Smith, S. Mantik, I.L.Markov[1] "Waterarking techniques for Intellectual Property Protection"

Advantages- The problem of protecting various types of multimedia content has attracted significant attention from academia and industry. One approach to this problem is using watermarking, in which some distinctive information is embedded in the content itself and a method is used to search for this information in order to verify the authenticity of the content.

Disadvatages- Watermarking approach may not be suitable for already-released content without watermarks in them. Watermarking may not be effective for the rapidly increasing online videos, especially those uploaded to sites such as YouTube and played back by any video player.

Jian Lu[2] " Video fingerprinting for copy identification: from research to industry application"

Advantages- In this approach, signatures (or fingerprints) are extracted from original objects. Signatures are also created from query (suspected) objects downloaded from online sites. Then, the similarity is computed between original and suspected objects to find potential copies.

Many previous works proposed different methods for creating and matching signatures. These methods can be classified into four categories: spatial, temporal, color, and transform-domain. Spatial signatures (particularly the block-based) are the most widely used.

Disadvatages- Spatial signatures weakness is the lack of resilience against large geometric transformations. Temporal and color signatures are less robust and can be used to enhance spatial signatures. Transform-domain signatures are computationally intensive and not widely used in practice

Petro Cano and Eloi Batlle, Ton Kalker and Jaap Haitsma[3]" A Review of Algo for Audio Fingerprinting"

An audio fingerprint is a content-based compact signature that summarizes an audio recording. Audio Fingerprinting 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. The different approaches to fingerprinting are usually described with different rationales and terminology depending on the background Pattern matching, Multimedia (Music) Information Retrieval or Cryptography (Robust Hashing).

Sunil Lee[4]" Robust Video Fingerpriting for Content Based video Identification"

Youtube Content ID, Vobile VDNA, and MarkMonitor are some of the industrial examples which use fingerprinting for media protection, while methods such as can be referred to as the academic state-of-the-art. Video fingerprints are feature vectors that uniquely characterize one video clip from another. The goal of video fingerprinting is to identify a given video query in a database by measuring the distance between the query fingerprint and the fingerprints in the database. The performance of a video fingerprinting system, which is usually measured in terms of pair wise independence and robustness, is directly related to the fingerprint that the system uses.

R. Amirtharathna et al. [5]"Prevention Mechanism for Redistribution of Audio Contents in Cloud"

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.

III. Proposed System

System present a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types. In our proposed system present complete multi-cloud system for multimedia content protection. The system supports different types of multimedia content and can effectively utilize varying computing resources. Novel method for creating signatures for videos. This method creates signatures that capture the depth in stereo content without computing the depth signal itself, which is a computationally expensive process. New design for a distributed matching engine for high-dimensional multimedia objects. This design provides the primitive function of finding -nearest neighbors for large-scale datasets. The design also offers an auxiliary function for further processing of the neighbors. This two-level design enables the proposed system to easily support different types of multimedia content. The focus of this paper is on the other approach for protecting multimedia content, which is content-based copy detection (CBCD). In this approach, signatures are extracted from original objects. Signatures are also created from query (suspected) objects downloaded from online sites. Then, the similarity is computed between original and suspected objects to find potential copies

ADVANTAGES OF PROPOSED SYSTEM:

1. Accuracy.
2. Computational Efficiency.
3. Scalability and Reliability.
4. Cost Efficiency.
5. The system can run on private clouds, public clouds, or any combination of public-private clouds.

6. Our design achieves rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources.
7. The design is cost effective because it uses the computing resources on demand.
8. The design can be scaled up and down to support varying amounts of multimedia content being protected.

MODULES:
1. Data owner Module
2. Data User Module
3. Encryption Module
4. Rank Search Module

IV. Modules Description:

Data owner Module

Protect different multimedia content types, including images, audio clips, songs, and music clips. The system can be deployed on private and/or public clouds. Our system has two novel components: (i) method to create signatures (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage.

Data User Module

Matching engine achieves high scalability and it is designed to support different multimedia objects. implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud. Our experiments with more than 11,000 and 1 million images show the high accuracy and scalability of the proposed system. In addition, we compared our system to the protection system used by YouTube and our results show that the YouTube protection system fails to detect most copies, while our system detects more than 98% of them

Encryption Module

Multimedia content protection systems using multi-cloud infrastructures .The proposed system supports different multimedia content types and it can be deployed on private and/or public clouds. Two key components of the proposed system are presented. The first one is a new method for creating signatures. Our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image.

Rank Search Module

Rank needs to store the whole reference dataset multiple times in hash tables; up to 32 times. On the other hand, our engine stores the reference dataset only once in bins. Storage requirements for a dataset of size 32,000 points indicate that Rank needs up to 8 GB of storage, while our engine needs up to 5 MB, which is more than 3 orders of magnitude less. These storage requirements may render Rank not applicable for large datasets with millions of points, while our engine can scale well to support massive datasets.

V. Conclusion

The system presented a new design for multimedia content protection systems using multi-cloud infrastructures. The proposed system supports different multimedia content types and it can be deployed on private and/or public clouds. Two key components of the proposed system are presented. The first one is a new method for creating signatures of 3-D videos. Our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image. Thus, it captures the depth signal of the 3-D video, without explicitly computing the exact depth map, which is computationally expensive. Our experiments showed that the proposed 3-D signature produces high accuracy in terms of both precision and recall and it is robust to many video transformations including new ones that are specific to 3-D videos such as synthesizing new views.

The work in this paper can be extended in multiple directions. For example, our current system is optimized for batch processing. Thus, it may not be suitable for online detection of illegally distributed multimedia streams of live events such as soccer games. In live events, only small segments of the video are available and immediate detection of copyright infringement is crucial to minimize financial losses. To support online detection, the matching engine of our system needs to be implemented using a distributed programming framework that supports online processing, such as Spark. So research has to be carried out in this direction

Referance

[1]. [1] 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.

[2]. [2] J. Lu, “Video fingerprinting for copy identification: From research to industry applications,” in Proc. SPIE, 2009, vol. 7254, pp. 725402:1–725402:15.

[3]. [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]. [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]. [5] 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.

[6]. [6] Mohamed Hefeeda , Senior Member, IEEE, Tarek ElGamal , Kiana Calagari, and Ahmed Abdelsadek, “Cloud-Based Multimedia Content Protection System”, **IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 17, NO. 3, MARCH 2015.**

[7]. [7] W. Lu, Y. Shen, S. Chen, and B. Ooi, “Efficient pro

[8]. cessing of k nearest neighbor joins using MapReduce,” in Proc. VLDB Endowment (PVLDB), Jun. 2012, vol. 5, no. 10, pp. 1016–1027.

[9]. [8] E. Metois, M. Shull, and J. Wolosewicz, “Detecting online abuse in images. Markmonitor Inc.,” U.S. Patent 7925044, Apr. 12, 2011. [18] H. Müller, W. Müller, D. Squire, S. Marchand-Maillet, and T. Pun,

[10]. [9] P. Ram and A. Gray, “Which space partitioning tree to use for search,” in Proc. Adv. Neural Inf. Process. Syst. (NIPS’13), Lake Tahoe, NV, USA, Dec. 2013, pp. 656–664.

[11]. [10] 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.

Mrs. Shubhangi B. Aradle "A Secure System For Multiedia Content Protection Using 3d Signatures "International Journal of Engineering Science Invention (IJESI), vol. 07, no. 05, 2018, pp 26-29