International Conference on Advance Studies in Engineering and Sciences
Sri Satya Sai University of Technology and Medical Sciences , Sehore (M.P.) ICASES-17
2nd December 2017, www.conferenceworld.in ISBN: 978-93-86171-83-2

Multimedia data Security of cloud based System

Mahale Rahul Bhaskar[1],Mr. Kailash Patidar[2] Mr. Manojkumar Yadav[3]

[1]M.Tech Scholar ,[2]Head of Department CSE, [3] Asst. Professor, CSE

SSSUTMS, Sehore,M.P (India)

ABSTRACT

We implemented the proposed system and deployed it on two clouds: Amazon cloud and our private cloud. Our experiments with more than 11,000 3-D videos 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 of 3-D videos, while our system detects more than 98% of them. This comparison shows the need for the proposed 3-D signature method, since the state-of-the-art commercial system was not able to handle 3-D videos. We propose a new design for large-scale multimedia content protection systems. Our design leverages cloud infrastructures to provide cost efficiency, rapid deployment, scalability, and elasticity to accommodate varying workloads.

Keywords:(CBCD): content-based copy detection

I.INTRODUCTION

We present a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types, including regular 2-D videos, new 3-D videos, images, audio clips, songs, and music clips. The system can run on private clouds, public clouds, or any combination of public-private clouds. 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. 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: (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.

1.1 Overview of Cloud Based System

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 [10], 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. Watermarking requires inserting watermarks in the multimedia objects before releasing them as well as mechanisms/systems to find objects and verify the existence of correct watermarks in them. Thus, this approach may not be suitable for already-released content without watermarks in them. The watermarking approach is more suitable for the somewhat controlled environments, such as distribution of multimedia content on DVDs or using special sites and custom players. 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. Watermarking is not the focus of this paper. The focus of this paper is on the other approach for protecting multimedia content, which is content-based copy detection (CBCD) [15]. 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. However, their 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. For more details, see surveys for audio fingerprinting [5] and 2-D video fingerprinting [15]. Youtube Content ID [9], Vobile VDNA,1 and MarkMonitor [17] 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 multimedia content and can leverage multi-cloud infrastructures to minimize the cost, expedite deployment, and dynamically scale up and down. That is, we design our system such that previous content-based copy detection methods for creating and matching signatures can be implemented within our system. In addition to our cloud-based system, we propose a new method for 3-D video fingerprinting, and a new design for the distributed matching engine.

1.2 Key Concept of Multimedia data Security of cloud based System

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.

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.

1.3 Types of data Security.

such as:

1.3.1 3-D Video Signatures

Content-based copy detection of 3-D videos is a fairly new problem; we are aware of only two previous works [20] and [11]. The work in [20] computes SIFT points in each view and buses the number of matching SIFT points to verify matches. Comparing all SIFT points in each frame is not practical for large databases due to the storage overhead and search complexity. On the other hand, the work in [11] assumes that the depth maps are given or estimated. Estimating the depth map from stereoscopic videos is quite expensive. The method in [11] is suitable for 3-D videos encoded in the video plus depth format, but not for stereoscopic videos. Our 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.

1.3.2 Distributed Matching Engine

Our proposed 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, we divide the engine into two main stages. The first stage computes nearest neighbors for a given data point, and the second stage post-processes the computed neighbors based on the object type. In addition, our design supports high-dimensionality which is needed for multimedia objects that are rich in features. Computing nearest neighbors is a common problem in many applications. Our focus in this paper is on distributed techniques that can scale to large datasets such as [13], [16], [3], [21]. Liao et al. [13] build a multi-dimensional index using R-tree on top of the Hadoop distributed file system (HDFS). Their index, however, can only handle low dimensional datasets—they performed their experiments with two dimensional data. They solve the nearest neighbors over large datasets using MapReduce [6]. Lu et al. [16] construct a Voronoi-like diagram using some selected pivot objects. They then group the data points around the closest pivots and assign them to partitions, where searching can be done in parallel. The system in [16] is also designed for low dimensional datasets; it did not consider data with more than 30 dimensions. In contrast, in our experiments we used images and videos with up to 128 dimensions. Aly et al. [3] propose a distributed system for image retrieval.

II.LITERATURE SURVEY

2.1 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.

2.2 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.

2.3 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.

III. PROBLEM IDENTIFICATION

3.1 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.

3.2 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.

IV.PROPOSED METHODOLOGY

4.1 We present a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types.

4.2 In our proposed system we present complete multi-cloud system for multimedia content protection. The system supports different types of multimedia content and can effectively utilize varying computing resources.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

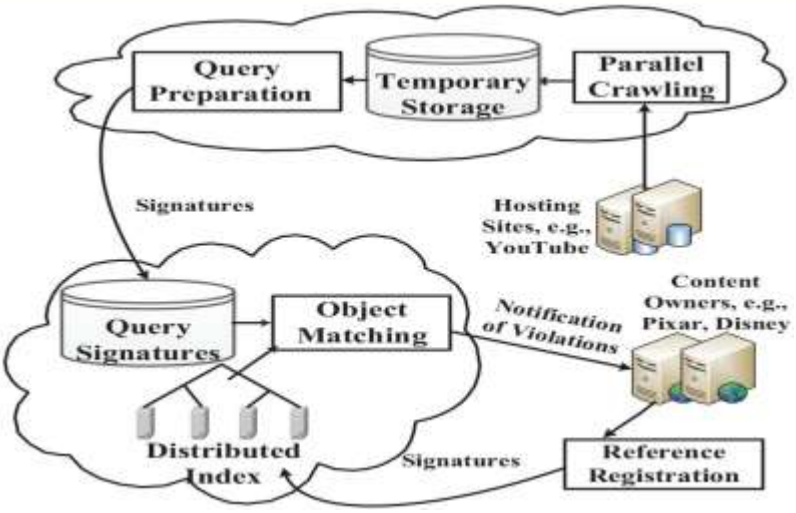
V.EXPERIMENTAL RESULT

5.1 Design Goals and Approaches A content protection system has three main parties: (i) content owners (e.g., Disney), (ii) hosting sites (e.g., YouTube), and (iii) service providers (e.g., Audible Magic). The first party is interested in protecting the copyright of some of its multimedia objects, by finding whether these objects or parts of them are posted on hosting sites (the second party). The third party is the entity that offers the copy finding service to content owners by checking hosting sites. In some cases the hosting sites offer the copy finding service to content owners. An example of this case is YouTube, which offers content protection services. And in other, less common, cases the content owners develop and operate their own protection systems. We define and justify the following four goals as the most important ones in multimedia content protection systems.

• Accuracy: The system should have high accuracy in terms of finding all copies (high recall) while not reporting false copies (high precision). Achieving high accuracy is challenging, because copied multimedia objects typically undergo various modifications (or transformations). For example, copied videos can be

subjected to cropping, embedding in other videos, changing bit rates, scaling, blurring, and/or changing frame rates. Our approach to achieve this goal is to extract signatures from multimedia objects that are robust to as many transformations as possible. • Computational Efficiency: The system should have short response time to report copies, especially for timely multimedia objects such as sports videos. In addition, since many multimedia objects are continually added to online hosting sites, which need to be checked against reference objects, the content protection system should be able to process many objects over a short period of time. Our approach to achieve this goal is to make the signatures compact and fast to compute and compare without sacrificing their robustness against transformations. • Scalability and Reliability: The system should scale (up and down) to different number of multimedia objects. Scaling up means adding more objects because of monitoring more online hosting sites, having more content owners using the system, and/or the occurrence of special events such as sports tournaments and release of new movies. Conversely, it is also possible that the set of objects handled by the system shrinks, because, for example, some content owners may terminate their contracts for the protection service. Our approach to handle scalability is to design a distributed system that can utilize varying amounts of computing resources. With large-scale distributed systems, failures frequently occur, which require the content protection system to be reliable in face of different failures. To address this reliability, we design the core parts of our system on top of the MapReduce programming framework, which offers resiliency against different types of failures. • Cost Efficiency: The system should minimize the cost of the needed computing infrastructure. Our approach to achieve this goal is to design our system to effectively utilize cloud computing infrastructures (public and/or private). Building on a cloud computing infrastructure also achieves the scalability objective discussed above and reduces the upfront cost of the computing infrastructure.

5.2 Architecture and Operation The proposed cloud-based multimedia content protection system is shown in Fig. 1. The system has multiple components; most of them are hosted on cloud infrastructures. The figure shows the general case where one or more cloud providers can be used by the system. This is because some cloud providers are more efficient and/or provide more cost saving for different computing and communication tasks. For example, a cloud provider offering lower cost for inbound bandwidth and storage can be used for downloading and temporarily storing videos from online sites (top cloud in the figure), while another cloud provider (or private cloud) offering better compute nodes at lower costs can be used to maintain the distributed index and to perform the copy detection process (lower cloud in the figure). The proposed system can be deployed and managed by any of the three parties mentioned in the previous section: content owners, hosting sites, or service providers. The proposed system has the following main components, as shown in Fig. 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;

• 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 versus reference signatures 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, which is described in Section V. The second and third components deal with signature creation, which is described in Section IV. 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. The proposed system functions as follows. Content owners specify multimedia objects that they are interested in protecting. Then, the system creates signatures of these multimedia objects (called reference objects) and inserts (registers) them in the distributed index. This can be one time process, or a continuous process where new objects are periodically added. The Crawl component periodically (e.g., once a day) downloads recent objects (called query objects) from online hosting sites. It can use some filtering (e.g., YouTube filtering) to reduce the number of downloaded objects. For example, for video objects, it can download videos that have a minimum number of views or belong to specific genre (e.g., sports). The signatures for a query object are created once the Crawl component finishes downloading that object and the object itself is removed. After the Crawl component downloads all objects and the signatures are created, the signatures are uploaded to the matching engine to perform the comparison. Compression of signatures can be performed before the upload to save bandwidth. Once all signatures are uploaded to the matching engine, a distributed operation is performed to compare all query signatures versus the reference signatures in the distributed index.

VI.CONCLUSION

Distributing copyrighted multimedia objects by uploading them to online hosting sites such as YouTube can result in significant loss of revenues for content creators. Systems needed to find illegal copies of multimedia objects are complex and large scale. In this paper, we 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 second key component in our system is the distributed index, which is used to match multimedia objects characterized by high dimensions. The distributed index is implemented using the MapReduce framework and our experiments showed that it can elastically utilize varying amount of computing resources and it produces high accuracy. The experiments also showed that it outperforms the closest system in the literature in terms of accuracy and computational efficiency. In addition, we evaluated the whole content protection system with more than 11,000 3-D videos and the results showed the scalability and accuracy of the proposed system. Finally, we compared our system against the Content ID system used by YouTube. Our results showed that: (i) there is a need for designing robust signatures for 3-D videos since the current system used by the leading company in the industry fails to detect most modified 3-D copies, and (ii) our proposed 3-D signature method can fill this gap, because it is robust to many 2-D and 3-D video transformations. 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. In addition, composite signature schemes that combine multiple modalities may be needed to quickly identify short video segments. Furthermore, the crawler component needs to be customized to find online sites that offer pirated video streams and obtain segments of these streams for checking against reference streams, for which the signatures would also need to be generated online. Another future direction for the work in this paper is to design signatures for recent and complex formats of 3-D videos such as multiview plus depth. A multiview plus depth video has multiple texture and depth components, which allow users to view a scene from different angles. Signatures for such videos would need to capture this complexity, while being efficient to compute, compare, and store.

REFERENCES

[1] A. 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 Map Reduce," 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, "Map Reduce: 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] 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.