

# Novel System for Multimedia Content Protection on Cloud Infrastructures

**Syeda Ayesha Siddiqua**

*M. Tech Scholar*

*Department of Computer Science & Engineering*

*Princeton College of Engineering & Technology, Ghatkesar,*

*RR Dist., Telangana*

**Prof. Ashok Verma**

*Associate Professor & Head of Dept.*

*Department of Computer Science & Engineering*

*Princeton College of Engineering & Technology, Ghatkesar,*

*RR Dist., Telangana*

## Abstract

In this paper, 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. The proposed system can be used to protect different multimedia content types, including 2-D videos, 3-D videos, 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 of 3-D videos, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage. The distributed matching engine achieves high scalability and it is designed to support different multimedia objects. 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. This work is implemented using .net tool.

**Keywords:** 3D, Cloud computing, Multimedia, image

## I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides an emerging paradigm where computing resources make available as service of the Internet. This paradigm provides facility to Customer to Consumer and businesses without installation of this application and provides access to personal files at any computer with internet access. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. This also provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Upon these benefits, there are privacy and security concerns too. For the past few years, cloud-based storage has oscillated somewhere between a replacement strategy for existing back-up storage solutions (i.e. tape) and a typically inexpensive but complex real-time storage solution for online web properties and enterprises. Data transmission and storage can fall under many regional regulations involving the security and availability of personal information. Multimedia can be defined as multi and media, where multi means many, much or multiple and medium means an intervening substance through some data is transmitted or carried on. Multimedia is typically used to mean the combination of different content forms such as text, audio, images, animation, video and interactive content.

Advances in processing and recording equipment of multimedia contents as well as the availability of free online hosting sites have made it relatively easy to illegally duplicate copyrighted materials such as videos, songs, images, and music clips. Copyright is the legal protection of all forms creative expression on any form of media. Copying and illegally redistributing multimedia contents over the Internet can result in significant loss of revenues for content creators. Protecting Various Multimedia Contents such as video and image by signature creation and Multimedia copy detection using matching index.

The objective of the project is design a novel system for multimedia content protection on cloud infrastructures and to achieve rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources

## II. PROPOSED WORK

The goal of the proposed system for multimedia content protection is to find illegally made copies of multimedia objects over the Internet. In general, systems for multimedia content protection are large-scale and complex with multiple involved parties. In this section, we start by identifying the design goals for such systems and our approaches to achieve them. Then, we present the high-level architecture and operation of our proposed system.

### A. 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.

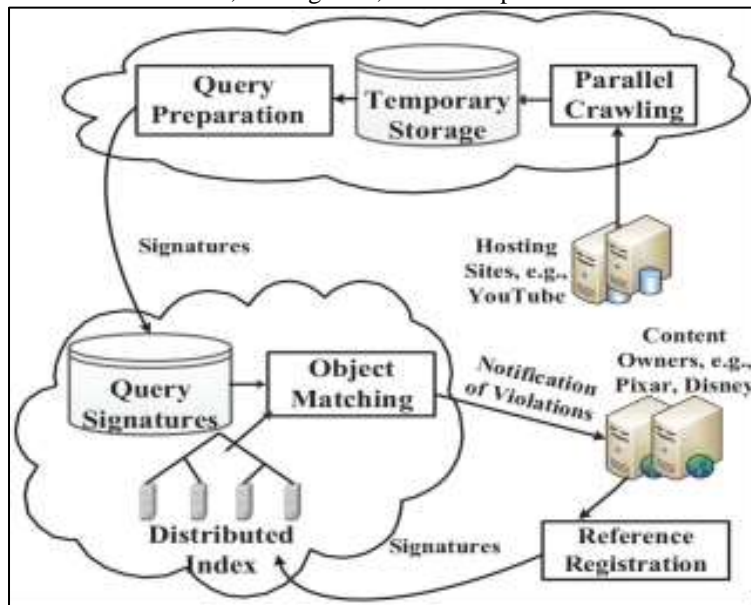


Fig. 1: shows proposed cloud-based multimedia content protection system.

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.

## **B. Signature Creation:**

The proposed system is designed to handle different types of multimedia objects. The system abstracts the details of different media objects into multi-dimensional signatures. The signature creation and comparison component is media specific, while other parts of the system do not depend on the media type. Our proposed design supports creating composite signatures that consist of one or more of the following elements:

- Visual signature: Created based on the visual parts in multimedia objects and how they change with time;
- Audio signature: Created based on the audio signals in multimedia objects;
- Depth signature: If multimedia objects are 3-D videos, signatures from their depth signals are created;
- Meta data: Created from information associated with multimedia objects such as their names, tags, descriptions, format types, and IP addresses of their uploaders or downloaders.

The proposed method is composed of the following main steps.

- 1) Step 1) Compute Visual Descriptors for Left and Right Images.
- 2) Step 2) Divide Each Image Into Blocks.
- 3) Step 3) Match Visual Descriptors
- 4) Step 4) Compute Block Disparity.
- 5) Step 5) Compute Signature.

## **C. Modules Implemented**

### *1) Data owner Module*

Protect different multimedia content types, including 2-D videos, 3-D videos, 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 of 3-D videos, and (ii) distributed matching engine for multimedia objects. The signature method creates robust and representative signatures of 3-D videos that capture the depth signals in these videos and it is computationally efficient to compute and compare as well as it requires small storage.

### *2) Data User Module*

Matching engine achieves high scalability and it is designed to support different multimedia objects. 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

### *3) 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 of 3-D videos. Our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image.

### *4) 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.

## **III. SIMULATION RESULTS & DISCUSSIONS**

The software packages used in our proposed are Microsoft .NET and Microsoft SQL Server 2000 Meta Data Services.

A. User:



Fig. 2: project user window



Fig. 3: shows registration form window

This section covers the snapshots that show the results of the proposed work. The snapshots are self-explanatory. The result varies from input to input. The snapshot makes the user understand easily the working operations in the project work



Fig. 4: shows user login



Fig. 5: shows search option



Fig. 6: shows search file details



Fig. 7: shows file upload option



Fig. 8: shows file upload details

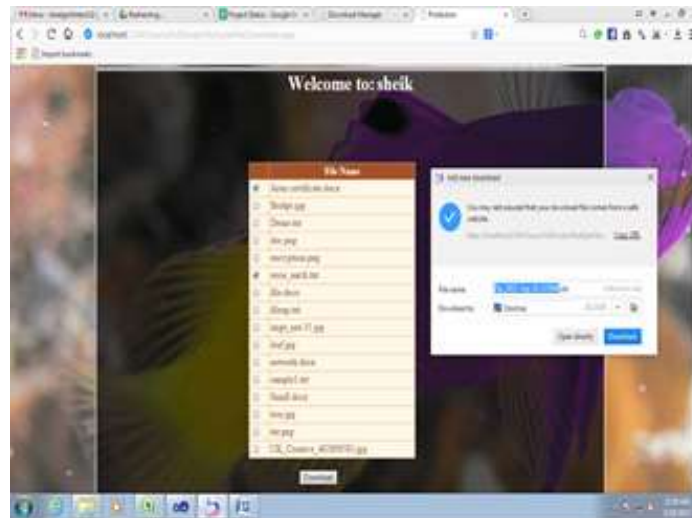


Fig. 9: shows file name and downloaded



Fig. 10: shows profile created details



Fig. 11: shows graph

**B. Admin**

The screenshot shows the 'ADMIN' section of the system. It displays a table with the following columns: user, login, status, last, time, ip, email, and password. The data is as follows:

user	login	status	last	time	ip	email	password
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789

Fig. 12: shows ADMIN details

The screenshot shows the 'FILES' section of the system. It displays a table with the following columns: user, login, status, last, time, ip, email, and password. The data is as follows:

user	login	status	last	time	ip	email	password
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789
Like Content System	sheik	ok	2/14/2013	8:30:21 AM	192.168.1.1	sheik@sheik.com	123456789

Fig. 13: shows file uploaded and ID details



Fig. 14: shows file uploaded details

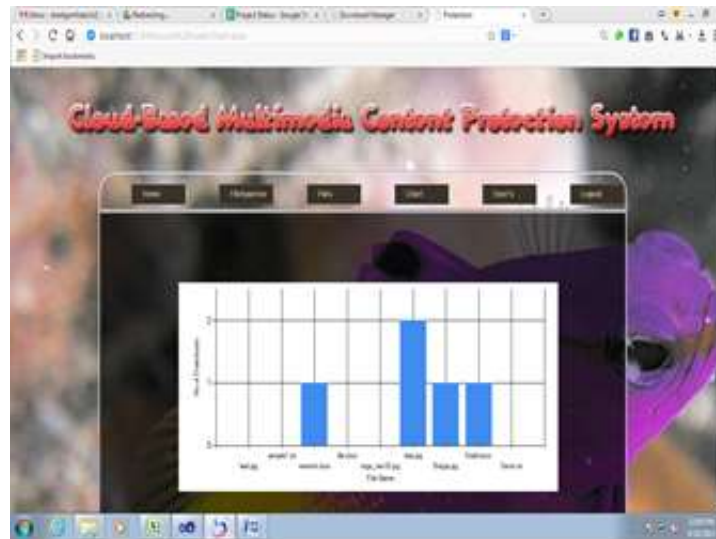


Fig. 15: shows graph

The screenshot displays a table of registered user profiles. The table has columns for Sno, Name, Email, User Name, Password, Date of Birth, and City.

Sno	Name	Email	User Name	Password	Date of Birth	City
1	dash	dash@gmail.com	dash	dash	25-01-1993	Shimoga
2	madhu	madhu@gmail.com	madhu	madhu	23-03-1993	Shimoga
3	hira	hira@gmail.com	hira	hira	2-08-1997	Tyler
4	hansa	hansa@gmail.com	hansa	hansa	4-11-1994	Maduru
5	haha	haha@gmail.com	haha	haha	8-1-1994	Tyler
6	madhu	madhu@gmail.com	madhu	madhu	25-01-1993	Shimoga

Fig. 16: shows details profile registered



## IV. CONCLUSION AND FUTURE WORK

### A. Conclusion

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.

### B. Future Work

In future we will provide protection of Multimedia content using Hadoop system. In addition, quickly identifying short video segments using composite signature schemes.

## REFERENCES

- [1] Sonal Guleria and Dr. Sonia Vatta, To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm, IJAIEM, Volume 2, Issue 6, June 2013.
- [2] Er. Mandeep Singh Sandhu and Er. Sunny Singla, An Approach to Enhanced Security of Multimedia Data Model Technology Based on Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013.
- [3] Priyanka Gupta, Amandeep Kaur Brar, An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server, International Journal of Engineering Research and Applications Vol. 3, Issue 4, Jul-Aug 2013.
- [4] Vaishali Dewar, Priya Pise, A Mechanism for Copyrighted Video Copy Detection and Identification, International Journal of Science and Research (IJSR), 2013.
- [5] Ujwala Pawar, Prof. Dhara T. Kurian, Security of Multimedia Data Transmission stored on Cloud – Watermark Technique, iPGCON-2015.
- [6] Youjin Song, Yasheng Pang, An Approach of Risk Management for Multimedia Streaming Service in Cloud Computing, International Journal of Multimedia and Ubiquitous Engineering, Vol.9, No.4 , 2014.
- [7] 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.
- [8] Mani Malekesmaeili, Mehrdad Fatourehchi, and Rabab K. Ward, Video Copy Detection Using Temporally Informative Representative Images, International Journal of Engineering Research and Applications 2014.
- [9] V. Ramachandra, M. Zwicker, and T. Nguyen, 3D Video Finger-printing, in Proc. 3DTV Conf.: True Vis. — Capture, Transmiss. Display 3D Video (3DTV'08), Istanbul, Turkey, pp. 81–84, May 2008.
- [10] Aleksandar Stupar, Sebastian Michel, Ralf Schenkel, RankReduce – Processing K-Nearest Neighbor Queries on Top of MapReduce, LSDS-IR'10.