**Cloud-Based Multimedia Content Protection System**

**ABSTRACT:**

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.

**EXISTING 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, 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.
* 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.
* 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.

**DISADVANTAGES OF EXISTING 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.

**PROPOSED SYSTEM:**

* We 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 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.
* 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:**

* Accuracy.
* Computational Efficiency.
* Scalability and Reliability.
* Cost Efficiency.
* 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.

**SYSTEM ARCHITECTURE:**



**MODULES:**

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

**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. We 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.