National Conference on Innovations in Computing and Networks (NCICN) - 2019
©2019 IJSRSET | Volume 5 | Issue 9 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099

Cloud-Based Multimedia Content Protection

Salini S Nair*[1], Dr. T. Mahalakshmi[2], Athulya S U[3]
*[1]Assistant Professor, Sree Narayana Institute of Technology, Kerala, India
[2]Principal, Sree Narayana Institute of Technology, Kerala, India
[3]Student, Sree Narayana Institute of Technology, Kerala, India

ABSTRACT

Web has millions of multimedia contents such as videos and images. It may happen that each and every multimedia content has duplicated copies. There is lots of mechanism available that provides easy way for editing, publishing or uploading multimedia contents so that it may leads to security problem and also reduplicating the identity of content owner and also loss of revenue to the content owner. So that this system can be used to protect the multimedia contents such as 3D videos or images from duplication. The main goal of this system is to provide cost efficiency, rapid development, scalability and elasticity to accommodate varying workloads and improve the accuracy as well as computational efficiency and also the reliability. This system can be deploying on cloud concept. Cloud is used to store and retrieve the multimedia contents which are uploaded on the web. This is considered as a small view for the whole system and this system show high accuracy for some videos and images.

Keywords : Multimedia Content security, Depth Signature Algorithm, Key generation

I. INTRODUCTION

Now a days, multimedia contents and availability of free online hosting sites have made it easy to duplicating copyrighted material, like images and videos for finding illegally made copies over internet is complex. In this system, there are three methods which are present first are Crawler to downloads the multimedia contents, Signature creation method for downloaded multimedia contents, Distributed matching engine to match the multimedia contents. This system can be deployed on cloud. It is helpful for all content owners and also cloud supports the different multimedia contents. This can be used to utilize the computing resource on their demand. The contributions of this paper are as follows Parallel crawler to download thousands of multimedia contents

from various online hosting sites. The 64-bit division algorithm can be used to create signature. This method create signature based on the downloaded multimedia contents. The signature is in the form of numbers that is binary packet format .This created signature is stored in distributed index. Another method to match the match the signature which is stored in distributed index. The Depth first search algorithm is used to matching multimedia contents. If this signature is matched in distributed index then the system gives notifications that the contents are matched and if signature is not matched then through reference register it stored in distributed index. When we upload a new video or images then they get a key for providing security. For downloading any uploaded video or image then corresponding key is required that is get from SMS when we request to download it.

II. METHODS AND MATERIAL

In this system a user can upload videos and images then it is divided into binary packets. For that this system use a new concept called Depth Signature. And here it is used to check the similarities between the contents. That

means the contents are divided into frames and compared with the contents in cloud for security.

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

Here also a key generation is implemented for giving extra security for the content. This means when a user uploads a video or image then they gets a key as SMS generated by the system. And for downloading the corresponding content from the cloud the user need to enter the key and this is get from the SMS when the user request the content for search.

III. IMPLEMENTATION

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. 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) Compute Visual Descriptors for Left and Right Images- Visual descriptors are local features that describe salient parts of an image. Different types of descriptors can be used, including Speeded-Up Robust Feature (SURF), Scale Invariant Feature Transform (SIFT), and HOG (Histogram of Oriented Gradients). The default descriptor used in our method is SURF. Each descriptor has a fixed number of dimensions or features. For example, each SURF descriptor has 64 dimensions. Each descriptor is computed at a specific pixel in the image, which has a location of . The result of this step is two sets of descriptors; one for the left image and one for the right image where and are the number of descriptors in the left and right images, respectively and is the number of dimensions in each descriptor.

2) Divide Each Image Into Blocks- Both the left and right images are divided into the same number of blocks. In general, blocks can be of different sizes and each can be a square or other geometrical shape. In our implementation, we use equal-size square blocks. Thus, each image is divided into blocks.

3) Match Visual Descriptors- For each visual descriptor in the left image, we find the closest descriptor in the right image. We consider the block that the descriptor is located in and we find its corresponding block in the right image. We draw a larger window around this corresponding block. This is done to account for any slight changes in the visual objects between the left and right views. Different types of similarity measures can be used to compute the distance between feature vectors. In our implementation, we use the Euclidean distance to compute the distance between descriptors. We compute the distance between each visual descriptor in the left image and all descriptors in the corresponding block of the right image. The corresponding match is the descriptor with the smallest distance.

4) Compute Block Disparity- We compute the block disparity between each block in the left image and its corresponding block in the right image. The disparity of a single descriptor is given by where is the position of descriptor in the left image, and is the position of the corresponding descriptor in the right image. We normalize the disparity by the width and the height of each block in the image. The disparity of block is denoted by and computed as the average disparity of all visual descriptors in that block. If a block or its corresponding block in the right image does not have any descriptor, the disparity is set to 0.

5) Compute Signature- We note that the signature is compact and fixed in size as the total number of blocks is fixed and small. In summary, our method constructs coarse-grained disparity maps using stereo correspondence for a sparse set of points in the image. Stereo correspondence tries to identify a part in an image that corresponds to a part in the other image. A finegrained disparity map of a pair of images describes

the displacement needed for each pixel to move from one image to the correct position in the other image. The disparity map is inversely proportional to the depth map, meaning that the disparity is larger for objects near the camera than objects far away from the camera. Since fine-grained disparity maps are expensive to compute, we create our signature from coarse-grained disparity maps, which are computed from blocks of pixels.

IV. RESULTS AND DISCUSSION

This is a novel system for multimedia content protection on cloud infrastructures. The system can be used to protect various multimedia content types. In 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. Here is a 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. 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.
There are some screenshot of this work is given below:

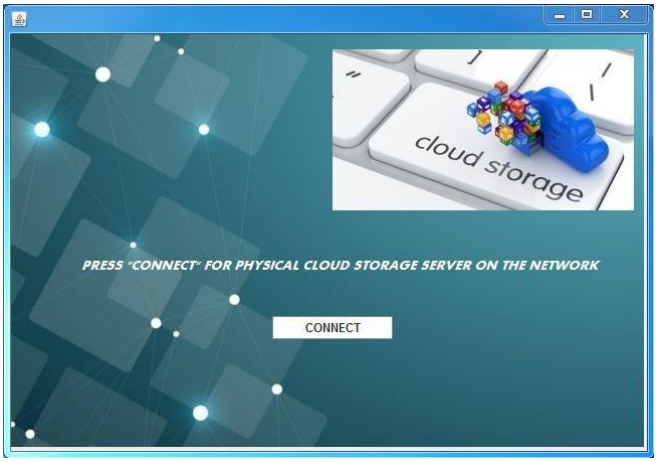

Figure1: Cloud connection

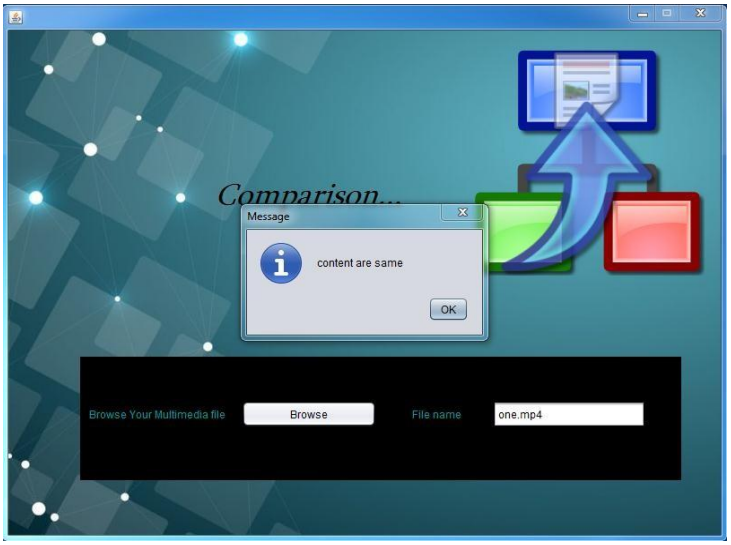

Figure 2: Content matching

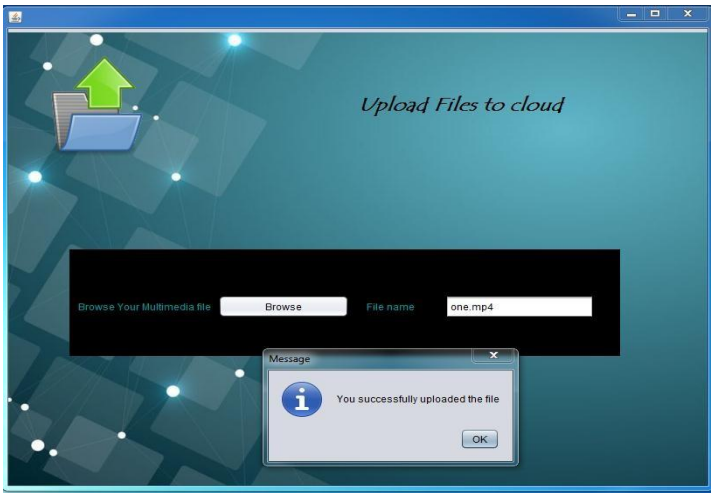

Figure 2: Successfully upload content

IV. 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 clouds. Two key components of the proposed system are presented. There is a new method for creating signatures of 3-D videos. Our method is that create binary packets for the images or videos in the site. 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 system 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. Here also a key generation is implemented and is generates as SMS which is required for downloading the content from cloud. This adds extra security to the content.

V. REFERENCES

[1]. 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.

[2]. 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

[3]. 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.

[4]. 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.

[5]. S. Ioffe, "Full-length video fingerprinting. Google Inc.," U.S. Patent 8229219, Jul. 24, 2012.

[6]. A. Kahng, J. Lach, W. Mangione-Smith, S. Mantik, I. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Watermarking tech- niques for intellectual property protection," in *Proc. 35th Annu. De- sign Autom. Conf. (DAC'98)*, San Francisco, CA, USA, Jun. 1998, pp. 776–781.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.