ISSN 2278-3091
Volume 5, No.4, July – August 2016
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse10542016.pdf

An Efficient Method for Protecting Hypermedia & Reducing Computation Cost Using Cloud Resources

Momin Farha[1], Dr. M Sreedevi[2]
[1]Madanapalle Institute of Technology & Science, India, mominfarha04@gmail.com
[2]Madanapalle Institute of Technology & Science, India, sreedevim@mits.ac.in

ABSTRACT

Now-a-days rich hypermedia content is uploaded to different sites but patent resources such as record, song and similes are hosted in sites which fatalities the proceeds of at ease creators for this problem. We recommend new design to protect hypermedia content by utilizing cloud resources which minimizes outlay, scalability and stretch. The new system is a collection of public cloud and private cloud. The designed new system contains two important components one is efficient method to create signatures of 3D-videos which captures the intensity sign of 3D videos lacking of computing the exact deepness map, which is computationally it is an exclusive process. The second is distributed Matching Engine which is used to make out duplicate hypermedia object, between the creative one and the alleged one.

To overcome this problem, we have designed an Index R++ tree. In this the object of signatures will be maintained and it offers best efficiency signatures are to be protected, finally this new method shows efficiency in terms of identification duplicate hypermedia objects reduces communication and totaling cost.

Key words: Hypermedia, 3-D video, distributed matching engine, Cloud applications, Digital signatures, Index R++ tree.

1. INTRODUCTION

As we know that due to the advances in giving out and footage tools of hypermedia as well as the accessibility of at no cost online hosting have made relatively to easy the photocopy the copies. The copies such as videos music images audio clips. As illegally redistributing the hypermedia content over the internet will cause the loss of revenues for content creators. If we want to find the illegal copies over the internet it will be a complex and computationally costly process because of the qualification or absolute amount of the accessible at ease in the hypermedia over the internet and it will be complex to identify and comparing the copies. The structure can run on private clouds or public clouds or any grouping of public-private clouds. This intend achieves quick deployment of at ease shield structure because it is based on cloud infrastructure that can rapidly provide hardware and software assets.

The difficulty of protecting different types of hypermedia contented has involved considerable attention from academic world and commerce. one method of this problem is using watermarking in order to find and verify the authenticity of the content in which some distinctive information is embedded in the content itself. Watermarking require inserting watermarks in hypermedia objects ahead of releasing them as well as the structure to find the objects and authenticate the correct watermarks in them. This approach is not suitable for already released content without watermarks in them, the watermarking is more appropriate for the illegal environment such as sharing of hypermedia content on DVDS or using extraordinary site and custom players. For rapidly increasing online videos watermarking approach is not applicable especially the categories of videos like YouTube and played back any videotape performer.

The structure is quite composite with several works which includes crawler is second-hand to download many objects from online hosting sites. Signature technique is used to produce representative fingerprint from hypermedia objects. To store the signature of original objects distributed matching engine is used to match them against query suspected objects. In this structure for the crawler we are using the off-shell-tools. In this component we have tested more than thousands of component and up to 1 million images in a running system. In this system we deployed two models one is Amazon cloud with varying number of machines and another one is private cloud which is used for the other parts of the system. To show the flexibility of the structure and it utilize with varying amount of computing resources such as minimizes the cost and it offers different pricing models for computing and network resources so for all the purposes we are using the deployment models.

The main focus of this paper is for protecting hypermedia content which is content based copy detection. In this signatures are extracted from the original objects signatures and which are downloaded from query suspected objects from online sites. Then similarity is taken form query objects and suspected objects to find the potential copies. These methods can be classified in to four categories such as spatial, temporal, color and transform domain. Spatial signature is

mostly used for the block based. Though there is a not have of flexibility aligned with large geometric transformations. Temporal and color signatures are a smaller amount forceful and it will be used to enhance the spatial signatures transform domain are mostly thorough computationally and it will be not widely used in perform.

A content protection has three main parties content owners hosting sites and service provider .The first party is protecting the hypermedia from the copyright objects example is Disney the second party is used to find the whether the object is posted on any hosting site example is you tube and the third party is offers finding the content owners by checking the hosting sites example is audible magic and in less cases the content owners operate their own protection system. The main following goals in protecting content of hypermedia are expenditure competence.

1.1 System Design

The entire multi cloud structure for hypermedia is content protection. The structure supports unusual types of multimedia content and can efficiently use varying computing assets. Methods that are used in this paper are as follows:

1.2 Signature Creation

This technique generates signatures that capture the intensity in personal stereo deficient compute the intensity sign itself, which is computationally a costly method. This structure is intended to hold different types of hypermedia objects. In multidimensional signatures the abstracts the information of unusual types of media objects. The signatures formation and comparison module is media specific, while further parts of the structure do not depend on the media type. Our aim supports creating complex signatures that consists individual or more of the subsequent elements:

Illustration signature: It is created based on the visual parts in hypermedia objects and how they modify with the time.
Auditory signature: It will be created based on the audio signals in hypermedia objects.
Intensity signature: If objects of hypermedia are 3D videos then signatures are created from depth signals.
Meta data: It will be created from the information associated with hypermedia objects such as their names, tags, and IP addresses of their up loaders or from the downloader's.

Our method computes a signature of the depth signal exclusive
of computing the depth signal itself.

1.3 Distributed Matching Engine

We intend a matching engine which is appropriate for different types of hypermedia objects that is scalable and stretchy. We need scalability in hypermedia feature that allow our structure to exploit varying amount of computing assets accessible on cloud infrastructures. A Stretchy is used to allow utilizing unreliable amount of cloud resources.

Our method matching engine is general and it can hold different types of hypermedia objects such as 2D videos and 3D videos. To achieve this, we split the engine in to two main points. The first point computes the nearest neighbor for a given data point and next point post processed the computed neighbor based on the object type. Our aim supports high dimensionality which is desirable for hypermedia objects that are rich in features. They resolve large datasets by Map Reduce.

Map reducing provides a communications that will be run on a group of machinery which will mechanically manage the executions of much computation in similar the infrastructure amongst this computation. This distributed intend allow leveling the large amount of data and using variable total of computational resources.

It will maintain the signatures of the object by using the Index R++ tree; they avoid overlapping of interior nodes by inserting an object in too many leaves if necessary as we can say that this technique shows efficiency in terms of identification of duplicate hypermedia objects which reduces communication and computation cost and it will take less time to match the signatures.

2. DESIGN AND PROCESS

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary

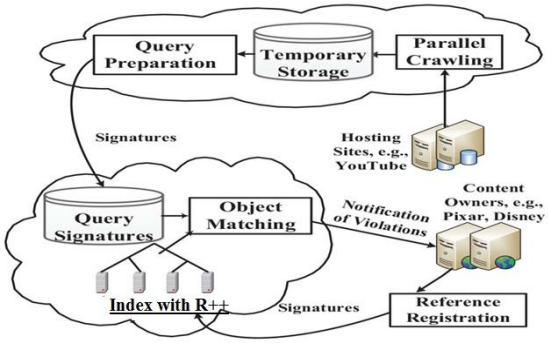

Figure 1: System Architecture

The cloud based hypermedia content protection is shown in fig: The structure has multiple components and it will be mostly hosted on cloud infrastructure. We can use one or more cloud systems because some cloud providers are more efficient and provide cost saving for different computation and communication tasks. In this system we are using two cloud systems. The top cloud in the figure it shows that it is used for downloading and storing temporary videos from

online sites. The lower cloud offers better compute nodes it will be used to maintain the distributed index and it can perform the copy detection process at lower costs.

The system can be deployed and managed by three main parties: content owners hosting sites or service providers. It will have the following components and it will be shown in fig:
R++ tree: Maintains signature of objects by using a dynamic index R++ tree. It offers the enhanced signatures to be confined with top competence.

They keep away from overlapping of inner nodes by inserting an object in too many leaves if essential.

Reference Registration: The content owners which are interested in protecting the objects it creates signatures for the objects and it will be inserted in to the R++ tree.
Query Preparation: The objects which are downloaded from online sites. It will create signatures which are known as query signatures and these signatures are uploaded to a common storage.
Object Matching: To find the potential copies it will compare the uncertainty signatures in opposition to the allusion signatures in the R++ tree. If any of the duplicate copies are found, then it will send notifications to the content owners.
Parallel Crawling: Download hypermedia stuff from different online hosting sites.
Temporary Storage: This will be used to store the temporary objects which are downloaded from online sites.

The Distributed index and object matching components which is known as the Matching engine.

We designed and implemented a parallel crawler and it will be used to download videos from you tube. The structure is as follows:

The hypermedia objects which are interested in protecting it will be specified in content owners then hypermedia creates signature for this objects which is known as reference objects and it will be registered in to index R++ tree. We can that it is a onetime process or the continuous process and periodically the new objects will be added. Uncertainty downloads the recent object from online hosting. We can filter various types of objects to reduce the number of downloaded objects.

Once the crawler component finishes its downloading we can create signatures for this query objects and the object itself is removed. To perform the comparison, the crawler component downloads all objects and signatures and it will be uploaded to matching engine. A distributed operation is performed when all the signatures are uploaded to matching engine and then in distributed index it will compare the query signatures versus the reference signatures. As shown in the above figure 1.

3. ALGORITHM

Input: objects, signatures
Output: Download objects
Step 1: Create distributed index with R++ tree.
Step 2: Signature creation for objects that is interested to R++ tree. Signatures are created in the form of Digital way by using the two algorithms Secure Hashing Algorithm (SHA-1) and Advanced Encryption Standard (AES) where as SHA-1 gives 160 bits and AES 128 bits.
Step 3: Uploading the signatures to a common storage.
Step 4: Sending notifications to owner if found matched the copy object.
Step 5: Downloading objects from online hosting sites.

From this system Architecture we are creating distributed index with R++ tree. In other words, we can say that we are replacing distributed index with R++ tree. Due to its better efficiency and good performance.

The objects which are interested in creating the signatures for that the content owner will create the signatures and it will be stored in R++ tree.

Following creating the signatures this will be used to store the temporary objects which are downloaded from online sites. We designed and implemented a parallel crawler and it will be used to download from online sites.

After uploading the object if we want to download the object in meanwhile if an attacker has attack the object by changing the details and other it sends notifications to content owner to verify the potential copies it will compare the uncertainty signatures opposed to the allusion signatures in R++ tree. If none of duplicate copies are found, then it won't send notifications to the content owners.

Finally, it will download the object from online hosting sites which is requested.

4. WORK FLOW

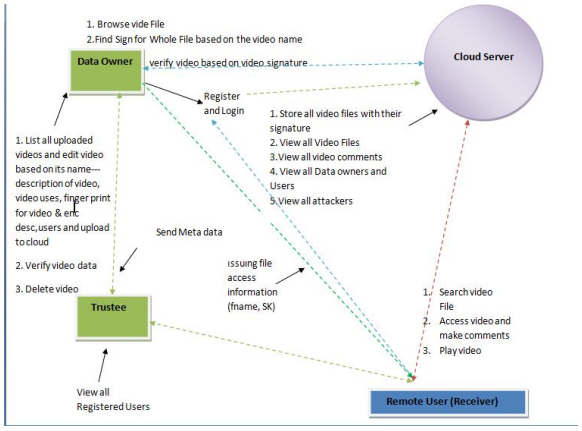

Figure 2: Flow Process

In this mainly four categories are there: As shown in figure 2.

Data Owner: An individual unit or reject to way in certain data & its responsible for its exactness, reliability and correctness.

Trustee: Trustees is an individual or firm those holds or administer assets or resources for the benefit of a third party. It will be appointed to many of the purposes for maintain the authenticities. Location

Remote User: When an identity is working on a central processing unit that is access from another location. These links are through in excess of the internet or by means of personal network with several form of inaccessible access.

Cloud Server: A cloud attendant is a consistent server that is build, hosted & delivered during a cloud computing stage in excess of internet.

The flow in a way that the data owner will upload the vide file. If he is accessible otherwise there is a registration form which consists of some details. After uploading the file then, the owner can verify and edit the details and a Digital signature is created and a secret key, then all these objects are uploaded to the cloud. If an attacker has attacked the objects and details by modifying some variations, then automatically it will send notifications to the owner. Then owner can verify it.

5. RESULT ANALYSIS

Figure 3: Analysis of result

Graph 1: Analysis of result

In the above graph figure 3The graph shows that we have taken two points that is Distributed Index (DI) and Index R++ tree (IR++ tree) X and Y axes. In the X axis signatures and Y axis the Accuracy for that the object is uploaded from the previous method it shows the highest accuracy (blue color) as shown above.

6. CONCLUSION AND FUTURE WORK

Distributing the copyrighted objects in hypermedia which will loss in terms of content creator structure needed to find all these which will be a large and compound method. By using multi-cloud infrastructure, we presented a novel method to protect this hypermedia by using the private and public cloud which will minimizes the cost, elasticity and scalability. The first method creates signatures of 3D videos this captures the depth signal of 3D videos without computing the depth signal itself, which is computationally it is an expensive process. The second method which is distributed matching engine used to match the hypermedia objects which is characterized with high dimensionality this distributed index which is implemented by using the map reduce framework and with the help of R++ tree we can protect the hypermedia content with better efficiency and good performance.

In hypermedia we are finding the potential copies. We match the object between the innovative one and the assumed one. If the matching objects is found then we can say that it is a legal object if the matching objects is not found, then attacker has attack the object with some modifications and we can say that it is an illegal object. Furthermore, to improves the signatures of objects by using an index R++ tree. It offers best efficiency and signatures are to be protected because they avoid overlapping of internal nodes by inserting an object in to multiple leaves if necessary and query performances are good.

This paper can be extended for design signatures for current and composite formats of 3D videos such as multi-view plus depth. A multi-view plus depth has compound texture and depth component which allows an abuser to view a view from different angles. Signatures of such type of should need to be capture the complexity and efficient to store compute and compare.

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 MapReduce;** 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] G. Kart hick, Mrs. M. Sreedevi (2013). **Scalable and Secure Decentralized information sharing in the cloud;** International Journal of Advance Research in Computer science and software Engineering, 3,490-99.

[7] 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.

[8] Mohamed Hefeeda, **Cloud-Based Multimedia Content Protection System**; IEEE transactions on multimedia, vol. 17, no. 3, march 2015.

[9] 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.

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

[11] W. Lu, Y. Shen, S. Chen, and B. Ooi, **Efficient processing of knearest neighbor joins using MapReduce;** in Proc. VLDB Endowment(PVLDB), Jun. 2012, vol. 5, no. 10, pp. 1016–1027.

[12] M.Sreedevi, L.Manjula(2013).**Automated Cloud based file storage nodes balancer**; .International journal of Advance Research in computer science and software Engineering, 3, 490-493.

[13] 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, May 2008, pp. 81–84.

[14] A. Stupar, S. Michel, and R. Schenkel, **Rankreduce – processing k-nearest neighbor queries on top of mapreduce;** in Proc. Workshop Large-Scale Distrib. Syst. Inf. Retrieval (LSDS-IR'10), Geneva, Switzerland, Jul. 2010, pp. 13–18.

[15] K. Tasdemir and A. Cetin, **Motion vector based features for content based video copy detection;** in Proc. Int. Conf. Pattern Recog. (ICPR'10), Istanbul, Turkey, Aug. 2010, pp. 3134–3137.

[16] Siva Kumar, A, Tech,M,Sreedevi,Mrs M&Tech, M (2013) **Deployment of on-demand services in cloud based on performance of Servers;** International Journal of Computer science and Engineering, 2, 229-236.

[17] N. Khodabakhshi and M. Hefeeda, **Spider: A system for finding 3Dvideo copies;** in ACM Trans. Multimedia Comput., Commun., Appl.(TOMM), Feb. 2013, vol. 9, no. 1, pp. 7:1–7:20.

[18] E. Metois, M. Shull, and J. Wolosewicz, **Detecting online abuse in images. Mark monitor Inc.;** U.S. Patent 7925044, Apr. 12, 2011

s