A FRAMEWORK FOR PROTECTING MULTIMEDIA CONTENT OVER PUBLIC CLOUD FROM PIRATING

T.S.Srinivas[1], Dr V.B.Narasimha[2], Dr. M.E.Puroshothamman[3]
[1]Associate Professor, CSE, MarriLaxman Reddy Institute of Tech &Management, Telangana, Hyderabad.
[2]Associate Professor, 3Professor, Dept of CSE Osmania University, Telangana, Hyderabad.
[3]Dean Department of CSE TKR college of Engg Hyderabad

Abstract
Cloud computing is emerging field because of its performance, high availability, least cost and many others. In cloud computing, the data will be stored in storage provided by service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing. we proposed a new design for multimedia content protection system. The system can be used to protect various multimedia content types like text, audio, videos, 2D videos and 3D videos. Due to high availability of free online sites, it has made it easy to duplicate copyright and illegally redistributing content over internet. Finally it caused losses for content creators. This is the challenging problem to be addressed. Of late Hafeeda et al. proposed a cloud based system for protecting multimedia content. They proposed a method for signature creation and another method for distributed matching in order to achieve this. However, their system is not evaluated for 3D videos with multiview plus depth. In this paper we focused on the Copy right protection of Videos using online Signature scheme. The composite signature scheme that combines multiple modalities may be needed to quickly identify short video segments. The proposed system also focuses to design signature for recent and complex formats of 3-D videos such as multiview plus depth that allow users to view a scene from different angles. Our empirical results revealed that our system is effective in protecting multimedia content.

Index Terms – Cloud computing, signature generation, distributed matching, multi-view plus depth videos

INTRODUCTION

Recent advancements in technologies paved way for multimedia content delivery and its related applications. At the same time cloud computing has emerged as an important pool of resources to be shared to users across the globe. As the cloud provides scalable and available services for storage with huge amount of computing resources, organizations that generate and maintain multimedia content started depending on cloud storage services. In this context there is growing interest in storing and protecting multimedia content in cloud. Many researches came into existence to contribute towards it. The techniques covered protection of multimedia content including audio, 2D video, 3D video and others. The solutions are pertaining to both hardware and software.

The existing techniques were able to protect the video content using signature mating. However, they were not able to generate accurate signature for multi-view plus depth videos. In this paper we addressed this problem by proposing a novel architecture for protecting multimedia content including 3D videos with multi-view plus depth features. Our contributions in this paper include the design and implementation of an algorithm that can protect 3D and other videos. It also generates signatures for 3D videos with multi view plus depth. Thus the proposed system provides a comprehensive approach in protecting multi-media content in cloud computing environment. The remainder of the paper is structured as

follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents experimental results while section V concludes the paper.

RELATED WORKS

This section reviews literature on multimedia content protection. Bianchi and Piva [1] explored digital watermarking for multimedia content protection. Apart from watermarking they also studied other schemes such as asymmetric fingerprinting protocols, zero-knowledge protocols, commitment schemes, and homomorphic encryption. Saraswathi and Venkatesulu [2] proposed a block cipher algorithm which is based on binary trees and random substitution for protecting multimedia content. Greveler et al. [4] studied the content identification mechanisms using power usage profiles of smart meters. Zhou et al. [5] employed one dimensional chaotic maps for encryption of images. This approach was able to withstand various attacks besides handling data loss. Zhou et al. [6] proposed architecture for multimedia security in presence of Internet of Things (IoT). Their architecture is generic and guides to have security for multimedia content.

Akhtar et al. [7] explored steganography for multimedia content protection. They used RC4 algorithm to enhance the security and quality of communications. Hermassi et al. [8] studied chaotic permutation and image encryption for secure content distribution. In [9] there is fingerprinting applied for full length videos. It was the approach which got US patent. Wei et al. [10] proposed an auditing tool for storage in cloud computing. The tool was named as SecCloud. It provides signature based storage and content verification. Khodabakshi et al. [11] proposed a copy detection system which is content based and works for 3D videos. It has mechanism to find video copies and the tool is named as Spider. Hafeeda et al. [12] proposed a cloud based mechanism for multimedia content protection. They used signature generation and signature matching approaches. Our work is closer to this work but unlike the work of [12], it supports multi-view plus dept video files as well.

Boutada et al. [13] studied interactive multimedia computing and observed recent trends. They found various issues with multimedia content. They are interactive computing for convergence, content protection, multimedia processing, processing digital signals, multimedia communications over networks, digital management, interactive multimedia and appliances, intelligent extraction of information, indexing, visualization, and databases. Lu et al. [14] studied k-Nearest joins for retrieval of data from large databases using MapReduce programming paradigm. Patsakis et al. [15] studied the need for privacy and security in Online Social Networks (OSNs). They provided insights in the form of issues in OSNs and countermeasures. Zhang et al. [16] focused on digital rights management for multimedia content. They built a prototype for the same. Jean-Henry et al. [20] focused on digital rights management and provided insights on the issues of the subject. Niharika and Sahoo [18] proposed a cloud based system for protecting 3D videos. Our work is close to this as well but this work does not support 3D videos with multi-view plus depth. Ye et al. [17] focused on the secure distribution of multimedia content in the context of Machine to Machine (M2M) systems. Fund et al. [19] studied the issues related to copyrighted multimedia content. They summarized the issues, legal limitations in protecting multimedia content.

Aly et al. [3] studied distributed Kd-Trees for efficient retrieval of multimedia content from large databases. They implemented it in distributed programming environment using MapReduce model. They found their method to take very less time to retrieve images. Esmaeili et al. [22] studied content based fingerprinting for video copy detection. They proposed fast matching approach for the verification of copy videos with reference fingerprint videos. Dalakleidi et al. [24] proposed a method for formally representing multimedia content using ontology. This could improve efficiency in content management. Wang et al. [25] proposed a model known as view synthesis distortion model for multiview depth video coding. It was used to have optimized frame level rate. Similar kind of work was done by Zhang et al. [26] for having video quality assessment. Ekmekcioglu et al. [27] proposed an adaptive approach for delivering multiview videos with respect to Digital Video Broadcast (DVB) for robustness.

Su et al. [28] proposed a mechanism for graph-based representation of images with multi-view.

Thus rate distortion was optimized. Aflaki et al. [29] studied Multi-view plus dept videos for subjecting them to advanced video coding standard. Zilly et al. [30] employed mixed narrow and wide baseline for generating multi-view plus dept videos. The literature review in this section found that multimedia content protection systems were available for 3D videos. However, there is little research in protection of multi-view plus dept 3D videos. In this paper we proposed a cloud based system for protecting such videos from unauthorized distribution over Internet.

M-Protect: THE PROPOSED SYSTEM

The aim of the proposed system is to extend the signature scheme in order to protect 3-D videos with multi view plus dept. The existing solution does not support signature for such videos. This is achieved by using multiple descriptors to represent the video in different angles. Both colour and depth of the data of video are considered while making descriptors. The intermediate views are used in order integrate with final view so as to improve the accuracy of signature. The quality of the signature and the detection accuracy is thus increased in the proposed system. Both temporal and inter-view references are considered at the same to in order to have complete representation of the video in terms of a signature. The procedure to create this kind of signature is as follows.

- Take 3-D video with multi view plus depth as input.
- Find the features of the video and create descriptors using image processing.
- Find out all the intermediate views and create descriptors.
- Use temporal and inter-view references to construct descriptors.
- Use all the descriptors that fully represent video and generate signature.

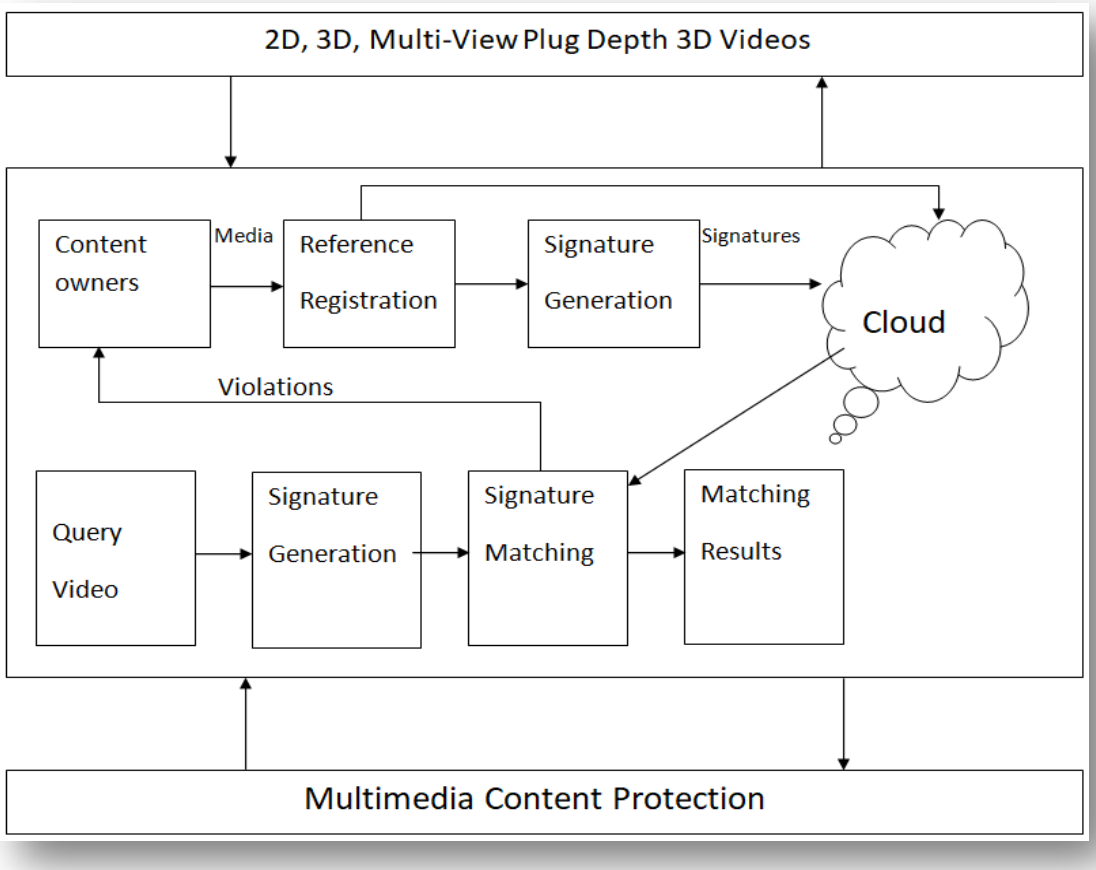

Figure 1: Overview of the proposed system M-Protect

As shown in Figure 1, there are operations like registration, signature generation, and signature matching and protecting multimedia content. For a genuine user the system allows registration of videos as the video signature is new. The matching operation can detect the video is either genuine or pirated by comparing with already existing signatures. The system also supports multi-view depth videos. In order to achieve this, we proposed an algorithm

named Multi-View Depth Signature Algorithm (MDSA). The algorithm can take multi-view depth videos as input and produce signatures representing multi-view depth video in order to protect intellectual property in cloud. In fact the proposed algorithm makes use of multiple descriptors of video in order to represent multi-view depth.

Algorithm: Multi-View Depth Signature Algorithm
Input: Multi-view depth video ***MVDV***
Output: Signature representing multi-view depth video and protection
to intellectual property in cloud

Initialization
01 Initialize video database ***VDB***
02 Initialize video ***v***
03 Initialize signature vector ***S***
04 Initialize media type ***mt*** to video
05 Initialize multi-view descriptor vector ***MVD***
06 Initialize a view vector ***view***
07 Initialize ***found*** to Boolean
08 Input multi-view depth video ***MVDV***
Signature Generation
09 IF media == ***mt*** THEN
10 For each ***view*** in ***MVDV***
11 Extract data
12 Add data to ***MVD***
13 End For
14 END IF
15 Generate signature ***s'*** for ***MVDV*** from ***MVD***
Signature Matching
16 Populate ***VDB***
17 Populate ***S*** from ***VDB***
18 For each ***s*** in ***S***
19 IF ***s'*** == ***s*** THEN
20 ***found*** = true
21 END IF
22 End For
Applying Protection
23 IF ***found*** = true THEN
24 Treat ***MVDV*** as pirated
25 Protect the cloud by not allowing such video
26 ELSE
27 Allow ***MVDV*** into the cloud
28 End IF

The algorithm has five phases. They are known as Initialization, Signature Generation, Signature Matching and Applying Protection. The initialization section initializes different variables needed to complete the procedure. In the signature generation phase the system takes multi-view depth video and generate signature which reflects multiple descriptors pertaining to multi-view plus depth video. Afterwards, signature matching takes place in order to know whether the signature is matching. Once matching is completed, it may result in either true or false. If the matching is resulted in true then the multi-view depth video is considered to be pirated copy. In this case the system alerts the user to prevent such video for uploading into cloud. If not the video is allowed to be outsourced to cloud storage. The proposed system provides the advantages as given here. Even 3d videos are also protected from redistribution. Content protection system becomes more robust and accurate in

identifying and reporting redistribution. Content providers gain more in terms of revenues and customer loyalty.

Signature Generation

Signature is generated by the proposed system for different multimedia objects. When a media object is given, the system takes it and abstracts it to have its details. The signature generation process involves many steps. The signature creation process is based on the media. When a multi view plus depth 3D video is given as input, the system needs to create multiple descriptors and have a composite signature to reflect all. Each descriptor captures particular aspects of the video. A visual part of the video and its temporal dynamics are captured into a visual descriptor. Based on the audio signals present in the audio a descriptor is created to represent the audio. A multi-view plus depth descriptor is created specifically to represent the multi-view plus depth of the video. There is another descriptor created for maintaining metadata of the object. It holds data about data such as video name, its format, its size, its origin etc. Creating visual signatures for 2D videos was found in [32]. With respect to creating audio signatures, a method is found in [31]. Creating them is supported by the proposed system. Besides it focused more on the 3D videos with multi-view plus depth.

The proposed system takes 3D video with multi-view depth as input and considers two views in it before generating descriptors and final signature which is a composite of all descriptors. The two views are known a left view and right view. The left view is related to left eye while the right view is related to right eye. Each view is a collection of frames that reflect stream of frames with respect to the frames of other view. Different steps are involved in the process of generating signature. In the first step descriptors are created for both left and right views. SURF (Speeded-Up Robust Feature) is used in this paper for creating descriptors. SURF has 64 dimensions or features to represent media object. Eq. (1) and Eq. (2) are basis for signature generation. They help in capturing left view and right view of media object.

$D_i^L = (f_{i1}, f_{i2} \ldots\ldots\ldots f_{iF})$, i=1,2,3 $\ldots\ldots L_n$ (1)

$D_i^R = (f_{j1}, f_{j2} \ldots\ldots\ldots f_{iF})$, j=1,2,3.... R_n (2)

Number of descriptors in left and right images are denoted as L_n and R_n. Number of dimensions is denoted by F. In step 2 each images pertaining to video in both left and right views are divided into equal number of blocks. In the third step, the visual descriptors of left and right views are to be matched for efficiency. Matching of visual descriptors is done as in Eq. (3) with descriptors for multi-view plus depth videos.

D_i^L-D_i^R=$\sqrt{(f_{i1} - f_{j1})^2 + \cdots \ldots\ldots + (f_{iF} - f_{jF})^2}$ (3)

The distance between visual descriptors of left and right views is computed and the descriptor that exhibits minimum distance is finally matched. For effective signature generation, in the fourth step, block disparity is considered. It is computed between left and right descriptors pertaining to views. For any single descriptor present in views block disparity is computed as in Eq. (4).

$\sqrt{(x_i - y_j/W_b)^2 + \cdots \ldots\ldots + (y_i - y_j/H_b)^2}$ (4)

The position of given descriptor *i* is represented as (x_i, x_i) for left image and (x_j, x_j) for right image. The width Wb and height Hb parameters are used to normalize the computed disparity. In the final step, actual signature is generated that contains all descriptors used to reflect multi-view plus depth video.

Signature Matching

We proposed a mechanism for signature matching as part of detecting copy videos. The data structure used to implement matching is known as directed tree as explored in [33]. It is a space partitioning tree which groups similar things. The data structure has two things namely directed tree and bins. Bins are actually used to store data in the form of files. And bins are leaf nodes in the tree. The intermediate nodes do not store actual data needed for matching. Instead, they store metadata based on the data stored in the bins. Thus the intermediate nodes can help in processing queries faster. The signature matching mechanism has two important steps. They are known as building index and matching media objects. Indexing is created from reference data points provided to the system while the matching is made against query points by matching them with reference objects whose data is there in the bins of the data structure.

Storing data only in leaf nodes is the strategy that helps in reducing space complexity. By

keeping this tree in many nodes in distributed environment, it is possible to have parallel processing and get rid of single point of failure problem. The directed tree is binary tree. Once the tree is constructed with index and actual data points in bins, the matching is done in 3 steps. A query dataset is partitioned in the first step. In the second step, k-nearest neighbours are found for each data point present in the given query dataset. In the third step actual object matching is done in distributed environment. MapReduce programming with Hadoop which is a distributed programming framework is made for realizing the application in distributed environment.

We evaluated signature matching process in terms of accuracy of k-nearest neighbours retrieved. Towards this end, a metric known as Precision@Kp is used to compute accuracy. This metric is computed as shown in Eq. (5).

$$\text{Precision@}K_p = \frac{\sum_{i=1}^{K}\{T_i = K\}}{K} \quad (5)$$

The rank of a true neighbour is represented as T_i. T_i<=K is true if a true neighbour is found in K otherwise it results in false. Then the average precision of al neighbours is for given set of queries Q is computed as in Eq. (6).

$$\text{AvgPrecision@K} = \frac{\sum_{i=0}^{|Q|}\{precision\ \ @K(i)\}}{|Q|} \quad (6)$$

The metric is finally AvgPrecision@K which is used to evaluate our work. Our system is compared with RankReduce [34]. The experimental results without prototype application are presented in the ensuing section.

EXPERIMENTAL RESULTS

We built a prototype which is a web based application to demonstrate proof of the concept. The results of experiments are presented in this section. The results of the proposed system are compared with the results of YouTube's content protection system [9], Hafeeda et al. [12] system and RankReduce [34]. Different transformations are made as shown in Table 1 for experiments. The transformed multimedia objects are used to evaluate the performance of the proposed system. Datasets used for experiments YouTube videos and 3D videos with multi-view plus dept from [35].

	Accuracy in terms of Recall		
Transformation	**YouTube**	**Hafeeda et al. [12]**	**Proposed System**
Blur	0	1	1
File format change (mp4 to avi)	1	1	1
Re-encoding: same bit-rate	0	1	1
Re-encoding: different bit-rate	0	1	1
Re-encoding: different resolution	0	1	1
Frame dropping	0	1	1
30 seconds clip	0.166	1	1
35 seconds clip	0.333	1	1
40 seconds clip	0.666	1	1
45 seconds clip	0.8333	1	1
Anaglyph	0.833	0.833	0.833
Row-interleaved	0.833	1	1
Column-interleaved	1	1	1
2D-plus-depth	0	1	1
View synthesis	0	1	1

Table 1: Accuracy comparison in terms of Recall with other systems (3D videos)

The results reveal the accuracy of the proposed system and other systems such as YouTube's content protection system and Hafeeda et al. [12] content protection system. These results are related 3D videos. YouTube's content protection system is not able to detect copy video for transformations such as blur, re-encoding with same bit rate, re-encoding with different bit rate, re-encoding with different resolution, 2D plus depth and view synthesis. Hafeeda et al. [12] system and the proposed system showed similar performance with

respect to matching 3D videos. They show 100% accuracy for all transformations except anaglyph transformation for which they shows 0.833 accuracy. The accuracy value is considered between 0 and 1. The value 1 indicates 100% accuracy. A value in between such as 0.3 indicates 30% accuracy.

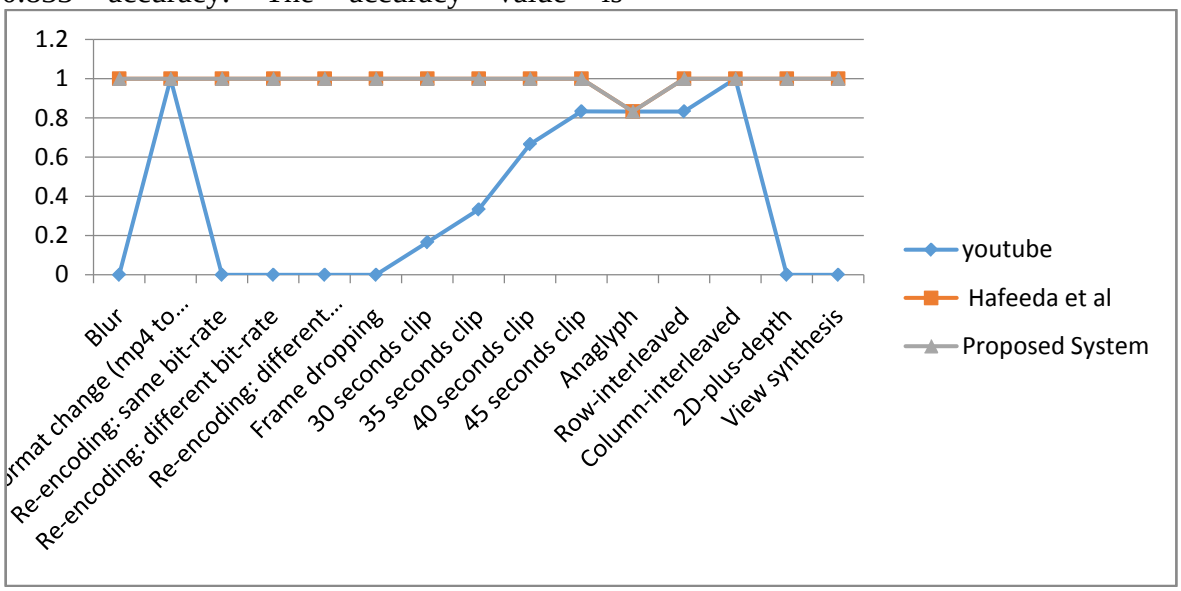

Figure 2: Accuracy comparison of the systems against different transformations (3D Videos)

Accuracy of the proposed system in comparison with other systems is visualized in Figure 2. The results reveal the performance of the three systems in protecting multimedia content. The copy videos with different transformations are subjected to detection process and the accuracy is presented. The results show that proposed system and the Hafeeda et al. [12] system exhibit similar kind of performance. These two outperform the system employed by YouTube in case of all transformations except two transformations such as Colum-interchanged and file format change.

Transformation	YouTube	Hafeeda et al. [12]	Proposed System
Blur	0	0	1
File format change (mp4 to avi)	0	0	1
Re-encoding: same bit-rate	0	0	1
Re-encoding: different bit-rate	0	0	1
Re-encoding: different resolution	0	0	1
Frame dropping	0	0	1
30 seconds clip	0	0	1
35 seconds clip	0	0	1
40 seconds clip	0	0	1
45 seconds clip	0	0	1
Anaglyph	0	0	0.833
Row-interleaved	0	0	1
Column-interleaved	0	0	1
2D-plus-depth	0	0	1
View synthesis	0	0	1

Table 2: Accuracy comparison in terms of Recall with other systems (3D videos with multiview plus depth)

As sown in Table 2, the accuracy comparison results in terms of recall for 3D videos with multi-view plus depth are presented. The statistics reveal clearly that both YouTube's content protection system and Hafeeda et al. [12] system are not able to handle 3D videos

with multi-view plus depth. Therefore their accuracy is little and proposed system is especially to deal with the 3D videos with multi-view plus depth. For all transformations, the proposed system shows 100% accuracy while 0.833 accuracy is recorded for anaglyph transformation

.

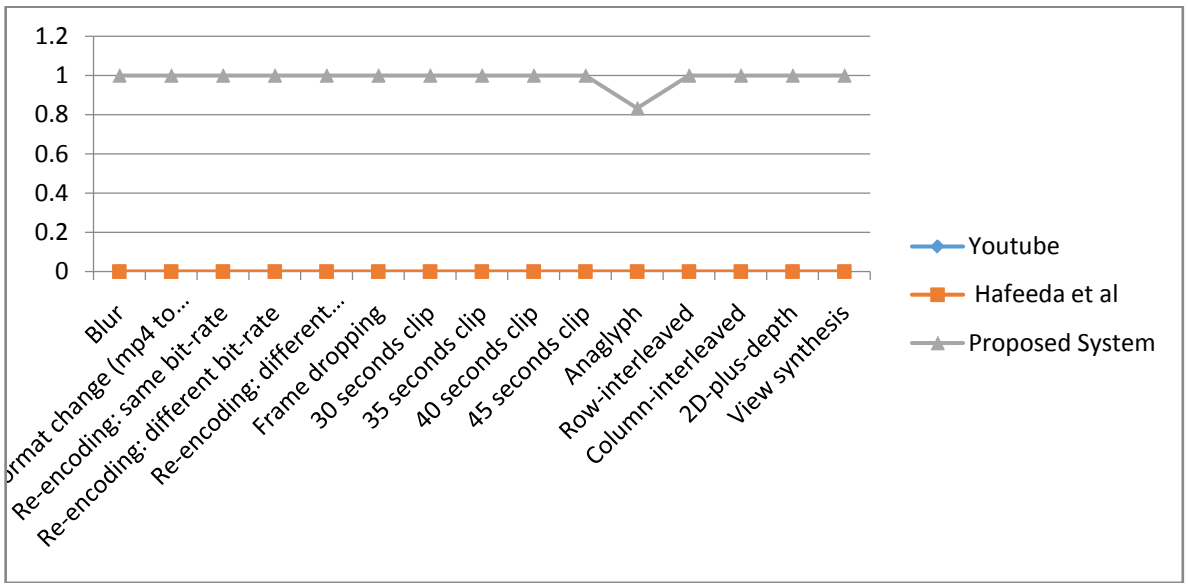

Figure 3: Accuracy comparison of the systems against different transformations (3D Videos with Multiview Plus Depth)

As presented in Figure 3, the accuracy of the proposed system reveals superior performance over other systems. The rationale behind this is that the proposed system is improved with image descriptors suitable to capture details of 3D videos with multi-view plus dept. The signature generation and signature matching operations are specially built to handle 3D videos with multi-view plus depth apart from other multimedia objects. The efficiency of the proposed system is thus higher than other systems where such videos are not supported for signature generation and matching.

Scanned % of Dataset	**Average Precision**		
	Rank Reduce	**Hafeeda et al. [12]**	**Proposed System**
5	0.45	0.5	0.6
10	0.7	0.88	0.9
15	0.8	0.92	0.94
20	0.87	0.96	0.98
25	0.9	1	1

Table 3: Performance comparison in terms of precision

Average precision computed when K value is 20 and results are presented in Table 3 for all algorithms. The results are captured at different percentage of scanned dataset. The results are recorded for percentages between 5 and 25 incremented by 5 each time. The proposed system shows high performance over other systems with all scanned percentage of dataset. The protection system of Hafeeda et al. [12] showed significant performance improvement over RankReduce [34]. The proposed system has comparable performance improvement over Hafeeda et al. [12] system besides outperforming RankReduce. The average precision at 5% scanned dataset is 0.45, 0.5 and 0.6 for RankReduce, Hafeeda et al. [12] and the proposed system respectively. The precision at 25% scanned dataset is recorded as 0.9, 1 and 1 respectively for the three systems.

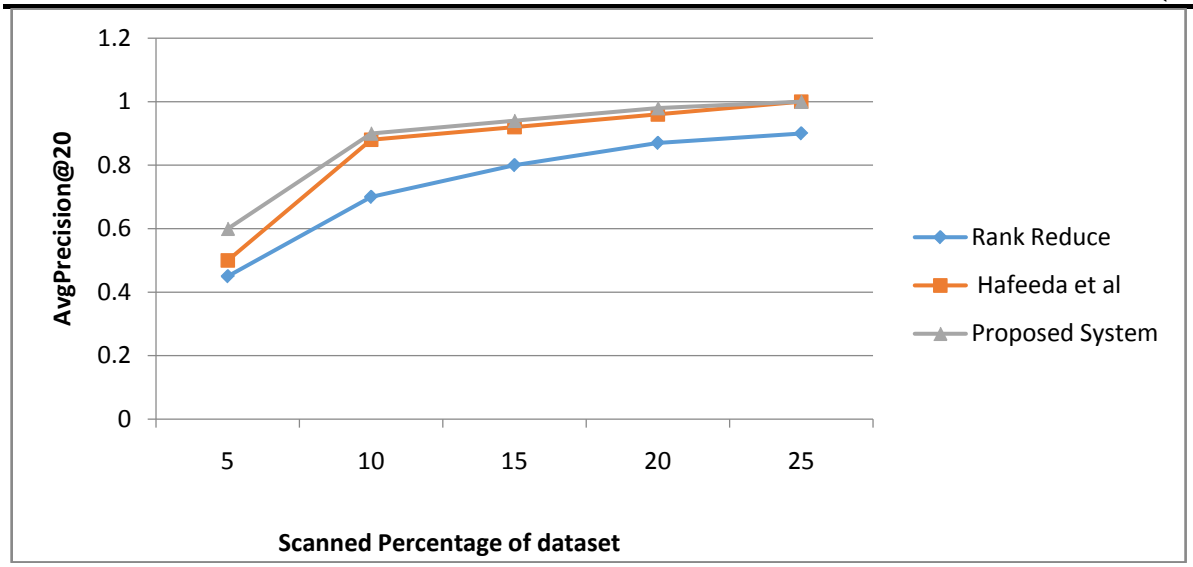

Figure 4: Precision comparison of multimedia content protection systems

The average precision at different percentage of scanned dataset is presented in Figure 4. The results reveal two significant trends in the functionality of the systems for content protection. As the percentage of scanned dataset is increased, there is increase in the average precision. As the precision depends on the % of scanned dataset, the influence is reflected clearly. Proposed system has increased average precision for all % of scanned dataset consistently. However, in case of 25%, the average precision of the proposed system and that of Hafeeda et al. [12] showed similar performance. However, proposed system and Hafeeda et al.'s system outperforms RankReduce. 128, 64, 32, 16, 8

Reference DB Size (millions)	**Running Time (minutes)**				
	128 Machines	**64 Machines**	**32 Machines**	**16 Machines**	**8 Machines**
25	13	13	13	25	30
50	28	55	88	80	60
75	75	123	200	150	160

Table 4: Performance with different number of machines

Reference database size and different number of machines used in the distributed environment can have their impact on the execution time of the proposed algorithm. The number of machines considered for experiments include 8, 16, 32, 64 and 128. The reference dataset size considered is 25, 50 and 75 millions. The execution time with reference dataset size 25 million for the proposed system is 13 minutes when 128, 64, and 32 machines are used. It is 25 and 30 minutes when 16 and 8 machines are used respectively. When the number of machines are more the execution time is reduced. When the reference dataset size is increased the execution time is also increased. With 75 million reference dataset size the execution time for 128 machines is 75 minutes while the same for 8 machines is 160 minutes.

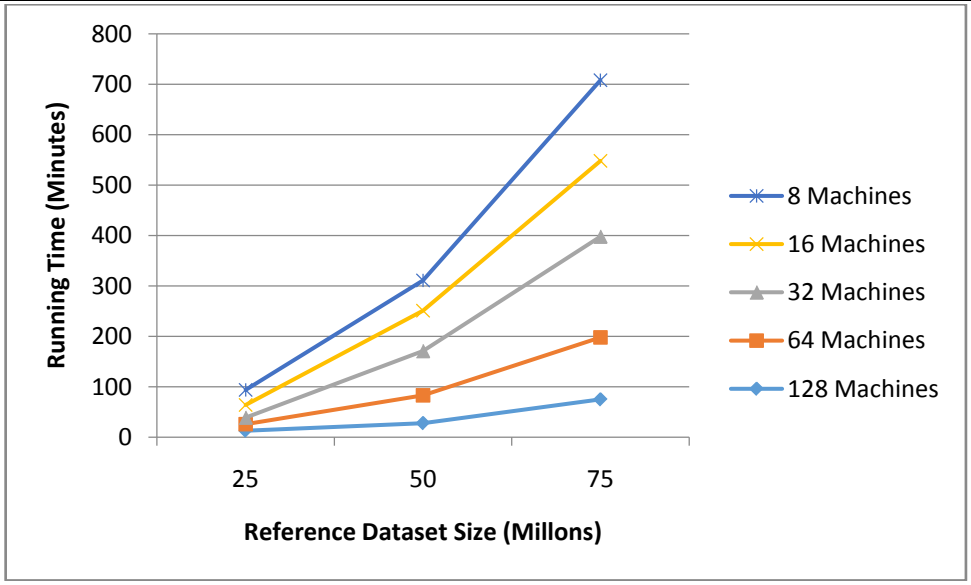

Figure 5: Performance Comparison with different machines

As shown in Figure 5, it is evident that the reference dataset size and number of machines used for experiments in distributed environment have their impact on the execution time. As the reference dataset size is increased, it needs more time to process the given set of queries. In the same fashion, when number of machines is less, it consumes more time to process the requests.

# of K-Nearest Neighbours	AvgPrecision
5	0.95
10	0.93
15	0.90
20	0.85
25	0.80

Table 5: K-nearest neighbours vs. average precision

Table 5 shows the results of experiments meant for finding the influence of K value on the performance of the system in terms of average precision. The results revealed that the K value has its impact on the average precision.

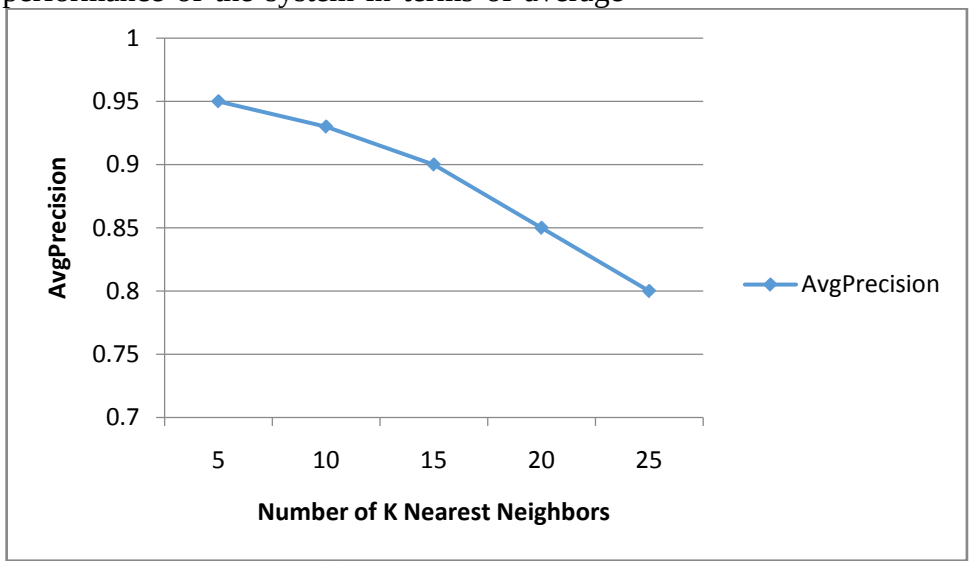

Figure 6: K-nearest neighbours vs. average precision

As presented in Figure 6, it is evident that precision is increased when k value is decreased. When the number of neighbours to be considered in the matching process of the proposed system is changed, it has its effect on the average precision.

# of K-Nearest Neighbours	Running Time (min)
5	10
10	10.1

15	10.1
20	10.1
25	10.2

Table 6: Number of K-nearest neighbours vs. running time

As shown in Table 6, when the number of k nearest neighbours is changed, the execution time is not significantly changed. There is little impact of K value in the experiments made to understand the execution time dynamics.

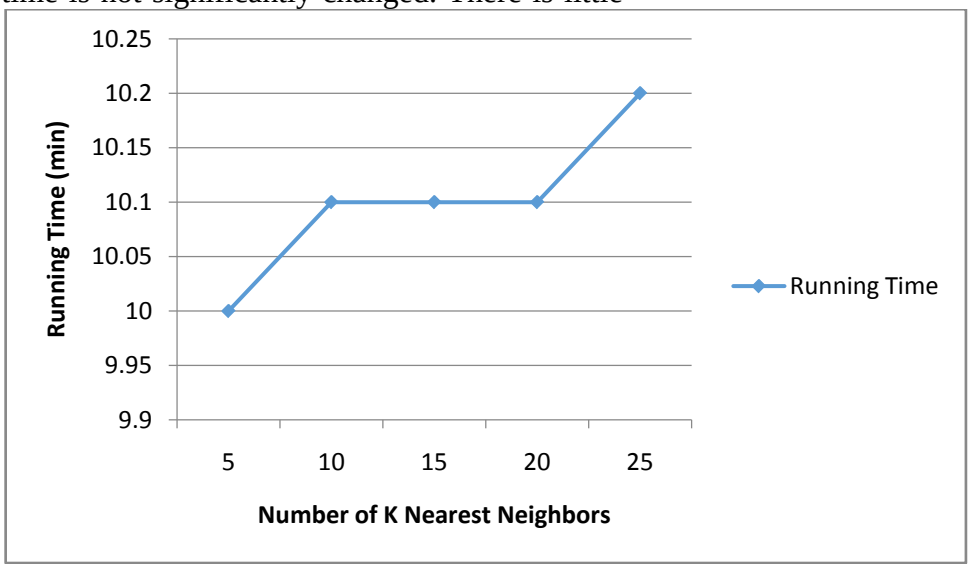

Figure 7: Number of K-nearest neighbours vs. running time

As presented in Figure 7, the results revealed that the execution time is almost same for all K values. There is slight difference in the execution time. Nevertheless, it is observed that K value has limited influence on the running time of the proposed system.

The proposed system M-Protect is able to protect multimedia content from unauthorized distribution over Internet by detecting copy videos. It not only works for 2D and 3D videos, but also for 3D videos with multi-view plus depth. The proposed system is compared with the content protection system used in YouTube and that of Hafeeda et al. [12]. Experiments are made in distributed environment with MapReduce programming paradigm. The input videos such as 3D videos and 3D videos with multi-view plus depth are subjected to different transformations in order to detect copy videos. The performance is evaluated with average precision as per Eq. (6), execution time in presence of different K values and different number of machines. Recall is also used to know the performance of the proposed system. Average precision with different scanned percentage of dataset revealed that the proposed system performed better than RankReduce and the system of Hafeeda et al. When K value influence on the average precision and execution time is evaluated, it is understood that proposed multimedia content protection system performed well. The influence of reference dataset size and the number of machines used for experiments is observed. With respect to k-nearest neighbours, K value has its influence on the average precisions and execution time. The experimental results revealed that the proposed system outperforms YouTube's content protection system and that of Hafeeda et al.

CONCLUSIONS AND FUTURE WORK

In this paper we proposed a framework for multimedia content protection in cloud computing environment. Due to innovative technologies and emergence of cloud computing multi-media content generation and maintenance became an improved phenomenon. At the same time there are many organizations that generate and maintain multimedia content. Content management and dissemination became easy with the advent of cloud computing in the real world. However, stealing content and reproducing or pirating became a challenging threat. Many techniques came into existence in order to protect intellectual properties of such organizations. However, they could not protect content in case of multi-view plus depth videos. To overcome this problem, in this paper, we proposed a framework and an algorithm named Muti-view Depth Signature Algorithm that can explore underlying descriptors of video to

generate signature. We built a prototype application to demonstrate the proof of concept. The empirical results revealed that the proposed system is working fine with multi-view plus depth videos as well. In future we intend to extend the research to consider live and streaming content for protection.

References

[1]. Tiziano Bianchi, Membe, Alessandro Piva and Senior Membe. (2013). Secure Watermarking for Multimedia Content Protection. *Politecnico di Torino*, p1-23.

[2]. P. Vidhya Saraswathi and M. Venkatesulu. (2012). A Block Cipher Algorithm for Multimedia Content Protection with Random Substitution using Binary Tree Traversal. *ISSN*, p1-6.

[3]. Mohamed Aly,Mario Munich and Pietro Perona. (2011). Distributed Kd-Trees for Retrieval from Very Large Image Collections. *ISSN*, p1-11.

[4]. Ulrich Greveler, Peter Glosekotterz, Benjamin Justusy and Dennis Loehr. (2011). Multimedia Content Identification Through Smart Meter Power Usage Profiles. *ACM*., p1-8.

[5]. Yicong Zhou, Long Bao and C. L. Philip Chen. (2014). A New 1D Chaotic System for Image Encryption. *Elsevier*., p1-21.

[6]. Liang Zhou, Nanjng University of Posts and Telecommunications Han-Chieh Chao, National Ilan University. (2011). Multimedia Traffic Security Architecture for the Internet of Things. *IEEE*., p1-6.

[7]. Nadeem Akhtar, Pragati Johri and Shahbaaz Khan. (2013). Enhancing the Security and Quality of LSB Based Image Steganography. *IEEE*, p1-12.

[8]. Houcemeddine Hermassi , Rhouma Rhouma and Safya Belghith. (2012). Security analysis of image cryptosystems only or partially based on a chaotic permutation. *IEEE*, p1-20.

[9]. S. Ioffe. FULL-LENGTH VIDEO FINGERPRINTING. (2012). United States Patent, p1-11.

[10]. Lifei Wei , Haojin Zhu a, Zhenfu Cao , Xiaolei Dong a, Weiwei Jia , Yunlu Chen and Athanasios V. Vasilakos. (2014). Security and privacy for storage and computation in cloud computing. *Elsevier*., p1-16.

[11]. NAGHMEH KHODABAKHSHI. (2013). Spider: A System for Finding 3D Video Copies. *DOI*, p1-20.

[12]. Mohamed Hefeeda , Senior Member, IEEE, Tarek ElGamal , Kiana Calagari, and Ahmed Abdelsadek. (2015). Cloud-Based Multimedia Content Protection System. *IEEE*. 17, p1-14.

[13]. Raouf Boutaba Kyung-Yong Chung andMitsuo Gen. (2014). Recent trends in interactive multimedia computing for industry. *IEEE*. . , p1-14

[14]. Wei Lu Yanyan Shen Su Chen Beng and Chin Ooi. (2012). Efficient Processing of k Nearest Neighbor Joins using MapReduce. *vldb*. 5, p1-12.

[15]. Constantinos Patsakis, Athanasios Zigomitros, Achilleas Papageorgiou and Agusti Solanas. (2014). Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures. *Security in Computer Systems and Networks*. , p1-19.

[16]. Zhiyong Zhang, Zhen Wang and Danmei Niu. (2014). A novel approach to rights sharing-enabling digital rights management for mobile multimedia. *DOI*, p1-17.

[17]. Conghuan , Zenggang Xiong, Yaoming Ding, Xuemin Zhang, Guangwei Wang and Fang Xu. (2016). Secure Multimedia Content Distribution for M2M Communication. *International Journal of Security and Its Applications*. 10, p1-10.

[18]. M.Niharika and Dr. Prasanta Kumar Sahoo. (2016). Protecting Cloud Based Multimedia Content Using 3-D Signatures. *IJACTA*. 4 , p1-4.

[19]. Fraida Fund, S. Amir Hosseini and Shivendra S. Panwar. (2016). Under a cloud of uncertainty: Legal questions affecting Internet storage and transmission of copyright-protected video content. *IEEE*., p1-14.

[20]. Jean-Henry Morin, Shiguo Lian2 , Xin Wang and David Llewellyn-Jones4. (2010). Guest Editorial. *MULTIMEDIA*. 5 (.), p1-144.

[21]. Constantinos Patsakis, Athanasios Zigomitros, Achilleas Papageorgiou and Agusti Solanas. (2014). Privacy and Security for Multimedia Content shared on OSNs: Issues and Countermeasures. *Security in Computer Systems and Networks*. , p1-18.

[22]. Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward (2011). A Robust and Fast Video Copy Detection System

Using Content-Based Fingerprinting. *IEEE*. 6, p1-14.

[23]. Zhiyong Zhang , Zhen Wang and Danmei Niu. (2014). A novel approach to rights sharing-enabling digital rights management for mobile multimedia. *MULTIMEDI*, p1-17.

[24]. Kalliopi Dalakleidi, Stamatia Dasiopoulou, Giorgos Stoilos, Vassilis Tzouvaras, Giorgos Stamou and Yiannis Kompatsiaris. (2011). Semantic Representation of Multimedia Content. *MULTIMEDIA*, p1-32.

[25]. XuWang SamKwonga,b,n, HuiYuan , YunZhang , ZhaoqingPan . (2015). Viewsynthesisdistortionmodelbasedframelevelrate control optimizationformultiviewdepthvideocoding. *Signal Processing*., p1-10.

[26]. Xiangkai Liu, Yun Zhang, Member, Sudeng Hu and Sam Kwong, Fellow. Jay Kuo, Fellow, IEEE, and Qiang Peng. (2015). Subjective and Objective Video Quality Assessment of 3D Synthesized Views With Texture/Depth Compression Distortion. *IEEE*. 24 , p1-16.

[27]. Erhan Ekmekcioglu, C. Goktug Gurler, Ahmet Kondoz, Senior Member, A. Murat Tekalp and Fellow, IEEE. (2016). Adaptive Multi-View Video Delivery using Hybrid Networking. *IEEE*., p1-14.

[28]. Xin Su Thomas Maugey and Christine Guillemot. (2015). Rate-Distortion Optimized Graph-Based Representation for Multiview Images with Complex Camera Congurations. *JOURNAL OF LATEX CLASS FILES*,. 14 , p1-14.

[29]. Miska M. Hannuksela, Member, Dmytro Rusanovskyy, Wenyi Su, Lulu Chen, Ri Li, Payman Aflaki, Deyan Lan, Michal Joachimiak, Houqiang Li, Member, and Moncef Gabbouj, Fellow, IEEE. (2013). Multiview-Video-Plus-Depth Coding Based on the Advanced Video Coding Standard. *IEEE*. 22 , p1-11.

[30]. Frederik Zilly, Christian Riechert1, Marcus Müller, Peter Eisert, Thomas Sikora and Peter Kauff. (2013). REAL-TIME GENERATION OF MULTI–VIEW VIDEO PLUS DEPTH CONTENT USING MIXED NARROW AND WIDE BASELINE. *IEEE*. , p1-24.

[31] 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.

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

[33] P. Ram and A. Gray, “Which space partitioning tree to use for search,” in Proc. Adv. Neural Inf. Process. Syst. (NIPS’13), Lake Tahoe, NV, USA, Dec. 2013, pp. 656–664.

[34] 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.

[35] ftp://ftp.ivc.polytech.univ-nantes.fr/IRCCyN_IVC_DIBR_Videos/Videos/